Intelligent Management Experience on Efficient Electric Power System

A. Martín[1], C. León[1], and F. Biscarri[1]

[1] Department of Electronic Technology
E.T.S.I.I., Sevilla University
Avda. Reina Mercedes s/n. 41012 – Sevilla, Spain
Phone/Fax number: +0034 954 559991, e-mail: toni@us.es, cleon@us.es, fbiscarri@us.es

Abstract. Electric power system is one of the most critical and strategic infrastructures of industrial societies. Nowadays, it is necessary the modernization and automation of the electric power grid to increase energy efficiency, reduce emissions, and transit to renewable energy. Power utilities face the challenge of using information and communication networks more effectively to manage the demand, generation, transmission, and distribution of their commodity services. Communication network constitutes the core of the electric system automation applications, the design of a cost-effective, and reliable network architecture is crucial. To resolve this difficulty in this work we study the integration of advanced artificial intelligence technology into existing network management system. This work focuses on an intelligent framework and a language for formalizing knowledge management descriptions and combining them with existing OSI management model. We have normalized the knowledge management base necessary to manage the current resources in the telecommunication networks. Intelligent agents learn the normal behaviour of each measurement variable and combine the intelligent knowledge for the management of the network resources. We present an analysis of corporate network management requirements and technologies, together with our implementation experience with the development of an integrated management system for a company network.

Key words

Artificial Intelligent, Expert System, Intelligent agents, GDMO, MIB, Network Management, TMN.

1. Introduction

As a result of the electricity evolution, the electricity infrastructure will get more and more inter-linked with network infrastructures. However, the same networking capabilities that can provide these benefits have also introduced vulnerabilities that have resulted in these systems having been identified as one of the most vulnerable targets for an operational network. The advanced technology of intelligent agents provides a well-researched way of implementing complex distributed, scalable, and open Information and Communication Technology (ICT) systems in smart grid. Intelligent control systems are an integral part of the critical infrastructures of power utilities. The capabilities of networking these systems provide unprecedented opportunities to improve productivity, reduce impacts on the environment, and help provide energy independence. Recent years have seen explosive growth in the areas of power system monitoring using intelligent agents and distributed intelligence. Typical work in related fields include intelligent systems such as [1] who present an intelligent supervisory coordinator for process supervision and fault diagnosis. In [2] an online intelligent alarm-processing system is developed based on the architecture of the digital substation. Other examples of application of intelligent agents include [3] who propose different type of univariate randomly optimized neural network combined with discrete wavelet transform and fuzzy logic. This paper [4] will look at some diagnostic requirements and emerging technologies available for insertion into future ship integrated power systems. Many researchers have suggested that intelligent sensor network technologies could improve the effectiveness and efficiency of real-time management. The objective of [5] is to develop novel system, which can cover many of the existing challenges in distribution power systems and make distribution grid more intelligent. [6]. In [7] an expert system is developed by utilizing its fast reasoning mechanism and object-oriented features.

This work presents a technique for the design and implementation of a distributed intelligent system that is designed through the normalization and integration of knowledge management. The goal is the assignment and dispersed intelligent control of network resources, pertaining to hardware as well as software, to help operators manage their networks more effectively and also to promote reliability in network services. This approach increases energy efficiency, reduce emissions, and transit to renewable energy. We describe an intelligent technique, which processes management knowledge collected by intelligent agents and uses it to detect and to resolve the network anomalies and faults.

This paper is organized as follows. In the section, we evaluate the approach of using intelligent agents and distributed control in each of these control architectures particularly in the context of strategic energy plans. In the second part we base this architecture on the requirements identified and suggest that power systems with high penetration of distributed generation may be controlled as a loose aggregation of energy control. In the third part we formulate flexible control architecture for the future electric power system. Finally we outline the conclusion and future works.

2.   Management Network

Telecommunication systems are essential elements to improve efficiency and economy in energy operation, transmission, distribution, storage, and utilization. There are two dominant network management models, which have been used to administration and control the most of existing networks: Telecommunications Management Network (TMN) and Simple Network Management Protocol (SNMP). Both network management systems operate using client/server architecture. SNMP standards are defined in a series of documents, called request for comments or RFCs proposed by the Internet Engineering Task Force (IETF) and TMN is introduced by the ITU-T (the former CCITT). In the public environment, a more heterogeneous mix of de facto telecommunications industry standards has prevailed, with a move toward TMN support. TMN was the first who started, as part of its Open Systems Interconnection (OSI) program, the development of the architecture for network management. There are three basic components comprising the elements of the OSI management architecture.

An information component involved with five major functional areas: fault, configuration, accounting, performance, and security management, which facilitate rapid and consistent progress within each category's individual areas [7]. A communication component focussed upon how the information is exchanged between the managed systems [8], and a functional component involved with the various activities performed in support of network management [9]. According to the International Organization for Standardization (ISO), the OSI network management model defines a conceptual model for managing all communication entities within a network. This main concept is the managed object (MO), which is an abstract view of a logical o physical resource to be managed in the network. MOs provide the necessary operations for the administration, monitoring and control of the telecommunications network. For a specific management system, the management process involved will take on one of two possible roles. The Manager Role is an element that provides information to users and the Agent Role is part of a device in the network that monitors and maintains status about that device, figure 1:
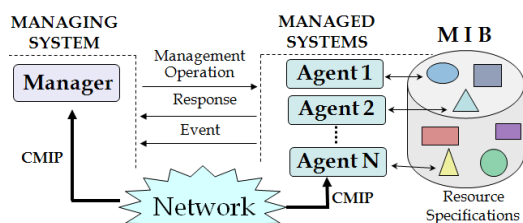

Fig. 1. OSI manager/agent architecture

The management functions currently exchange management information by means of techniques defined in ITU-T X.700. MOs are defined according to the Guidelines for the Definition of Managed Objects (GDMO), which has been established as a means to describe logical or physical resources from a management point of view. The guidelines for the definition of managed objects, ITU-T Recommendation X.722 allow

for a common data structure for MOs in the managed and managing systems. After this brief introduction to management elements, we will approach our research in the integration of knowledge management of expert system into MIB in the OSI management model.

3.   Management Knowledge Definition

Management information modelling and the denominated MO play a large part in this network management model. MO coordinates all the downstream real-time functions within the distribution network with the intelligent knowledge needed to manage the network in an efficient way. The management information model provides a common characterization of the network resources, enables multiple management functions to interact with each other, and supports different management functions. Management information is exchanged among management systems where management functions are implemented. Basically, GDMO prescribes how a network product manufacturer must describe the resource formally. GDMO uses an object-oriented approach to define the standardized functionality in substation devices [8]. A complete agent definition is a combination of a relationship between a class of managed objects, package, attribute, group of attributes, action, notification, parameter, connection of name, and behaviour, figure 2.
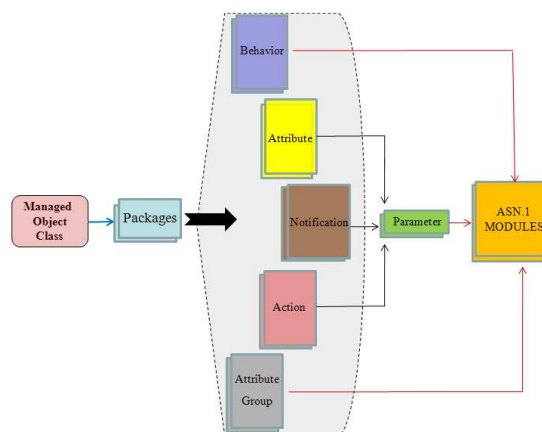

Fig. 2. Relations between GDMO standard templates

Managed Object Class (MOC) is the base of the formal definition of an intelligent agent (IA). The definition of a MOC is made uniformly in the standard template, eliminating the confusion that may result when different persons define objects of different forms. This template is used to define the different kinds of objects that exist in the system. This way we ensure that the classes and the management expert rules defined in system A can be easily interpreted in system B. MOC structure is show here:

```
<IA-label> MOC
  [DERIVED FROM  <IA-label> [,<IA-label>]*;]
  [CHARACTERIZED BY
      <IA_properties-label>[,<IA_properties-label>]*;]
  [CONDITIONAL PACKAGES
      <IA_properties-label>  PRESENT IF condition;
      <IA_properties-label>] PRESENT IF condition]*;]
  REGISTERED AS object-identifier;
```

DERIVED FROM, by using this clause, any attribute, operation, notification, and behaviour exposed by MOs, as

well as inheritance and containment relationships among MOs and MOCs, can be defined. Packages included in the object class definition are identified by the CHARACTERIZED BY and CONDITIONAL PACKAGES clauses. Finally, the REGISTERED AS clause identifies the location of the MOC on the OSI registration tree.

4. Intelligent Agent Modelling

In a heterogeneous and distributed energy context the application of IAs to perform soft real-time control functions for the power grid is a way to introduce new information management techniques and information security functions to the power grid. An IA is an autonomous hardware/software system, which can react intelligently and flexibly on changing operating conditions and demands from the surrounding processes. IA systems implement distributed decision-making systems in an open, flexible, and extensible way. IAs can actively and dynamically cooperate for solving problems by using integrated knowledge and intelligence reasoning. For this to occur, IAs are required to have knowledge management of their own local system and at least partial models of the global system [9]. To answer these questions, it will be necessary to make changes on the template of the GDMO standard.

Each intelligent object class may be seen as the integration of the following basic components: packages, name bindings, and behaviour characteristics. The elements that at the moment form the GDMO standard do not make a reference to the knowledge base of an expert system. We observe the need to define new structures for those cases in which it is necessary to express the knowledge. We propose to extend the GDMO with the following goals: facilitate the normalization and integration of the knowledge base of expert system into resources specifications. Thus the description of certain aspects of MO knowledge, e.g. the definition of expert rules, can be supported. We suggest a new description for the information management definition named GDMO+, which we add a new element named KNOW, as shown in figure 3.
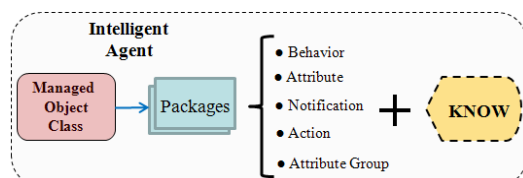

Fig.3. Template relations in GDMO+ methodology

Two relationships are essential for the inclusion of knowledge in the component definition of the network: Managed Object Class and Package. These templates allow IAs to have properties that provide normalized knowledge of a management dominion.

A. Package Archetype

The package template is used to specify the characteristics that represent a consistent set of specifications about an IA. The package template is a combination of behaviour definitions, attributes, attributes groups, operations, notifications, and parameters. The purpose of the package is to provide a set of reusable definitions that can be used in several intelligent agent class specifications. In addition to the properties indicated above, we suggest the incorporation of a new property called KNOWS, which contains all the specifications of the knowledge base for the expert system.

```
<IA-properties-label> PACKAGE
[BEHAVIOUR <behaviour-label> [,<behaviour-label>]*;]
[ATTRIBUTES
    <attribute-label> propertylist [,<parameter-label>]*
   [,<attribute-label> propertylist [,<parameter-label>]*]*;]
[ACTIONS <action-label> [<parameter-label>]*
         [<action-label> [<parameter-label>]*]* ;
[NOTIFICATIONS
    <notification-label> [<parameter-label>]*
   [<notification-label> [<parameter-label>]*]* ;]
[KNOWS    <know-label>  [,<know-label>]*;]
REGISTERED AS object-identifier;
```

Each IA has two types of knowledge: local network management for individual problem solving and community and local network management for coordination of associated node activities. KNOWS attribute will define all the aspects related to management knowledge in a specific intelligent system. This new property has an associated template called KNOW.

B. Knowledge Management Archetype Template

There are a number of different knowledge representation techniques for structuring knowledge in an expert system. The three most widely used techniques are expert rules, semantic nets and frames. For this study we use expert rules. We represented the knowledge in production rules. Rules are expressed as IF-THEN statements, which are relatively simple, very powerful as well as very natural to represent expert knowledge. A major feature of a rule-based system is its modularity and modifiability, which allow for incremental improvement and fine tuning of the system with virtually no degradation of performance. Template KNOW permits the normalized definition of the specifications of the expert rule to which it is related. This template allows a particular MOC to have properties that provide a normalized knowledge of a management dominion. The structure of the KNOW template is shown here:

```
<IA_know-label> KNOW
   [PRIORITY        <priority> ;]
   [BEHAVIOR <behavior-label> [,<behaviour-label>]*;]
   [IF occurred-event-pattern [,occurred-event-pattern]*]
   [THEN     sentence [, sentence]* ;]
   REGISTERED AS object-identifier;
```

The first element in a definition is headed. It consists of the name of the management expert rule <know-label> and a key word that indicates the type of template KNOW. After the head, the following elements compose a normalized definition of the management knowledge:
- BEHAVIOR: This construct describes the behaviour of the rule.
- PRIORITY: If there are two sources of evidence for some hypothesis, then this value represents the priority of

the rule, that is, the order in which competing management actions will be executed.

- IF: We can add a logical condition that will be applied to the events that have occurred or their parameters. The premise of a rule examines parameter or slot values, and once the condition evaluates to true, then the action part is executed.

- THEN: An agent's repertoire of tasks represents its capabilities or methods. These are actions and diagnoses that the management platform makes as an answer to network events that have occurred. Each task can have its procedural "how to do" component represented as expert rules.

- REGISTERED AS is an object-identifier and identifies the location of the expert rule on the OSI registration tree.

5. A Diagnostic Model

In order to validate our approach, we have developed intelligent control architecture in an electric power system. This system integrates the management knowledge into the network resources specifications. We study an example of alarm detection and intelligent resolution of incident concerning a private network. We have used a telecommunications network that belongs to a company in the electrical sector Sevillana-Endesa's (EA) a Spanish power utility. The Spanish power grid company has got a network using wireless on the regional high-tension power grid. Part of long-distance traffic in this net is controlled by a wireless intelligent system distributed throughout this private network. The use of integrate knowledge in agents can help the system administrator in using the maximum capabilities of the intelligent network management platform without having to use other specification language to customize the application.

The dynamic IA platform we have developed is named EXPAriel. The intelligent system development should meet the following requirements: it should be robust and management activity should not interfere with normal operations of the network and it should only intervene when necessary. We are going to use a SCADA system due to the management limitations of network communication equipment. SCADA consists of the following subsystems, figure 4:
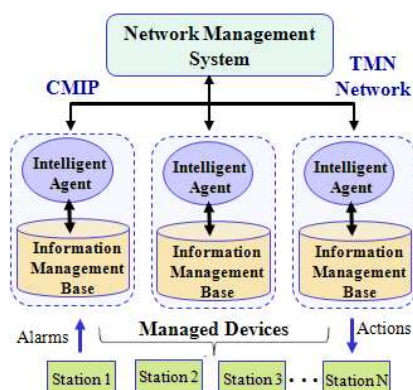

Fig. 4. Elements of the prototype EXPAriel

- Remote Terminal Units (RTUs) connecting to sensors in the process, converting sensor signals to digital data and sending digital data to the supervisory system.

- Communication infrastructure connecting the supervisory system to the RTUs.
- A supervisory (computer) system, gathering (acquiring) data on the process and sending commands (control) to the process, which is our IA.

SCADA systems are configured around standard base functions like data acquisition, monitoring and event processing, data storage archiving and analysis, etc. The RTU encodes sensor inputs into protocol format forwards them to the SCADA master. The fundamental role of an RTU is the acquisition of various types of data from the power process, the accumulation, packaging, and conversion of data in a form that can be communicated back to the master, the interpretation and outputting of commands received from the master, and the performance of local filtering, calculation and processes to allow specific functions to be performed locally. If we want to integrate a new RTU in an environment, then we will have to develop a new IA and its corresponding MIB module [10]. The supervision below and RTU includes all network devices and substation and feeder levels like circuit breakers, reclosers, autosectionalizers, the local automation distributed at these devices, and the communications infrastructure. Our system has three major components: an inference engine, a knowledge base, and a user interface, figure 5. Those elements are briefly discussed in the following:
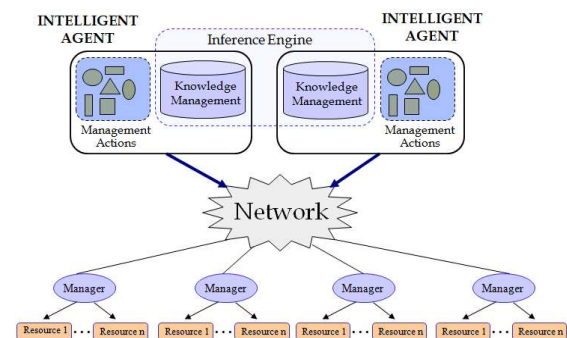

Fig. 5. Architecture System

- The inference engine: This is the processing unit that solves any given problems by making logical inferences on the given facts and rules stored in the knowledge base. Our system is implemented in Brightware's ART*Enterprise, an expert system shell. ART*Enterprise is a set of programming paradigms and tools that are focused on the development of efficient, flexible, and commercially deployable knowledge-based systems.

- The knowledge base: The core of the system, this is a collection of facts and if-then production rules that represent stored knowledge about the problem domain. The knowledge base of our system is a collection of expert rules and facts expressed in the ARTScript programming language ART*Enterprise. The knowledge base contains both static and dynamic information and knowledge about different network re-sources and common failures. The resultant expert system has about 600 rules and it has been employed Workstation to program the expert system.

- Human Machine Interface: EXPAriel reports to human operators over a specialized computer called Human-

Computer Interface (HCI). IAs sometimes need to communicate with operators. The HCI provides the operator with the best "as operated" view of the network. Each device provides a time-stamped message on events (starting, tripping, activation, etc.) through the bus. These events are sorted by time and transmitted to the event printers or to the monitoring system, figure 6.

Fig. 6. Network Alarm Monitor

6. The Communication Supervisory System

The nerve centre of any power network is the central control and management function, where the coordination of all operational strategies is carried out. EXPAriel operations use a supervision system called Communication Supervisory System (CSS). This system can monitor, in real time, the network's main parameters, making use of the information supplied by the SCADA, placed on the main company building, and the RTUs are installed at different stations. The CSS allows the operator to acquire information, alarms, or digital and analogical parameters of measure, registered on each IA or RTU. The CSS has the capability of selecting the IA that is best suited for satisfying the client's requirement, without the client being aware of the details about the agent. Further, the IA is able to communicate and negotiate with the other IAs. Figure 7 shows a hierarchical architecture that represents the whole network, the IA, RTU objects, and the network elements.
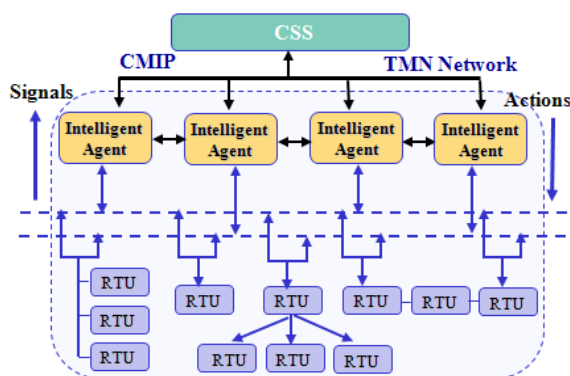

Fig.7. Communication Supervisory System (CSS)

Control functions are initiated automatically from software IA and directly affect power system operation. Automatic control is triggered by an event or specific time that invokes the control action. IA automatically initiates a set of sequential management actions to restore the network resource. The sending agent is aware of the interests of the other IAs and may notify other agents automatically when exception conditions are either detected or may be probable or imminent. IA adds a great

deal of intelligence and automation to our system management, making the management network much easier.

A. Example of Knowledge Management definition

Next paragraph shows a complete example of expert rules integration in the GDMO+ proposed standard. It defines a MOC named *radioTrasceiverCTR190* corresponding to a real device in the network of a power utility.

```
radioTransceiver_CTR190 MANAGED OBJECT CLASS
  DERIVED FROM radioTransceptor;
  CHARACTERIZED BY transceiverPackage;
  REGISTERED AS {nm-MobjectClass 1};
```

This is a device both sends and receives radio signals. Their primary purpose is to broadcast the signal. These units typically offer the convenient of multiple functions like establishing radio channel, control signals, monitoring station, monitored alarm condition, control logic to activate operations in response to commands received over said communications network, etc. [11]. The class *radioTransceiver* includes the compulsory *transceiverPackage* which contains all the specifications corresponding to the device. We can indicate the two expert rules which have been associated with the defined class by means of the KNOWS clause.

```
transceiverPackage PACKAGE
ATTRIBUTES reception Power GET, sense GET, …;
NOTIFICATION damageFeeding, inferiorLimit, …;
KNOWS transmissionError, powerError;
REGISTERED AS {nm-package 1};
```

Quite two typical examples of expert rules used in our GDMO Specification are *transmissionError* and *powerError*. These rules are defined by using the KNOW template. The expert rules are used within EXPAriel to capture and detect anomalies or defect of operations produced in the transceiver device and suggest the necessary measures for solving the problem.

```
transmissionError KNOW
 PRIORITY 4;
 BEHAVIOUR transmissionErrorBehaviour;
 IF (?date ?time1 ?local 7_TX_C2 ?remote ALARM)
 (?date ?time2 ?local 7_TX_C2 ?remote ALARM & :
  (<(ABS(? ?time1 ?time2)) 1.00))
 THEN ("Severity:" PRIORITY) ,
  ("Diagnostic: " It damages in the modulate transmission
between", ?local, "and" ?remote),
  ("Recommendation "Revision transceiver"");
REGISTERED AS {nm-rule 1};
```

The rule *transmissionError* is devoted to the detection of errors in the data transmission module of the transceiver CTR190.

7. System Evaluation and Testing

Validation constitutes an inherent part of the knowledge based expert system development for EXPAriel and is intrinsically linked to the development cycle. In order to check the improvements of the GDMO+ IAs with a real application in this section, we have compared ExpAriel with a traditional expert system. An important aspect of the design and implementation of an intelligent system is

determination of the degree of speed in the answer that the network provides. Figure 8 shows a sample plot of these parameters that was collected as a part of the experiment, which shows that the speed of the EXPAriel system improves the proceeding time and the average of the traditional expert system.
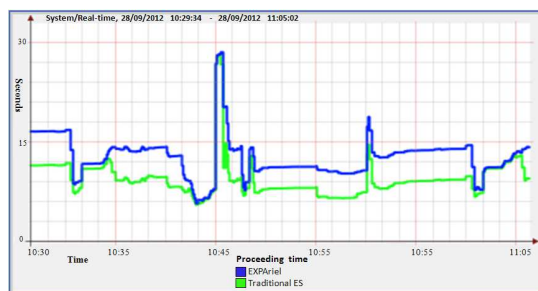

Fig.8. Performance EXPAriel & traditional ES

In Table I, we present the average set-up time for some measurements. As the table shows, the results for EXPAriel are 15.1% better than proceeding time and 19.5% better than executing time rules/sec in the traditional expert system. Another test of significance is the analysis of the number of alarms that have been automatically resolved by EXPAriel and the warnings received by the system operator. As noted in the next table 2, EXPAriel performs satisfactorily with about a 94.6% rate of success in real cases.

Table 1. Comparison Traditional Expert System & EXPAriel

	Traditional ES		EXPAriel	
	Proceeding time	Rules/Sec.	Proceeding Time	Rules/Sec.
A1	1,525 Sec.	109,120	1,250 Sec.	124,0000
A2	6,561 Sec.	45,773	5,249 Sec.	55,8202
A3	3,213 Sec.	69,156	2,975 Sec.	85,3782
A4	21,758 Sec.	17,125	17,982 Sec.	19,2415
A5	0,142 Sec.	388,983	0,118 Sec.	432,2034

Table 2. Performance management events and alarms

Alarms Number	Autonomous Resolution	Autonomous Resolution %	Managed Actions Executed	Operator Warnings
100	99	99	151	1
200	190	95	202	6
400	369	92,25	501	16
600	562	93,66	793	16
800	745	93,12	994	23
1000	946	946,1	1528	49

8. Conclusions

Current networks are very complex and demand ever-increasing levels of quality, making their management a very important aspect to take into account. The traditional model of network administration has certain deficiencies that we have tried to overcome by using a model of intelligent integrated management. To improve the techniques of expert management in a communications network, we propose the possibility of integrating and normalising the expert rules of management within the actual definition of the MOs. In this paper we show

possibilities to apply and integrate artificial intelligence techniques in network management and supervision by using the proposed standard GDMO. Distributing intelligent power system control and analysis is viewed as one of the fastest growing areas of research and new application development in network management. We have investigated the innovative control architecture in electric power systems, in which we are using IAs. We conclude by pointing out an important aspect of the obtained integration: the solution not only masks possible faults but also optimizes the management functions and efficiency of the distributed services and their resources by using an artificial intelligent strategy, while ensuring a high degree of functionality in power utilities.

Finally, future work is to improve the agent's performance using another method of knowledge representation and reasoning different to the rules: Semantic nets, neuronal nets, frameworks, etc. In addition to fault detection functional area we would also like to expand the scope of our current work to other functional areas like accounting management, configuration management, performance management and security management

References

[1] O.C. Akinyokun, A.A., Imianvan. Mobile agent system for computer network management Proceedings from the International Conference on Advances in Engineering and Technology, Pages 796-808. 2006.
[2] M.A., Bihina Bella, J.H.P. Eloff, M.S. Olivier. A fraud management system architecture for next-generation networks. Forensic Science International, Volume 185, Issues 1-3, 10. Pages 51-58. 2009.
[3] R.J. Brachman & H.J. Levesque. Representation and reasoning. San Francisco, CA: Elsevier/Morgan Kaufmann. 2004.
[4] S. Chantaraskul & L. Cuthbert. An intelligent-agent approach for congestion management in 3G networks, Engineering Applications of Artificial Intelligence, Volume 21, Issue 4, Pages 619-632. 2008.
[5] D. D'Addona & R. Teti. Intelligent Tool Management in a Multiple Supplier Network. CIRP Annals - Manufacturing Technology, Volume 54, Issue 1, 2005, Pages 459-462.
[6] G. Doukas, K.D. Patlitzianas, K. Iatropoulos & J. Psarras. Intelligent building energy management system using rule sets. Building and Environment, Volume 42, Issue 10, Pages 3562-3569. 2007.
[7] A. Martín, C. León, J. Luque & I. Monedero, "A framework for development of integrated intelligent knowledge for management of telecommunication networks", Expert Systems with Applications, Volume 39, Issue 10, Pages 9264-9274, 2012.
[8] S. Yang, Y. Chang, "An active and intelligent network management system with ontology-based and multi-agent techniques", Expert Systems with Applications, Volume 38, Issue 8, 2011.
[9] J. Ding, "Advances in network management", Boca Raton: CRC Press, 2010
[8] D. Nikolaou & T. Wolf, "Architecture of network systems", Burlington, Morgan Kaufmann, 2011
[10] L. Walsh, "SNMP MIB Handbook: essential guide to MIB development, use and diagnosis" Stanwood, WA : Wyndham, 2008
[11] J. Liebowitz, "Knowledge management handbook, collaboration and social networking" Boca Raton, Fla.: CRC Press, 2012