Rule-driven Mobile Intelligent Agents for Real-time Configuration of IP Networks

Kun Yang, Alex Galis

University College London, Department of Electronic and Electrical Engineering,
Torrington Place, London, WC1E 7JE, UK
{kyang, agalis}@ee.ucl.ac.uk

Abstract. Even though intelligent agent has proven itself to be a promising branch of artificial intelligence (AI), its mobility capacity has yet been paid enough attention to match the pervasive trend of networks. This paper proposes to inject intelligence into mobile agent of current literature by introducing rule-driven mobile agent so as to maintain both intelligence and mobility of current agent. Particularly, this methodology is fully exemplified in the context of real-time IP network configuration through intelligent mobile agent based network management architecture, policy specification language and policy information model. A case study for inter-domain IP VPN configuration demonstrates the design and implementation of this management system based on the test-bed developed in the context of European Union IST Project CONTEXT.

1 Background and Rationale

After years of recession, Artificial Intelligence (AI) regained it vitality relatively thanks to the inception of *Intelligent Agent* (IA). Agent was even highlighted as another approach of AI by S. Russell *et al.* [1]. Intelligent agent usually is a kind of software of autonomous, intelligent and social capability. Intelligent Agent and its related areas have been intensively researched over last decades and enormous achievement covering a wide range of research fields are available in the literature. As computers and networks become more pervasive, the requirement of intelligent agent being more (automatically) moveable is getting more a necessity than an option.

As an active branch of agent technology researches, mobile agent paradigm 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) such as CORBA, COPS (Common Open Policy Service) [2]. It turns out that more attention has been given to the mobility of mobile agent whereas the intelligence of mobile agent is seldom talked about in the mobile agent research community. Mobile agent technology is very successfully used in the network-related applications, especially network management, where its mobility feature is largely explored [3], but these mobile agents are usually lack of intelligence. We believe mobile agent is first of all an agent that has intelligence.

This paper aims to explore the potential use of mobile agent to manage IP network in a more intelligent and automated way. For this purpose, mobile agents should contain 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 sourceHost is within finance and time is between 9am and 5pm then useSecureTunnel*. Then mobile agent can take this rule and enforce it automatically. By using rules to give network management command or strategy, a unique method of managing network can be guaranteed. The use of rule to management network is exactly what so called *Policy-based Network Management* (*PBNM*) [4] is about since policies usually appear as rules for network management. Here in this paper, we don't distinguish the difference between rule-based management and policy-based management and in many cases, the term "policy-based" is more likely to be used.

In order to put this idea into practice, a specific network management task is selected, i.e., IP VPN (Virtual Private Network) configuration. VPN enables an organization to interconnect its distributed sites over a public network with much lower price than the traditional leased-line private network. VPN is a key and typical network application operating in every big telecom operator as a main revenue source. But the lack of real-time and automated configuration and management capabilities of current IP VPN deployment makes the management of growing networks time-consuming and error-prone. The integration of mobile agents and policy-based network management (as such making a mobile intelligent agent) claims to be a practical solution to this challenge.

This paper first discusses an intelligent mobile agent based IP network management architecture with emphasis on IP VPN; then a detailed explanation with respect to policy specification language and IP VPN policy information model is presented. Finally, before the conclusion, a case study for inter-domain IP VPN configuration is demonstrated, aiming to exemplify the design and implementation of this intelligent MA-based IP network management system.

2 An Intelligent MA-based IP Network Management Architecture

2.1 Architecture Overview

An intelligent MA based IP network management system architecture and its main components are depicted in Fig. 1, which is organized based on the PBNM concept as suggested by IETF Policy Working Group [5]. Please note that we use IP VPN configuration as an example, but this architecture is generic enough for any other IP network management tasks provided that the corresponding PDP and its information model are given.

The PBNM system mainly includes four components: policy management tool, policy repository, Policy Decision Point (PDP) and Policy Enforcement Point (PEP). Policy management tool serves as a policy creation environment for the administrator to define/edit/view policies in an English-like declarative language.

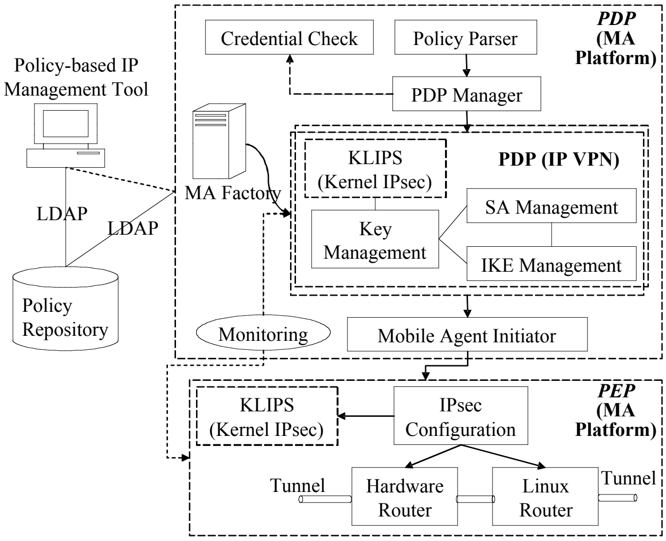

Fig. 1: Intelligent MA-based IP Network Management Architecture

After validation, new or updated policies are translated into a kind of object oriented representation and stored in the policy repository, which is used for the storage of policies in the form of LDAP (Lightweight Directory Access Protocol) directory. Once the new or updated policy is stored, signaling information is sent to the corresponding PDP, which then retrieves the policy by *PDP Manager* via *Policy Parser*. After passing the *Credential Check*, the PDP Manager gets the content of the retrieved policy, upon which it selects the corresponding PDP, in this case, *IP VPN PDP*. After rule-based reasoning on the retrieved policy which may involve in other related policies stored in Policy Repository, PDP decides the action(s) to be taken against the policy. Then corresponding mobile agents that are initiated via *Mobile Agent Initiator* carry the bytecode for the actions and move themselves to the PEP and enforce the policy on PEP. The automation of the whole procedure also depends on a proper policy information model that can translate the rule-based policies to the element level actions. This will be discussed separately in next section. Since there is plenty of work presenting rule-based reasoning in the knowledge engineering field, this paper prefers not to repeat them again. Please note that both PDPs and PEPs are in the form of mobile intelligent agents and intelligence is embedded inside the bytecode itself.

2.2 IP VPN Components

IP VPN operational part can be regarded as a type of PDP since it performs a subnet of policy management functionality. For easy demonstration in Fig. 1, all the VPN functional components are placed into one single PDP box. In actual implementation, they can be separated into different PDPs and be coordinated by a VPN PDP manager.

Our IP VPN implementation is based on FreeS/WAN IPsec [6], which is a Linux implementation of the IPsec (IP security) protocols. Since IP VPN is built up via the Internet which is a shared public network with open transmission protocols, VPNs must include measures for packet encapsulation (tunneling), encryption and authentication so as to avoid the sensitive data from being tampered by any unauthorized third parties during data transit. Three protocols are used: AH (Authentication Header) provides a packet-level authentication service; ESP (Encapsulating Security Payload) provides encryption plus authentication; and finally, IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two. KLIPS (kernel IPsec) from FreeS/WAN has implemented AH, ESP, and packet handling within the kernel [6]. More discussion is given to IKE issues which are closely related to the policies delivered by administrator via policy management tool.

Key Management Component: Encryption usually is the starting point of any VPN solution. These encryption algorithms are well known and widely exist in lots of cryptographic libraries. The following features need to be taken into consideration for key management component: key generation, key length, key lifetime, and key exchange mechanism.

IKE Management: IKE protocol was developed to manage these key exchanges. Using IPSec with the IKE, a system can set up security associations (SAs) that include information on the algorithms for authenticating and encrypting data, the lifetime of the keys employed, the key lengths, etc; and these information are usually extracted from rule-based policies. Each pair of communicating computers will use a specific set of SAs to set up a VPN tunnel. The core of the IKE management is an IKE daemon that sits on the node to which SAs need to be negotiated. IKE daemon is distributed on each node that is to be an endpoint of an IKE-negotiated SA. IKE protocol sets up IPsec connections after negotiating appropriate parameters. This is done by exchanging packets on UDP port 500 between two gateways.

The ability of cohesively *monitoring* all VPN devices is vitally important. It is essential to ensure that policies are being satisfied by determining the level of performance and knowing what in the network is not working properly if there are. The monitoring component drawn in PDP box is actually a monitoring client for enquiring status of VPN devices or links. The real monitoring daemons are located next to the monitored elements and are implemented using different technologies depending on the features of monitored elements.

3 Policy Specification Language and Information Model

Based on the above network management system architecture presented, this section details the design and implementation of this architecture in terms of two critical policy-based management concerns, i.e., policy specification language and policy information model.

A high level policy specification language has been designed and implemented to provide the administrator with the ability of adding and changing policies in the policy repository. Policy takes the following rule-based format:

```
        [PolicyID] IF {condition(s)} THEN {action(s)}
```

It means *action(s)* is/are taken if the *condition(s)* is/are true. Policy condition can be in both disjunctive normal form (DNF, an ORed set of AND conditions) or conjunctive normal form (CNF, and ANDed set of OR conditions). *PolicyID* field defines the name of the policy rule and is also related to the storage of this policy in policy repository.

An example of policy is given below, which forces the SA to specify which packets are to be discarded.

```
    IF (sourceHost == Camden) and (EncryptionAlgorithm ==
3DES) THEN IPsecDiscard
```

This rule-based policy is further represented by XML (eXtensible Mark-up Language) due to XML's built-in syntax check and its portability across the heterogeneous platforms [7]. The schema of the XML file is fully in line with the schema of LDAP-based policy repository as proposed by IETF Policy WG.

An object oriented information model has been designed to represent the IP VPN management policies, based on the IETF PCIM (Policy Core Information Model) [8] and its extensions [9]. The major objective of such information models is to bridge the gap between the human policy administrator who enters the policies and the actual enforcement commands executed at the network elements. IETF has described an IPsec Configuration Policy Model [10], representing IPsec policies that result in configuring network elements to enforce the policies. Our information model extends the IETF IPsec policy model by adding more functionalities sitting at a higher level (network management level).

Fig. 2 depicts a part of the inheritance hierarchy of our information model representing the IP VPN policies. It also indicates its relationships to IETF PCIM and its extensions. Some of the actions are not directly shown due to the space limitation. Please note that apart from the *PolicyAction* and *PolicyCondition* as described above, the IPsec actions such as *IPsecBypassAction* and *IPsecDiscardAction* are also reflected in this policy information model.

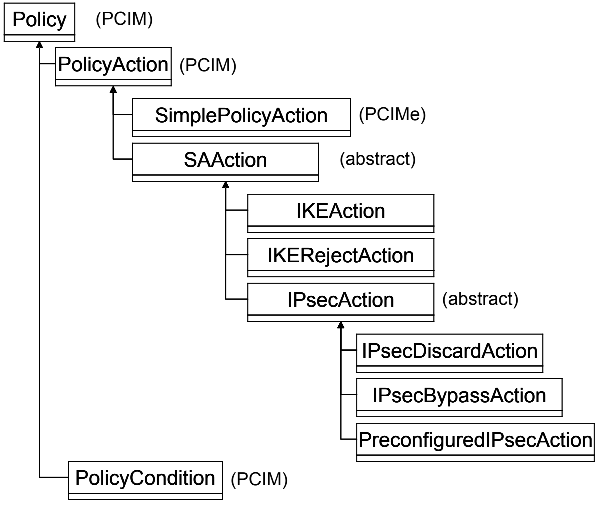

Fig. 2: Class Inheritance Hierarchy of VPN Policy Information Model

4 Case Study: Inter-domain IP VPN

Inter-domain communication is also a challenging research field in network management. This paper provides, as a case study, a solution to inter-domain communication by introducing the mobile intelligent agent. Mobile intelligent agent plays a very important role since the most essential components in PBNM, such as PDP and PEP, are in the form of mobile intelligent agents. 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 intelligent agents are also responsible for transporting XML-based policy across multiple domains. This case study had been implemented within the context of EU IST Project CONTEXT [11].

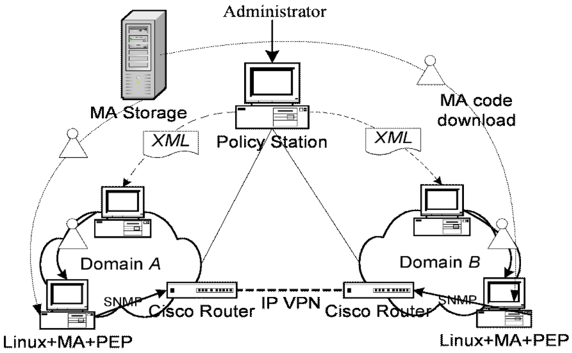

Fig. 3: Inter-domain IP VPN based on Intelligent Mobile Agents

The entire 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 intelligent agents. In this scenario, two mobile intelligent 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 policy. 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 and Future Work

As shown in the above case study, after administrator provided the input requirements, the entire configuration procedure processed automatically. Administrator doesn't need to know or analyse the specific sub-domain information thanks to the mobility and intelligence of mobile agents. The rule-driven mobile agents enable the achievement of many advantages, such as, the automated and rapid deployment of new services, the customisation of existing network features, the scalability and cost reduction in network management.

However, this is just a first step to bring intelligence and mobility of software agent into the field of IP network management. Defining a full range of rules for IP network management and the study of how they can coexist together towards a practical network management solution are the future work. Rule conflict check and resolution mechanisms will also require more work as the number of policies dramatically increases.

Acknowledgements

This paper describes part of the work undertaken in the context of the EU IST project CONTEXT (IST-2001-38142-CONTEXT). The IST programme is partially funded by the Commission of the European Union.

References

1. S. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Prentice-Hall, 1995.
2. K. Yang, A. Galis, T. Mota, and A. Michalas. "Mobile Agent Security Facility for Safe Configuration of IP Networks". *Proc. of 2nd Int. Workshop on Security of Mobile Multi-agent Systems*: 72-77, Bologna, Italy, July 2002.
3. D. Gavalas, D. Greenwood,M. Ghanbari, M. O'Mahony. "An infrastructure for distributed and dynamic network management based on mobile agent technology". *Proc. of Int. Conf. on Communications*: 1362 -1366, 1999.
4. M. Sloman. "Policy Driven Management for Distributed Systems". *Journal of Network & System Management*, 2(4): 333-360, 1994.
5. IETF Policy workgroup web page: http://www.ietf.org/html.charters/policy-charter.html
6. FreeS/WAN website: http://www.freeswan.org/
7. K. Yang, A. Galis, T. Mota and S. Gouveris. "Automated Management of IP Networks through Policy and Mobile agents". *Proc. of Fourth International Workshop on Mobile Agents for Telecommunication Applications (MATA2002)*: 249-258. LNCS-2521, Springer. Barcelona, Spain, October 2002.
8. J. Strassner, E. Ellesson, and B. Moore. "Policy Framework Core Information Model". IETF Policy WG, Internet Draft, May, 1999.
9. B. Moore. "Policy Core Information Model Extensions". IETF-Draft, IETF Policy Working Group. 2002.
10. J. Jason. IPsec Configuration Policy Model. IETF draft.
11. European Union IST Project CONTEXT web site: http://context.upc.es/