Automated Management of IP Networks Through Policy and Mobile Agents

Kun Yang[1], Alex Galis[1], Telma Mota[2], Stelios Gouveris[3]

[1] University College London, Department of Electronic and Electrical Engineering, Torrington Place, London WC1E 7JE, UK.
Email: {kyang | agalis}@ee.ucl.ac.uk
[2] Portugal Telecomm Inovacao, SA. Rua Eng. José Ferreira Pinto Basto 3810-106 AVEIRO, Portugal.
Email: telma@ptinovacao.pt
[3] University of Surrey, Centre for Communication Systems Research, Guildford Surrey GU2 7XH UK.
Email: s.gouveris@eim.surrey.ac.uk

Abstract. With the magnificent expansion of network, both in the types of network elements and the software components to manage them, driven by the increasing requirement of different services, it is getting more imperative to seek a means to deploy the network management tasks and services in a fast, ubiquitous and automated way. Mobile agent technology (MAT) provides a promising means to achieve this goal with more flexibility and automation of managing network than those traditional client/server based distributed methods, such as CORBA. Mobile agents, as an enabling technology, can easily represent one of the roles involved in the network management; therefore have great potential to be widely used in network management. This paper proposes to use Policy-based Network Management (PBNM) as an application for MAT to facilitate network management products' development. PBNM, as a newly introduced but widely welcomed technology in the Internet world, can take over the overall management of hybrid network whereas MAT enables the flexible implementation of PBNM system. On the other hand, the agents usually have intelligence, which can be well guided by established policies from PBNM, which makes MAT and PBNM perfectly matched to each other. The work presented in this paper has been developed in the framework of the Europe Union (EU) sponsored IST Project MANTRIP. A commercially oriented test-bed, which is fully based on mobile agent technology, has been set up, and a scenario for solving a practical network management challenge, i.e., inter-domain IP Virtual Private Network, is implemented on this test-bed, which predicts a very promising commercial use of mobile agent in real world. Moreover, the policy-based network management system presented in this paper also covers some of the network management issues under investigation in the EU IST CONTEXT project. This policy and MAT based network management system intends to provide a ubiquitous network management system regardless of the underlying network resources, either wired network elements as the main scope of MANTRIP project or wireless network elements as the main stream of CONTEXT project.

1 Introduction

With the rapid expansion of networks, both in the types of network elements and the software components to manage them, driven by the increasing requirement of different services, it is getting more imperative to seek a means that can deploy network management tasks in a fast, ubiquitous and automated way. A great deal of effort has been made, among which, CORBA and COPS (Common Open Policy Services) are widely accepted and are currently used in some of commercial products. But all of these solutions are based on traditionally client/server model therefore, at least theoretically, lack flexibility and have lower performance. Whereas mobile agent technology (MAT), typical representative of mobile code technology, provides a more promising means to achieve this goal than these client/server based distributed methods.

The mobile agent paradigm [1,2] intends to bring an increased performance and flexibility to distributed systems by promoting "autonomous code migration" (mobile code moving between places) instead of traditional RPC (remote procedure call). With code migration, the actual code or script moves from place to place and executes locally, achieving lower latency, little need for remote interactions and highly flexible control. Mobile agents can be effectively used in telecomm and network management as depicted in [3], as they can take over the burden of the complex interaction mechanisms between different network players, such as negotiations or new service injection. Mobile agents can easily represent one of the roles involved in the network management, such as service provider, connectivity provider, resource or end-user, and act on their behalf, based on established policies.

Mobile agents can have certain extent of intelligence to reasonably respond to the possible change in destination elements and perform negotiation. This kind of intelligence should reflect the management strategy of administrator. A straightforward way for network administrator to give network management command or guide is to produce high-level rules such as *if user is john and time is between 9am and 11am then set up VPN between routers jorg and prowl*. Then mobile agent can take this rule and enforce it automatically. By using rules to give network management command or strategy, a unique but ubiquitous method of managing network can be guaranteed. This idea is exactly what *Policy-based Network Management* (*PBNM*) is about since PBNM allows network operators to express business goals as a set of rules, or policies, which are then enforced throughout the network.

PBNM technology is very suitable for setting up the overall management architecture for large-scaled networks [4]. In comparison with previous traditional network management approaches such as TMN (Telecommunications Management Network) or TINA-C (Telecommunications Information Networking Architecture Consortium), PBNM focuses on users and applications rather than devices and interfaces, which leads to a holistic management of network [5]. Nevertheless, even though policies can be enforced in a distributed fashion, the definition of such policies has to be done and stored centrally. Moreover, according to the policy framework, policies are defined or modified by an administrative tool and the intervention of human is always required. These features of current PBNM system confine its wider

and ubiquitous application in some extent. MAT can resolve many of the problems inherent in current PBNM technology thanks to its mobility and intelligence.

The work presented in the paper has been developed in the framework of EU IST Project MANTRIP "MANagement Testing & Reconfiguration of IP based networks using mobile software agents", whose main objective is to provide novel IP network management applications using mobile agent technology [6]. A commercially oriented test-bed, which is fully based on mobile agent technology, has been set up in a nationwide telecomm and network provider, Portugal Telecomm, one of the MANTRIP partners, to evaluate the commercial use of mobile agent in real world.

The paper is organized as follows. Section 1, this section, described the existing challenge of IP network management and proposed to introduce mobile agent technology, together with PBNM, to cope with this challenge from the real commercial use's point of view. Section 2 presents the fully MAT-supported IP network management architecture designed by MANTRIP. Section 3 details the design and implementation of a generic network management architecture that are fundamentally based on policy management and technically enabled by mobile agents. The features covered in this management architecture are further integrated and verified in a practical IP network management scenario, inter-domain IP VPN (Virtual Private Network) configuration, which contributes to Section 4. Finally, Section 5 concludes this paper.

2 MANTRIP Mobile Agent Platform and Overall Network Management Architecture

The major objective of the MANTRIP project resides in providing a set of novel management applications for managing IP based networks [6]. Those applications are based on bringing management intelligence to the managed resources through *Mobile Agent Technology (MAT*). The three basic network management applications that have been developed within this project are the following:

- *Access Network Management Application*
- *QoS Configuration and Auditing Application*
- *Validation and Monitoring of Network Elements and Mobile Agents Application*

Mobile agents carry out all above specified network management applications functions. This paper aims to present part of the work done in the QoS Configuration and Auditing Application, which are fully based on the MANTRIP mobile agent platform.

2.1 Mobile Agent Platform - Grasshopper

Since its inception in 1990s, mobile agent has attracted enormous attention from industry and institutes, which leads to a long list of mobile agent platforms developed, either for academic usage or commercial purposes [7]. Among these, Grasshopper [8] is most popular and is adopted in this paper.

Grasshopper is a mobile agent development and runtime platform that is built on top of a distributed processing environment. Grasshopper has been designed in conformance with the Object Management Group's Mobile Agent System Interoperability Facility (*MASIF*) [9]. Furthermore, it is a commercial product with extensive documentation and future development under way, therefore is more suitable for commercially oriented network management. But it also provides the version for non-profitable use. Some of the main terminologies used in Grasshopper are as follows:

Place: provides a logical grouping of functionality inside an Agency. *Agency*: is the actual runtime environment for mobile and stationary agents. At least one agency must run on each host that shall be able to support the execution of agents. *Region*: facilitates the management of agencies and agents by providing directory-like region registry. Region is not mandatory for a MA platform.

Along with these elements there is also the concept of agent, which can be further categorized into mobile agent and stationary agent. Mobile agents can migrate autonomously between different locations whilst stationary agents reside permanently in their creation agency, offering services to other agents and possibly encapsulating non-agent based entities, i.e., serving as wrapper.

2.2 Mobile Agent based Network Management Architecture

This paper aims to present the work done in the QoS Configuration and Auditing Application, which architecture is depicted in Fig. 1, following the overall MANTRIP Network Management System (NMS) architecture, although only the components and resources used for QoS and IP VPN are shown.

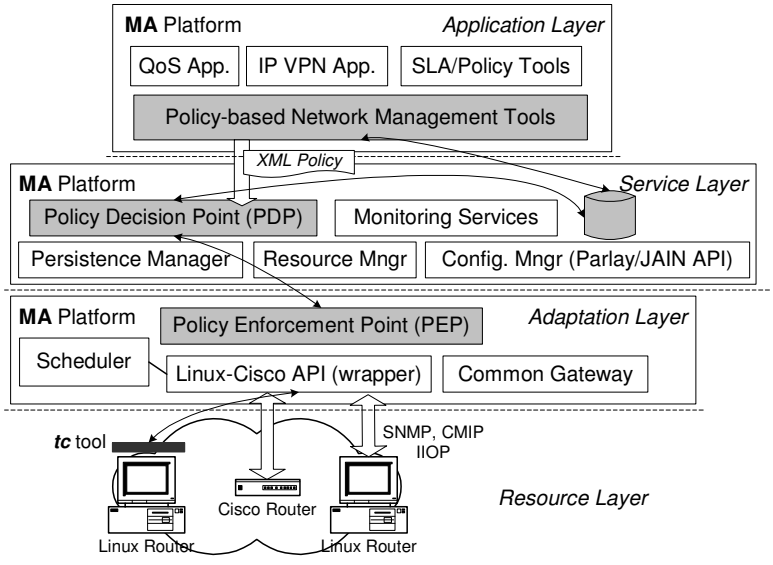

Fig. 1. Policy and MA based MANTRIP NMS Architecture

The MANTRIP NMS has four layers as follows:

- **Application layer**: includes the MANTRIP management user applications.
- **Service layer**: contains the MANTRIP management services (e.g. Parlay/JAIN API) that may be used by either the MANTRIP applications or some other third party applications. These services have been developed on the top of a mobile agent platform.
- **Adaptation layer**: is responsible for hiding the protocol details from the service layer. It contains the protocol adapters and/or the resource wrappers.
- **Resource layer:** contains the managed/controlled MANTRIP resources.

As shown in Fig. 1, except resource layer, which is about the controlled elements themselves, every layer is based on mobile agent platform. All the components depicted in the architecture are in the form of agent, either stationary agents or mobile agents, depending on their functionalities. The components of PBNM system spread in different layers and contribute the core of this management architecture.

It is time-consuming and error-prone for network administrator or resource manager/broker to configure his system manually. And it is extremely hard for him to configure his local resource while considering other domains in the whole network system. PBNM relieves administrator from this by allowing administrator just to give English-like policies at end-to-end application level without caring about the implementation in network level. Mobile agents, guided by these policies, will travel across networks to fulfil policies with the assistance of stationary agents. By doing in this way, the overall management of whole IP network can be achieved with more flexibility and automation. The next section will describe a PBNM architecture implemented in MANTRIP that shows how the integration of mobile agent technology and PBNM could be used to overcome many management problems inherent in traditional management approaches.

3 PBNM System Architecture enabled by Mobile Agent Technology

A policy-based network management system architecture designed and implemented for MANTRIP network management system, together with its components, are shown in Fig. 2, which is fully in line with the PBNM system architecture outline proposed by IETF [10] but with detailed design and MAT-based implementation.

3.1 Policy Tools and Mobile Agent based Policy Transport

Two levels of policy tools are provided, namely user-level and domain-level. User-level policy tool enables network administrator to input or edit policies directly whereas domain-level policy tool provides mechanisms to receive policies transported from other management stations. This reflects the hierarchical structure of policies. To simplify using the system, *Policy Editor GUI* creates and displays policies at a high level of abstraction by using English-like commands and in a visualised way. This policy tool also enables network administrator to group users according to their

characteristics, and classify routers as backbone or edge routers. This policy tool also translates the policies created in the editor GUI into XML-based entries that match predefined schemas for storage within the policy repository. The extension of policy core information model (PCIM) [11] defined by the IETF Policy working group [10], in the form of XML schema, expresses the syntax of XML-based policy. This ensures the interoperability of this PBNM system with other PBNM systems. Alerts should be issued notifying other parts of the system the coming or change of the policy.

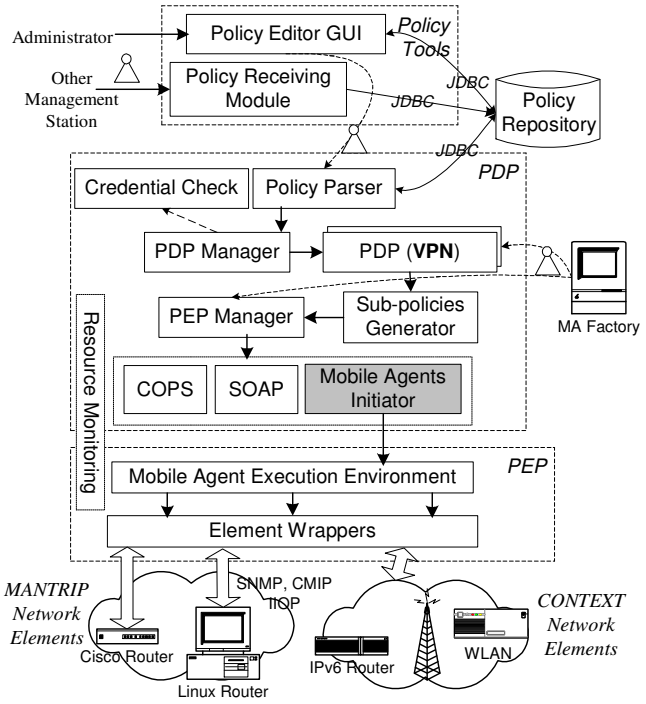

Fig. 2. PBNM Architecture enabled by Mobile Agents

Policy Receiving Module is implemented as a stationary agent to receive XML-based policies transported by mobile agent and to store the policy into policy repository. These received policies are given by upper or peer management station.

3.2 Policy Repository Components

The policy repository is used for the storage of policies, after they have been defined and validated by the policy management tool. The general framework of IETF does not require a specific implementation for the policy repository, or the repository access protocol. In our work, SQL Relational database management system, *PostgreSQL*, is used for policy database, which is connected to Policy Tools and Policy Decision Point (PDP) via JDBC.

3.3 Mobile Agent based Policy Decision Point (PDP)

PDP is the component that retrieves policies from repository, parses them thus evaluates them and eventually sends the necessary commands to the policy target. Additionally, the PDP performs a local conflict check, checking only those devices that are controlled by the specific PDP. The PDP also checks if the resources needed for a specific policy are available in all the controlled devices.

The main role of *PDP manager* is to co-ordinate the different PDPs to support integrated scenarios, and resolve possible conflict. PDP manager can also dynamically download PDP code according to the availability of the code. PDP manager also serves as the coordinator of PDP, Policy Parser and Credential Check Module. It uses Policy Parser to read policy from policy repository and to parse policy with the help of XML parser, and then it calls Credential Check Module to check the validity of policy user using the user and security data stored in the policy repository. The existence of PDP manager makes the whole policy management middleware extensible to contain other future PDPs.

The *Credential Check* module is in charge of checking the privileges for services granted to any actor. Each actor that asks for the use of network resources should also submit a credential. The Credential Check Component then takes this credential and looks in the policy repository for a meta-policy related with that credential to check if the intended management actions (policies) are available to the actor that presented the credential. Finally, if the credential is correct, i.e., the actor has the corresponding privileges; these policies are passed to PDP, e.g., QoS PDP or VPN PDP.

PDP Module together with *Sub-policies Generator* can translate inter-domain policy into sub-domain level policies, with the information from monitoring service. After receiving the policies in XML file, which also has passed the credential check, the PDP Module checks if the policy needs to be applied within multiple domains. If yes, it extracts from the XML file the information needed for sub-domain level network configuration and passes them to the Sub-policies Generator, who maintains domain information such as location, element types and interfaces, to generate the domain-specific sub-policies. Then, PDP Module decides when this policy should be applied by looking at the conditions of the policy thus deciding whether it needs any information to make a decision. If so, it will ask Monitoring Service to register the condition to be monitored. Otherwise, it asks the resource Monitoring Service if there are enough resources or if it is the proper time to apply this policy. If the answer is positive, the policy will be passed to PEP Manager Module to be fulfilled. All the policies are based on fixed schema as defined by PCIM, so they are understandable by different levels.

The *Resource Monitoring* service module receives the registration of resource monitoring according to the requirement of policies and make sure that all the resources registered can be monitored. If the necessary metering code (daemon) is not currently instantiated, the resource monitoring service module will try to make a query to a specific resource monitoring code base so that the corresponding monitoring daemon code, in the form of mobile agent, can be downloaded and run itself. Monitoring Service component just enquiries the Resource Monitoring Daemon to get the necessary information. Resource monitoring functionality also exists in PEP to monitor the enforcement result of the policy.

According to the given policy, *PEP Manager* can use more than one protocol to communicate policy information to PEP, typical examples of which include SNMP (Simple Network Management Protocol), SOAP (Simple Object Access Protocol) [12] and COPS [13]. All of these mechanisms are based on traditional client/server mode and lack flexibility and automation compared to mobile agent technology in a general basis. In our system, mobile agent takes the responsibility of communication between PDP and PEP. The intelligence of mobile agent also decreases the complexity of PDP by automatic adapting to the change of network elements. This also minimizes the message passing between PDP and PEP.

Then *Mobile Agent Initiator* can automatically initiate mobile agents with the corresponding policy given by PEP manager. Mobile agents then migrate themselves to the specific PEPs to enforce the policy.

3.4 MAT based Policy Enforcement Point (PEP)

The policy target is the managed device, where the policy is finally enforced. All PEPs are implemented in the form of stationary agents waiting for the communication with mobile agents coming from PDPs. In order for mobile agents to communicate with different controlled elements, such as Linux routers, Cisco Routers or other computing resources, the corresponding element wrapper functionalities are also provided by PEP stationary agents.

As long as the corresponding policies and element wrappers for wireless network are given, this architecture can very happily adapt to the management of converged networks covering both IPv6 and WLAN (Wireless Local Area Networks) within the scope of another EU IST project CONTEXT, as shown in Fig. 2.

4 Case Study: Inter-domain IP VPN Provisioning using MANTRIP Management Architecture

Based on the policy and mobile agent based network management architecture given above, this section presents a case study to evaluate this architecture, i.e., inter-domain IP VPN provisioning guided by policies and fulfilled by mobile agents. Inter-domain communication is also a challenging research field in network management. This paper provides, as a case study, a solution towards inter-domain communication by introducing the integration of mobile agent technology and policy-based network management technology. Mobile agent plays a very important role since the most essential components in PBNM, such as PDP and PEP, are in the form of mobile agents therefore can move themselves to the required place dynamically and begin working with guidance from policies. Other non-movable components in PBNM architecture, such as policy receiving module, are in the form of stationary agents waiting for the communication with coming mobile agents. Mobile agents are also responsible for transporting XML-based policy across multiple domains.

This scenario has been implemented in the test-bed provided in Portugal Telecomm with its own products inside, aiming to enable full use of mobile agent

technology in real commercial world, as one of important motivation of MANTRIP project.

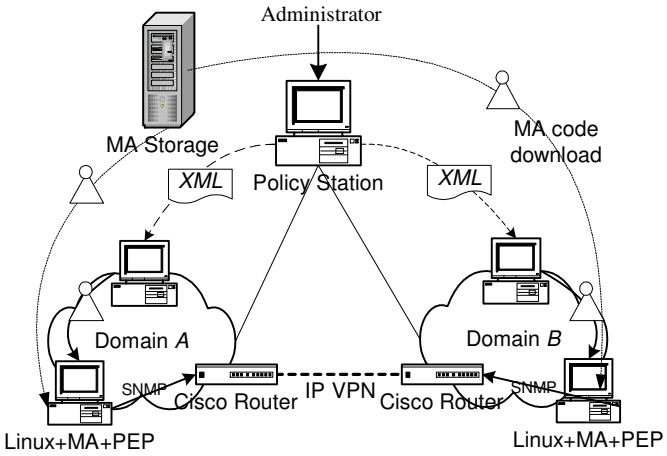

Fig. 3. Inter-domain IP VPN using MA-enabled PBNM

The whole scenario is depicted in Fig. 3. Network administrator uses Policy Management Station to manage the underlying network environment (including two domains with one physical router and one Linux machine next to Cisco router at each domain) by giving policies, which are further translated into XML files and transported to relevant sub-domain PBNM stations using mobile agents. In this scenario, two mobile agents are generated at the same time, each going to one domain. Let's take one mobile agent for example. After the mobile agent arrives at the sub-domain management station, the mobile agent communicates with the stationary agent waiting at the sub-domain management station. Based on this policy, the sub-domain PDP manager can download the proper PDP, which is in the form of mobile agent, to make the policy decision. After this, the selected or/and generated policies are handed to PEP manager, which, also sitting on the sub-domain PBNM station, requires the availability of PEP code, e.g., for new IP tunnel configuring, according to the requirement given in XML file. The PEP, also in the form of mobile agent, moves itself to the Linux machine, on which it uses SNMP (Simple Network Management Protocol) to configure the physical router so as to set up one end of IP VPN tunnel. Same process happened at the other domain to bring up the other end of IP VPN tunnel.

5 Conclusions

As shown in the above case study, after administrator provides the input requirements, the entire management procedure processed automatically. Administrator doesn't need to know or analyse the specific sub-domain information. The whole system scales automatically to the dynamics of the application requirement thanks to the inherent mobility of mobile agent and its intelligence empowered by

policies. The network management system presented in this paper, are applicable to other network systems, such as these in the CONTEXT project, as long as the corresponding policies and element wrappers are specified and developed.

MAT allows the dynamically enhancement of the management architecture, the introduction of new application or device specific policies, tailored to realize complex tasks, and the automation of the network management tasks. The combination of PBNM and MAT enables the achievement of many advantages, such as, the automated and rapid deployment of new services, the customisation of existing service features, the scalability and cost reduction in network and service management. All these mean a ubiquitous network management architecture that will further promote the appearance of new services and business opportunities.

Acknowledgements

This paper describes part of the work undertaken in the context of the EU projects MANTRIP (IST-10921) and CONTEXT (IST-38142). The IST programme is partially funded by the Commission of the European Union.

References

1. Galis, A., Griffin, D., Eaves, W., et al.: Mobile Intelligent Agents in Active Virtual Pipes: Support for Virtual Enterprises. In: Magedanz, T., et al. (eds.): On The Way To Information Society. IOS Press, Amsterdam, Netherlands, April 2000. pp. 427-450
2. Yang, K., Galis, A., Mota, T., and Michalas, A.: Mobile Agent Security Facilities for Safe Configuration of IP Network. In: Fischer, K., Hutter D. (eds.): Proceedings of the 2nd International Workshop on Security in Mobile Multi-agent Systems (SEMAS2002), Bologna, Italy, July 2002. http://www.dfki.de/~kuf/semas/semas-2002/
3. Glitho, R.H., Magedanz, T., eds: IEEE Network, Special Issue on Applicability of Mobile Agents to Telecommunications, Vol. 16, No. 3, May/June 2002.
4. Sloman, M., Lupu, E.: Security and Management Policy Specification. IEEE Networks, Vol 16, No. 2., April 2002.
5. D. Kosiur. Understanding Policy-based Networking. John Wiley & Sons, Inc. 2001.
6. MANTRIP project website: http://www.solinet.com/mantrip, July 2002.
7. Mobile agent system list: http://mole.informatik.uni-stuttgart.de/mal/mal.html
8. Grasshopper http://www.grasshopper.de, 2002
9. Milojicic, D. et al.: MASIF: The OMG mobile agent system interoperability facility. In: Proceedings of 2nd Int. Workshop on Mobile Agents. Springer-Verlag, Lecture Notes in Computer Science, vol. 1477, Sept. 1998.
10. IETF Policy Working Group website: http://www.ietf.org/html.charters/policy-charter.html, 2002
11. IETF Policy Core Information Model Extensions on web: http://www.ietf.org/internet-drafts/draft-ietf-policy-pcim-ext-08.txt, May 2002.
12. Simple Object Access Protocol (SOAP) on W3C website: http://www.w3.org/TR/SOAP/, 2002.
13. IETF COPS (Common Open Policy Services) draft on RAP working group website: http://www.ietf.org/internet-drafts/draft-ietf-rap-cops-frwk-01.txt, June 2002.