# ABSTRACTS-YEAR 2004

## DISSERTATION

## COMPUTER SCIENCE

**Diss CS-04-01**

MOBILE AGENT-BSED SERVICE MIGRATION MANAGEMENT IN VIRTUAL ACTIVE NETWORKS

Mr. Surasak Mungsing
Prof. Ramakoti Sadananda

Service-oriented application is becoming attractive to service providers, particularly in emerging telecommunication networks, via the concept of virtual active network and distributed management by delegation. The concept of virtual active network separates active networks into isolated computing environments so that each customer can provide and manage application specific services to end-users. Management by delegation provides a paradigm for distributed and flexible network management that overcomes the key limitations of current centralized management schemes.

Security is a major concern in both active network and agent-based system. The nature of active networks introduces difficulties in security control of capsules that come to an active node for execution. Each capsule has to be authenticated before execution in order to protect active nodes. Authentication of capsules in active networks is expensive and also presents some difficulties concerning the identification of the principal of the capsules. In a distributed agent environment, though less authentication measures are required but the system may face threats such as misuse of host by mobile agents, misuse of agents by other agents, misuse of agent by host, and misuse by underlying network infrastructure. Active networks that allow customers to migrate or install a service in a virtual active network or migrate a service between virtual active networks in response to the client requirements may cause the network face security threats from malicious customers.

This work addresses the security concerns for service migration between Virtual Active Networks by employing policy enforcement and agent-based security control mechanisms. The frameworks designed for secure service migration in Virtual Active Networks describes architecture of an active node, which includes Security Execution Environment, and secure service management architecture for service migration management in single-provider-domain Virtual Active Networks. The designed security model in this framework employs security mechanisms that comprise Policy Interpretation Agent, Authentication Agent, and Authorization Agent. These agents work cooperatively with the Policy Manager of the network provider domain to protect active nodes. The infrastructure for Virtual Active Network provisioning and management deploys the ANET software whereas service code migration and management runs on the Grasshopper, a FIPA compliant agent platform, on Linux environments. Algorithms for service migration between Virtual Active Networks, and policy interpretation were developed for a general service migration scenario in an active telecommunication network. Authentication Agent deploys the security services supported by the Grasshopper agent platform, which include cryptographic mechanisms and secure communication channel.

The Secure Service Migration Management (SSMM) model has introduced intelligence into active network by applying agent technology into active network infrastructure. The designed SSMM model also illustrated the complementary of two areas of research in computer and communication networking, namely active networks and agent technology. The model is applicable for single-provider-domain Virtual Active Networks but, as future work, can be further developed to support multi-provider-domain Virtual Active Networks. A new component such as domain manager needs to be included, for each service provider, in order to manage resources of different network service providers.

Keyword: virtual active network, agent technology, security, service migration.