An Intelligent and Mobile Agent-based Approach for Dynamic Protection Set-up in Future Optical Networks

Daniel Rossier-Ramuz[†°], Dr. Daniel Rodellar[†], Dr. Rudolf Scheurer[°]
[†]*Swisscom Corporate Technology and* [°]*University of Fribourg*

Key words: Intelligent wavelength services, intelligent and mobile agents, FIPA, quality of protection

Abstract:

The future Wavelength Division Multiplexing (WDM) based optical networks are expected to provide new Intelligent Wavelength Services (IWS) for the transport of all types of data (voice, multi-media, Web-based data, etc.) at bit rates exceeding 1 TBit/s. The survivability of such networks will depend on efficient protection mechanisms. Although several protection strategies will be proposed to the customers, managing the complexity of protection-related interactions between client layers and the optical network will become a considerable challenge. In this paper, we develop a number of statements related to the management of IWS and we propose an approach based on intelligent and mobile agents in order to tackle the management of protection-related client requirements. In that scope, we introduce the notion of p-groups as a possible client requirement and we define a Quality of Protection (QoP) as a new metric to assess the protection quality during the lifetime of client connections.

1. INTRODUCTION

The tremendous growth of bandwidth needs expressed by end customers has made the Wavelength Division Multiplexing optical networks very attractive. But the client demand matrix has not only increased in terms of

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35491-0_28
A. Jukan (ed.), *Towards an Optical Internet*

bandwidth but also regarding the diversity of the client requirements related to the different protocols and architectures used on top of the Optical Transport Network (OTN).

The QoS-based end-to-end optical channel allocation and protection requirements for future mesh optical networks remain an important subject of research. At the University of Fribourg, the OPTIMA[1] project aims at studying new advanced solutions based on intelligent and mobile agents for the management of future OTN.

The investigations within OPTIMA will mainly focus on transparent OTN, i.e. transparent in the sense that the regenerators and wavelength converters within the OTN are fully operating in the optical domain, without electrical/optical conversion. We consider the transparent OTN as an intermediate step in the technological development towards a full-optical OTN based on optical packet switching OPTIMA is also intended to contribute to the conception of Intelligent Wavelength Services (IWS). The goal of IWS is to provide more intelligence and thus flexibility to OTN in order to integrate a multitude of client protocols as well as to cope with their specific requirements regarding protection.

In this paper, we first introduce the next generation of optical networks and the concept of Intelligent Wavelength Services (Chapter 2). In a next step we discuss the protection issues related to IWS as imposed by the complexity of dependencies between client protection requirements, and we introduce a way to formally define protection requirements and to express protection quality (Chapter 3). This will be the base for the introduction of the mixed stationary/mobile agent based architecture to manage the allocation of protection paths in IWS (Chapter 4). We finally present our conclusions so far and the plans for future work (Chapter 5).

2. NEXT GENERATION OPTICAL NETWORKS

New advances in optical technology now allow carrying signals optically in the network from end to end, and thus totally eliminating the need for electrical regeneration. Owners of the optical networks may use four network functionalities to make their transport networks more agile (protocols like IP and MPLS can also profit from these functions). The first function is the Optical Add-Drop Multiplexing (OADM) that allows inserting and removing a given wavelength from the optical fibre; the second one is wavelength routing that enables to route wavelengths from input fibres to the output ones. The third function is wavelength conversion.

[1] OPTical network management with Intelligent and Mobile Agents – project submitted to the Swiss National Science Foundation

Finally there is optical switching that enables wavelength switching capabilities from one fibre to another (the wavelength is present on one fibre or the other). The four functions are shown on *Figure 1*. Although they are all represented on a static basis for comprehension purposes, they could have a dynamic behaviour (variation as a function of time).

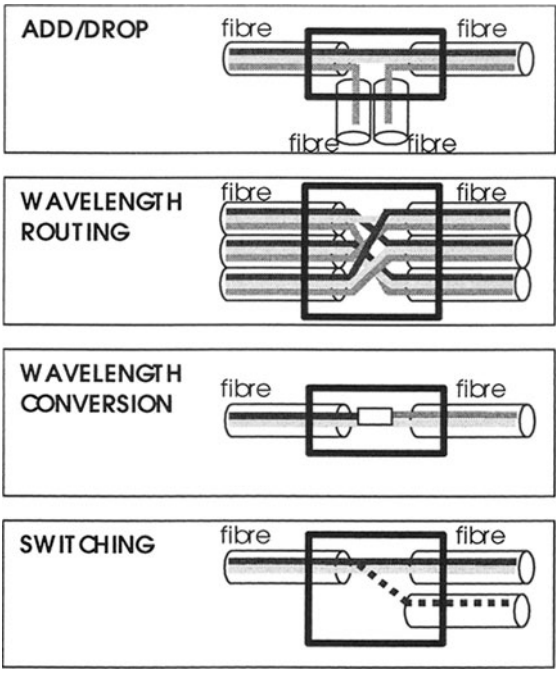

Figure 1. Four types of functionality of next generation optical network elements

The elements realising these functions can operate in the optical domain without requiring optical/electrical conversion. The WDM equipment should perform several of these functions concatenated. Full optical components capable to route whichever inputs to whichever outputs on whichever wavelengths will gradually appear on the market, going through intermediate ranges of limited equipment. Basically, the switch matrix is quite limited nowadays (in the order of 32 x 32 optical wavelengths) and the optical transponder does not provide full conversion between all the wavelengths. Wavelength continuity constraint consequently remains to be considered when new optical paths are being allocated. These constraints introduce potential blocking problems when the client demands are being allocated.

The concept of Intelligent Wavelength Services (IWS) will provide an advanced optical transport layer that will promote the Fibre To The Home

(FTTH). This paper proposes a novel agent-based architecture to tackle the dynamic protection management in an optical mesh network.

2.1 Intelligent Wavelength Services (IWS)

The future OTN will have to support all kinds of client protocols (IP, Gigabit Ethernet, PoS, clear-channel with bit rates from 2 Mbit/s to 2.5 Gbit/s, etc.) in a multi Service Providers (SPs) and multi Network Operators (NOs) environment. New business models are now emerging to support the new inter-parties interactions. We believe that this is a pre-requisite for a successful deployment of "fibre to the home" (FTTH) networks, in which the customers will dynamically allocate and release wavelength transport channels for specific data services (voice, digital TV, Internet, etc.). In this context, the elaboration of some kind of automatic Service Level Agreement (SLA) based negotiations as considered in the future UMTS networks seems to be a promising way to support the client requests.

Hereafter, we use the concept of Intelligent Wavelength Services (IWS) depicted on *Figure 2*. IWS support all the network and service management functions of the OTN, i.e. from the network element as well as from the customer viewpoint. It has to be noted that for IWS, the customer can be either a service provider or an end-user.

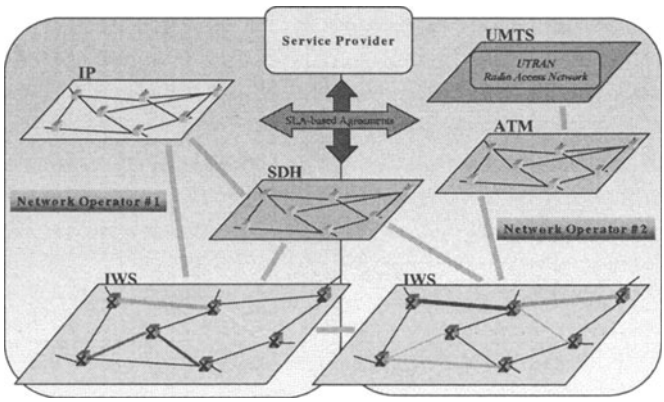

Figure 2. IWS in a multi-SP multi-NO environment and supporting multiple client protocols

The SLA in the IWS is used between the customer and the network operator to specify explicitly the traffic conditions regarding bandwidth, channel availability, protection requirements, type of interface, etc. The IWS

will configure the OTN dynamically in order to meet the objectives as described in the SLA. Normally, if one of the specified objective can not be satisfied, even for a limited period of time, the NO has to pay penalties to the customer. The description of the negotiation process taking place behind the SLA is out of the scope of this paper. A similar SLA-based approach for future UMTS networks can be found in [LRDC+Oct00].

2.2 Management Issues

The functional aspects of OTN management are currently under investigation in ITU-T. The Telecommunication Management Network (TMN) [M3100May96] is usually considered as the generic framework for the definition of all information related to managed objects and to the interactions between managers and agents. The TMN platform-centred approach however entails drawbacks in scalability, reliability, efficiency, and flexibility and is consequently unsuitable for large and heterogeneous networks [ZZ1998].

In TMN, two information streams are used for management purposes: the first stream uses the Data Communication Network (DCN) of TMN and usually requires an IP-based network. The second stream consists in an Embedded Communication Channel (ECC), in which in-band signalling can be passed through between Network Elements (NE). The signalling protocol is implemented by the transport protocol itself (SDH, ATM, etc.) and requires specific bytes from the overhead.

The search for optimal protection paths attached to an optical end-to-end connection can be based upon the definition of the Routing and Wavelength Assignment (RWA) problem described in the next section. The on-line computation requires a distributed version of the algorithms used to solve the RWA. The approach we are investigating consists in a combination of TMN legacy systems with advanced distributed mechanisms to deal with the dynamic client requests as well as with their protection requirements. To do this, we use intelligent agents making complex interactions between NEs possible.

The software agent-based architecture proposed in this paper uses as much local information as possible. Local information is called the *environment* of the agents. From the implementation viewpoint, access to the information is provided by the use of a specific gateway. In the future, the transport of messages between agents or the transport of the agents themselves will be possible thanks to new structures such as Digital Wrapper or ASON [NBJan99,D697Apr00]. Such an approach is already described in [RSDec99].

2.3 Dynamic Routing and Wavelength Assignment (RWA)

We define the *lightpath* as the optical path used for a client connection, i.e. the path between an optical source node and an optical destination node. A lightpath can use one or several wavelengths along the way.

The RWA can be divided into two sub-problems: the *routing problem* that is, finding the route between two optical nodes and the *wavelength assignment problem* that is, finding the best wavelength allocation along the discovered route. Combining the two sub-problems provides a solution minimising the number of wavelengths required in an optical network for a given traffic matrix. Both of the two sub-problems are difficult to solve (NP-complete) and require the usage of heuristics. An overview of RWA algorithms and heuristics as well as the mathematical formulation of the problem can be found in [EUR709Apr99], [ZJMJan00].

The RWA problem is originally considered during the network design and planning process, when business costs are relevant. Therefore, most of the algorithms proposed to solve RWA are based on a centralised architecture in which the entire network topology is known in advance. The traffic matrix is required by the RWA and is normally issued by statistical data. At this stage, there is no dynamic consideration. The working paths and the protection paths are established in a similar way.

This is possible as long as the traffic matrix does not differ from reality too much and the client demands are static. As soon as the client demands are dynamic and the requirements regarding the protection are different from one customer to another, as will be the case in IWS, the protection paths and the working paths have to be computed dynamically. The major problem of the dynamic approach resides in the blocking problem, i.e. there is no available wavelength to satisfy a client's demand.

The agent-based algorithms firstly require the study of distributed algorithms. For RWA, and more specifically for the wavelength assignment part, we have found the Dynamic Relative Capacity Loss (DRCL) algorithm. The implementation of DRCL with FIPA agents is explained in section 4.3.

2.3.1 Dynamic Relative Capacity Loss (DRCL)

The DRCL algorithm [ZJMJan00] is the distributed version of RCL. Briefly explained, DRCL consists in calculating the *relative capacity loss* for each path on each available wavelength every time the network state changes. For each client request, the route is first found using the Bellman-Ford algorithm; the wavelength minimising the RCL value is then selected.

The RCL values are stored locally in the optical node and are updated in a distributed way after a new path has been allocated.

In the IWS, the RCL values are handled by stationary agents (see section 4). RCL tables and agents are considered as the *environment* in which M-agents (mobile agents) evolve.

2.4 Protection Management

Since several Tbit/s will be transported through the OTN and since the protection will be considered as a value-added service, protection management in IWS is a strategic key issue. The protection schemes in OTN are derived from the mechanisms as specified by ITU-T [G841Jul95] for SDH networks; the dedicated protection (1+1) and shared protection (1:n or n:m) are two essential protection modes.

As considered in our research, however, the IWS, will give the customer the opportunity to select different protection strategies according to his needs. The protection might already be present at the client layer, or might be required at both layers (client + OTN layers).

2.4.1 Protection / Restoration

Two important strategies for protecting OTN are based on protection and restoration mechanisms. The former consists in allocating protection paths so that the protection mechanism can be raised using hardware mechanism and can thus react very fast. The latter is initiated right after the failure and consists in finding alternative paths in order to preserve the running services.

The restoration can be proposed as an ultimate way to keep a service running in case of failure. When a customer claims low quality protection, it might happen that no protection paths are available when a failure occurs. In this case, the only way to preserve the connection is to launch a restoration mechanism. We have not considered this approach in our research yet.

2.4.2 Dedicated / Shared Protection

The dynamic protection set up might result in a combination of mixed dedicated and shared optical channels, depending on the availability of protected paths at a given time and on the priority of client requirements. We assume that the dynamic reconfiguration capabilities of OTN allow the configuration of protected paths to be changed over time.

The client requirements related to QoS, including the protection, can be described in the SLA before the allocation of optical resources. At the

moment, we are investigating a possible description of protection-oriented requirements.

3. PROTECTION ISSUES IN IWS

In this chapter, we propose two concepts that allow us to figure out optimal protection paths: ***p-group*** and ***QoP***.

3.1 Inter-operability with Client Layers / Protected Group (p-group)

The future IWS will support all kinds of client protocols as well as advanced client requirements, particularly concerning the protection strategy. In this context, the customer could own a certain group of NEs like SDH, ATM or IP switches, for example. Virtual topology - or logical topology - is the set of connections that will be set-up by the higher-level network using the OTN. This kind of requirement also refers to the concept of Virtual Private Network (VPN).

Four different protection strategies have been identified according to the customer's wish (*Figure 3*): protection at the OTN layer, protection at the client layer, protection at both layers or no protection at all. As an additional requirement, the customer could also tell the IWS how many failures points do the client accept to have (single failure/multiple failures). Another kind of requirement consists in claiming special protection by giving a sub-topology, e.g. a critical zone, requiring better protection than the rest of the network. The customer could have experienced that a high traffic load will occur in a certain country at a certain point of time and could therefore require 100% protection for this part of the network.

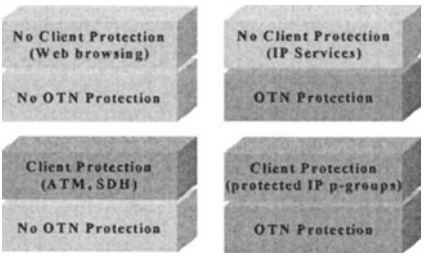

Figure 3. Possible Protection Schemes between client layers and the OTN

A possible way to express the client requirement regarding the protection strategy formally is the protected group (p-group, *Figure 4*), as described in [Cro1998]- "*the p-group represents the demands belonging to a common protected group of the higher level network. Each p-group is characterised by a number and is a list of demands*". The number refers to the level of protection (1 means that the client layer is able to support 1 failure).

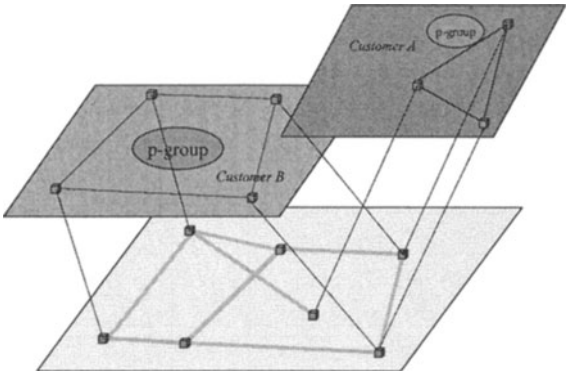

Figure 4. Two customers with their own protected VPN sharing the same physical OTN

The concept of p-group allows the customer to specify a virtual topology for the protected network components. In the future, the customer will decide which part of the VPN should be protected, and he will indicate the quality degree of the required protection. The interoperability of protection mechanisms between the client and the OTN must be considered and can lead to three potential problems: the *bottleneck*, *connectivity* and *multiple groups* problem. Details concerning interoperability issues can be found in [Cro1998].

3.2 Quality of Protection (QoP)

The second concept is based on a metric called Quality of Protection (QoP), which is being developed at our institute. Thanks to QoP, the agents will be able to assess the quality of protection dynamically and therefore to compare it with the requirements specified in the SLA. QoP(t) provides a temporal metric for an on-line measure of the protection quality.

To define a QoP metric, we first need to understand which components can fail and at which frequency. An analysis of this issue is proposed in [GRMar00]. In a first approach, we have decided to consider two components: *the entire node* and *the optical fibre*.

Let us define the following two functions: SN(t), the number of Shared Nodes along a protected path, SL(t) the number of Shared Links (fibres) along a protected path. It has to be noted that the shared link implies that the protection and working paths are on the same link but are using different wavelengths. In case of fibre failure, the connection obviously breaks down. Shared links are acceptable only in the case of optical channel malfunction within the optical node.

SN(t) and SL(t) are time dependent. The configuration of protected paths can change over time. If SL(t) is constantly equal to 0, it means that the protection path follows a dedicated (1+1) protection strategy. Moreover, if SN(t) = 0, the protection path uses disjoint nodes that those used for the working path.

Let us define $P_{NetworkFailure}$ as the probability that a failure occurs in the OTN layer (fibre cut, node malfunction) and $P_{ServiceFailure}$ as the probability of a service disruption. The *Dynamic Protection Set-up* (DPS) problem is stated as follows:

DPS: *given an end-to-end connection, find a protection path that maximizes QoP(t).*

$$QoP(t) = \begin{cases} QoP(t) = 1, & \text{if SL = 0 and SN = 0} \\ QoP(t) = \alpha\omega_1 \dfrac{1}{SN(t)}\beta(t), & \text{if SL = 0 (dedicated 1+1)} \\ QoP(t) = \alpha\omega_2 \dfrac{1}{SL(t)}\beta(t), & \text{if SN = 0} \\ QoP(t) = \alpha(\omega_1 \dfrac{1}{SN(t)} + \omega_2 \dfrac{1}{SL(t)})\beta(t), & \text{otherwise} \end{cases}$$

with $\omega_1 + \omega_2 = 1$

$0 < QoP(t) < 1$, 1 means that the quality of protection is maximal, 0 means no protection quality.

$0 < \alpha < 1$ is to be considered in case of multiple operators (or domains) interactions. α is a constant value and refers to horizontal interactions (see *Figure 5*). This factor can be used to assess the overall influence on the protection when an end-to-end connection needs to traverse several domains.

$0 < \beta < 1$ is a time function that assesses the respect of constraints related to the interoperability between the protected groups of the client layer

and OTN. The value of β depends on client demands and can change dynamically depending on the current configuration of protection paths. This factor is concerned with multi-layer interactions (see *Figure 5*). Details of this function are still under investigation.

$0 < \omega_1, \omega_2 < 1$ are two factors associated to the time function SN(t) and SL(t) accordingly. The customer can give them as part of his protection requirements and can also give information concerning the importance given to SN and SL functions (i.e. rather shared nodes, rather shared links).

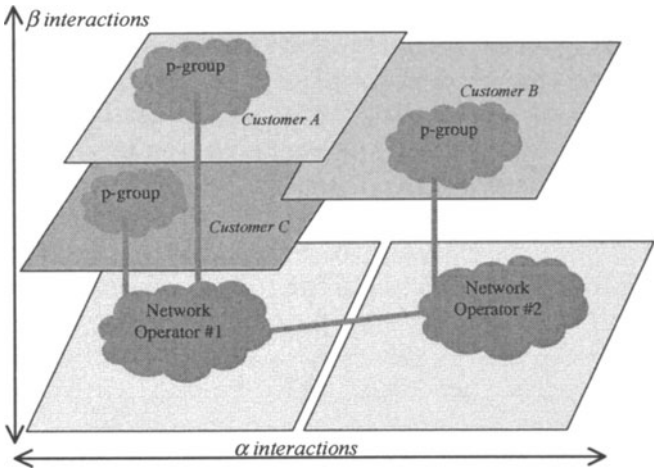

Figure 5. Two-dimensional interactions for the quality of protection (multi-layer, multi-NO)

From the customer's point of view, the protection requirement can be expressed as the probability that the service will be disrupted. This can be simply computed as follows:

$$\mathbf{P_{ServiceFailure} = P_{NetworkFailure} * (1 - QoP)}$$

The value $P_{ServiceFailure}$ can be monitored in a continuous way. If QoP is equal to 1, the protection is maximal and the probability that the service will be interrupted is reduced to 0. Without any protection, QoP is equal to 0, and the probability of being in trouble is equal to the probability to be in trouble at the OTN layer.

Having defined the p-group and QoP metric, the customer can now specify the protection level, the weight attached to shared nodes/shared links and the sets of p-group as possible protection-oriented requirements.

4. AN AGENT-BASED APPROACH

In this chapter, we describe an agent-based approach we are investigating in order to deal with the complexity of dynamic protection management based on complex requirements, as described in section 3. We introduce two families of agents, FIPA-agents – which handle DRCL tables - and M-agents – which use the QoP metric to find optimal paths.

Intelligent software agent technology can be considered as a natural extension of object-oriented technology. Although there is no widely adopted definition the agent itself, an intelligent agent should exhibit a minimal set of properties such as: *autonomy* – the agent has its own execution context (code+data), *reactivity* – the agent is able to react to external events (alarms, notification, etc.), *pro-activity* – the agent is able to make decisions according to its mental state, i.e. its internal representation of the environment, and *sociability* – the agent is able to communicate with other agents, i.e. to exchange complex knowledge in order to achieve certain objectives. The intelligence of such systems does not only refer to the agent behaviour itself but also to the intelligent behaviour that emerges from a society of agents that is, the results of co-operative work performed by all the agents. Methodologies for the design of multi-agent systems (MAS) are still under investigation. Further details about software agent can be found in [BZW1998,HBMar99].

The concept of intelligent agent in telecommunication has gained growing interest since Internet and the Java programming language appeared. The deployment of large-scale agent systems is now possible and can gradually be implemented into network devices. Standard organisations such as **FIPA**[2] or **OMG**[3] are promoting agent-based systems by focusing on interoperability between agent platforms.

In order to ensure that the message content exchanged between agents is correctly interpreted and to avoid mismatch between the different domains of management, the representation of terms and rules governing a given domain is precisely specified. This representation is called *ontology*. In the context of software agents, the ontology is the basic level of a knowledge representation scheme. It gives a meaning to terms, so that terms exchanged between agents can be correctly understood. Specifying ontology is particularly important in case of multiple domains (SPs/NOs) interactions. The definition of an ontology related to IWS is part of our research.

Based on the RWA decomposition, we are developing two families of intelligent agents. The first family of agents is constituted by stationary FIPA-compliant agents that reside in every optical node. Their objective is to

[2] Foundation of Intelligent Physical Agents – http://www.fipa.org

[3] Object Management Group – http://www.objs.org/agent

maintain RCL tables used by the DRCL algorithm in order to provide an optimal wavelength assignment for a given route. The second family contains adaptive mobile agents (M-agents) that are responsible for finding appropriate routes within the network. These agents are characterised by their ability to embed client requirements related to the protection strategy dynamically.

4.1 FIPA and FIPA-OS

FIPA agents can be implemented with the Nortel FIPA-OS[4] platform, the first publicly FIPA-compliant agent platform. FIPA-OS is an *Open Source* project and is well designed for telecommunication applications. FIPA-OS supports most of the FIPA specifications.

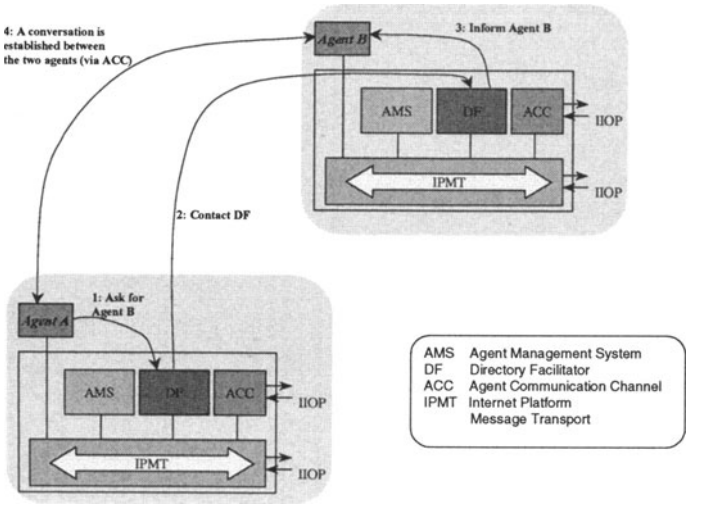

Figure 6. FIPA communication model for an agent platform

The distributed nature of agent-based applications requires advanced mechanisms for knowledge exchanges. The agents operate in an asynchronous way and can process messages belonging to several domains (SPs/NOs). FIPA has designed a communication model using the notions of *ontology* and *Agent Communication Language* (ACL). While the ontology is used to define a collection of terms and rules related to a specific domain,

[4] http://fipa-os.sourgeforge.net

the ACL gives the agents the flexibility required to establish some kind of advanced conversation. The ACL is made up of several types of messages called *performatives*. The performatives allow one agent to inform another agent of its intention. The agent then adapts its internal representation of the environment according to the message content. Examples of performatives are *request, query if, inform, reject*. The performative itself includes a message content expressed in a content language such as SL0 or RDF. Both languages are supported by FIPA-OS.

FIPA architecture has defined three basic agents (*Figure 6*): AMS, ACC and DF. Briefly explained, the AMS is considered as the kernel of the agent platform, the ACC is responsible for send/receive messages and the DF is a kind of "yellow page" service, which provides information about the registered agents.

4.2 Our approach: FIPA agent and M-agents

The software agent can be either *stationary* or *mobile*. Mobile agents are now easier to study since programming languages such as Java support code mobility. Several mobile agent platforms such Aglet, Odyssey, Voyager, Tacoma, and more recently Grasshopper[5] which is the first OMG MASIF[6] compliant mobile agent platform are available. At our institute, we are investigating new mobile agents (M-agent) and interaction models. We wish to use the abstraction of mobility as an efficient way of managing the protection requirements in the future IWS. Typically, M-agents will be used for the routing part of the RWA problem.

FIPA agents are stationary agents implemented into the optical nodes. The main function of a FIPA agent is to maintain the RCL table up to date and to manage the interactions with M-agents. The next section describes the implementation of DRCL into FIPA-agents using a peer-to-peer protocol for the knowledge exchanges.

4.3 Wavelength Assignment Using Stationary FIPA Agents

We now proceed to describe briefly the implementation of DRCL into FIPA agents.

[5] http://www.grasshopper.de

[6] Mobile Agent Service Interoperability Facilities http://www.omg.org

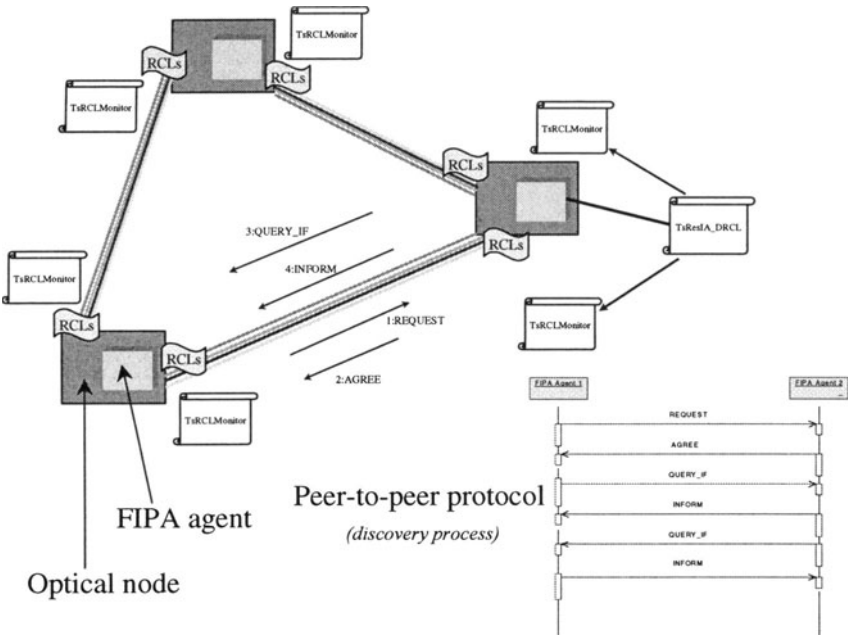

Figure 7. Implementation of DRCL with stationary FIPA-agents

Figure 7 shows the FIPA agent based architecture we are developing. The agents have to keep internal RCL tables up to date. The agent task starts with a discovery process which can be initiated everywhere in the network. The agent discovers the output ports and initiates a task *TsRCLMonitor* for each port. This task creates a RCL table (RCLs in the figure) and establishes a conversation with the remote agent according to the peer-to-peer protocol depicted on the figure. A permanent conversation is then set up and will be referred to when the agent needs to send a message to this port. The performative *inform* is used to transfer the XML-encoded RCL tables. A comparison mechanism allows avoiding cyclic updates.

The RCL table is made of triples (src, dst, rcl) on each wavelength. It is therefore possible to know which destination is reachable from a source node for a certain wavelength. Once the M-agent has discovered a satisfying protection path, the wavelength with the lowest *rcl* value is selected.

4.4 Protection Management with M-agents

In this chapter, we give a short overview of the basic agent-based mechanisms that are presently being implemented in our research group.

The conjunction of two active agents societies provides optimal configuration for protection paths. M-agents are used to capture the client

protection requirements that are formulated with a rule-based language, which is not described in this paper. The M-agents then evolve in the network and try to find an itinerary that is, a route. The itinerary of M-agents is mainly based on their internal rules. One of the rules consists in finding paths to maximise the QoP metric. There is one M-agent per end-to-end connection.

Stationary FIPA agents are used to provide additional information to mobile agents regarding the wavelength assignment by computing the relative capacity loss. Once the destination node has been reached, the M-agent returns to the source node by selecting the appropriate wavelengths thanks to RCL tables.

The M-agent architecture is currently being defined. So is an interaction model relying on the abstraction of agent mobility. In the end, each protection path can be configured separately in a co-operative way.

5. SUMMARY AND FUTURE WORK

In this paper we have presented some intermediate results of our research work in the framework of the OPTIMA project. The investigations so far represent a promising basis for the further research work within OPTIMA.

Software agents provide an open, scalable and flexible way to deal with the legacy network management systems and the embodiment of specific OTN-related algorithms. On the one hand, stationary intelligent agents are able to perform reasoning and to transfer knowledge regarding local optical nodes; on the other hand, reactive and adaptive mobile agents figure out optimal routes thanks to a QoP temporal metric and interaction models. Such an approach can support future protection-oriented client requirements.

Within the context of OPTIMA, we intend to investigate in more detail the coordination models for different combination degrees of intelligent and mobile agents. From the ATM world, we are aware of ongoing research work centered on market-based approaches for resource allocation using agent technologies. We will investigate to which extent such approaches may be adopted and included in the IWS concept.

Furthermore it is planned to work on an OTN modelling tool to get a flexible framework to perform the (mainly functional) evaluations of our agent-based approaches. This tool will have to integrate the FIPA platform and the co-ordination models as developed in OPTIMA.

6. REFERENCES

[BZW1998] Walter Brenner, Rüdiger Zarnekow, Hartmut Wittig, "Intelligent Software Agents", Springer-Verlag Berlin Heidelberg, 1998.

[Cro1998] O. Crochat, "Wavelength Division Multiplexing Networks And Failure Protection", PhD thesis Nr 1851, Ecole Polytechnique Fédérale de Lausanne, 1998.

[D697Apr00] ITU-T (USA), "Work on the automatic switched optical network", Delayed contribution D.697 (WP3/15).

[EUR709Apr99] EURESCOM Project P709, "Planning of Full Optical Network", http://www.eurescom.de/

[GRMar00] Ornan Gestel and Rajiv Ramaswami, "Optical Layer Survivability: A Services Perspective", IEEE Communications Magazine, March 2000.

[G841Jul95] ITU G.841, "Types and Characteristics of SDH Network Protection Architectures", July 1995.

[HBMar99] Alex L.G. Hayzelden, John Bigham, "Software Agents for Future Communication Systems", Springer-Verlag Berlin Heidelberg 1999.

[LRDC+Oct00] Jingming Lisalina, Daniel Rossier, Manuel Dinis, Laurie Cuthbert, Laurissa Tokarchuk & John Bigham, "Agent-based resource management for 3G networks", Mobile Communications Summit, Galway, Ireland, 1-4 October 2000.

[M3100May96] ITU M.3100, "Principles for a Telecommunications management network", May 1996.

[NBJan99] G. Newsome and P. Bonenfant, "A Proposal for Providing Channel-Associated Optical Channel Overhead in the OTN", ANSI T1X1.5/99-002, Jan 1999; available at http://www.t1.org/index/0816.htm

[RSDec99] D. Rossier-Ramuz, R. Scheurer, "An Introduction to Optical Agents: Intelligent and Mobile Agents for WDM Optical Network Management", in Proceedings of IMPACT'99, Impact of Agent Technology on Telecommunications, Seattle, USA, 2-3 December 1999, pp. 131-139.

[ZJMJan00] Hui Zang, Jason P. Jue, Biswanath Mukherjee, "A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks", Optical Networks Magazine, January 2000.

[ZZ1998] Dianlong Zhang, Werner Zorn, "Developing network management applications in an application-oriented way using mobile agent", Computer Networks and ISDN Systems 30 (1998), pp. 1551-1557.