A Policy Propagation Model using Mobile Agents in Large-scale Distributed Network Environments

Tae-Kyung Kim, Dong-Young Lee, Ok-Hwan Byeon, Tai M. Chung

Internet Management Technology Laboratory

School of Electrical and Computer Engineering, Sungkyunkwan University

300 Chunchun-dong, Chang-an-gu, Suwon, Kyounggi-do, Korea

Tel: +82-31-290-7222, Fax: +82-31-290-6673

Email: {tkkim, dylee}@rtlab.skku.ac.kr, ohbyeon@kisti.re.kr, tmchung@ece.skku.ac.kr

Contents

- Definition and Characteristics of IDS Models
- Overview of Mobile Agent
- Constitution of Mobile Agent
- Security Issue to a Mobile Agent
- Agent-based IDS
- Design of Rule Propagation System
- Negotiation Procedure of Security Rules
- Comparison of Performance
- Conclusion & Future work

Definition of Characteristics of IDS Models

- Intrusion
  - **Anderson(1980) : Any set of actions that attempt to compromise the integrity, confidentiality, or availability of computing resource via**
    - **Causing Denial of Service**
    - **Creating Backdoor(Trojan Horse)**
    - **Planting Viruses**
    - **Exploiting Software Vulnerability**
- Intrusion Detection System(IDS)
  - **Denning(1987) : A software with the functions of detecting, identifying and responding to unauthorized or abnormal activities on the target system**

Definition of Characteristics of IDS Models

Misuse Detection Model

- Efficient but hard to detect new intrusion patterns
- Possible to draw false negative detection
- Expert System, State Transition Analysis, Key Stroke Monitoring, Model Based Approach, Pattern Matching

Anomaly Detection Model

- High Cost, but capable of detecting unknown intrutions
- Possible to draw false positive detection
- Statistical Approaches, Predictive Pattern Generation, Neural Network

Overview of Mobile Agent

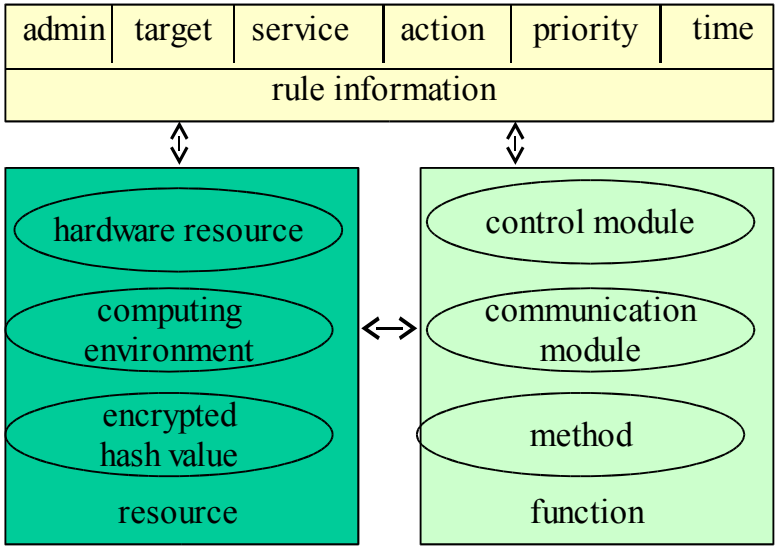
Mobile Agent

- A mobile agent is a kind of independent program, which can migrate from one node to another node in a distributed network by itself.
  - Can make proper use of existing resources so as fulfill user's assignment
  - Can debase network traffic
  - Can balance network load
  - Support fault-tolerance
  - Support mobile user
  - Support customized services

- Life cycle of mobile agent
  - Life cycle including the state of creating, halting, executing, service searching, arriving new host, migrating, returning to the original host and terminating.

Constitution of Mobile Agent

- **A mobile agent consists of three main parts**
  - Resource section
    - Containing hardware resource, computing environment and encrypted hash value
  - Function section
    - Including control module, communication module and method
  - Rule information

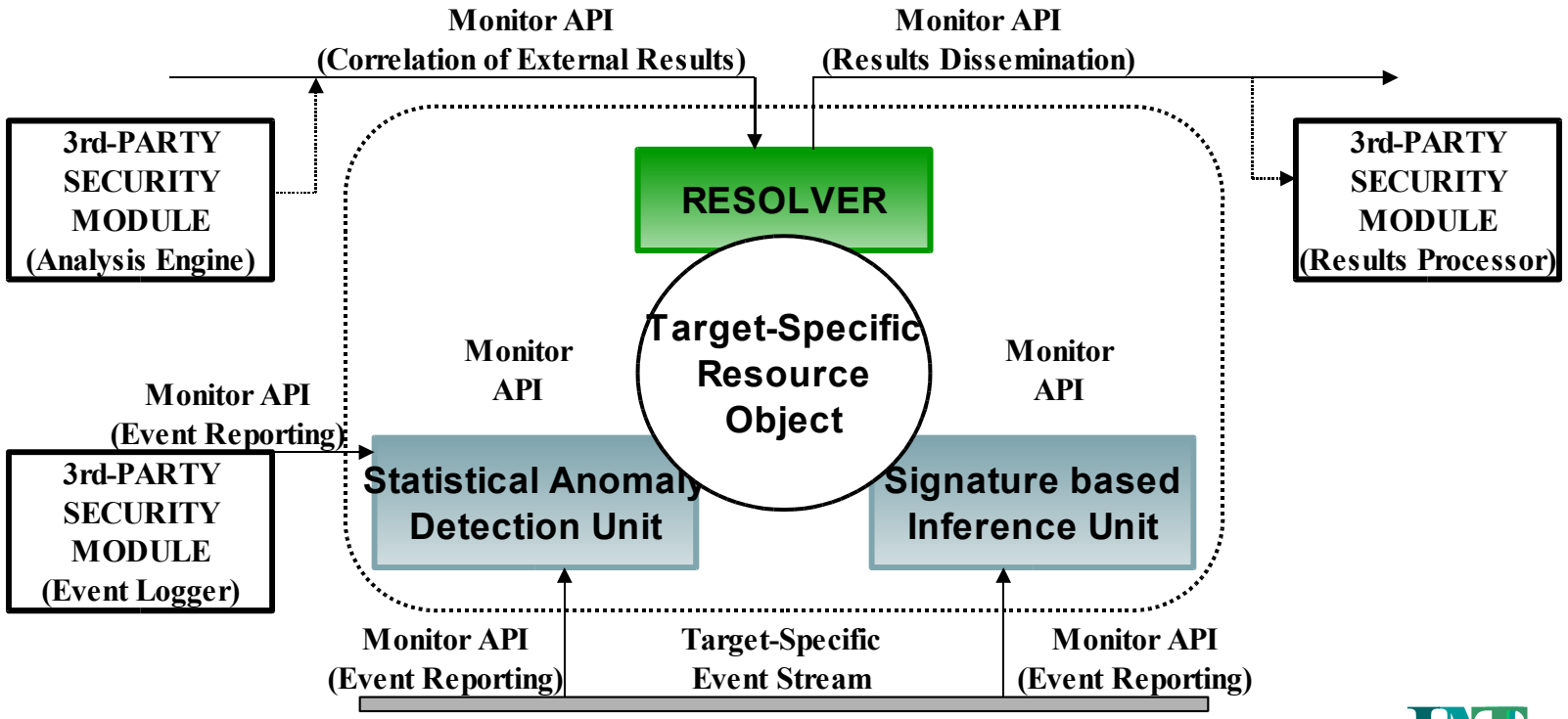


Security Issue to a Mobile Agent

- **Malicious Agent**
  - Protection of the host against agent and protection of other agents
- **Malicious Host**
  - Protection of a agent from the host and protection of network
- **Solution to Malicious Agent and Host**
  - Encrypted hash values guarantee the integrity of the mobile agent and protect unauthorized modification of the mobile agent
  - A trusted third party authenticates a mobile agent using a PKI infrastructure

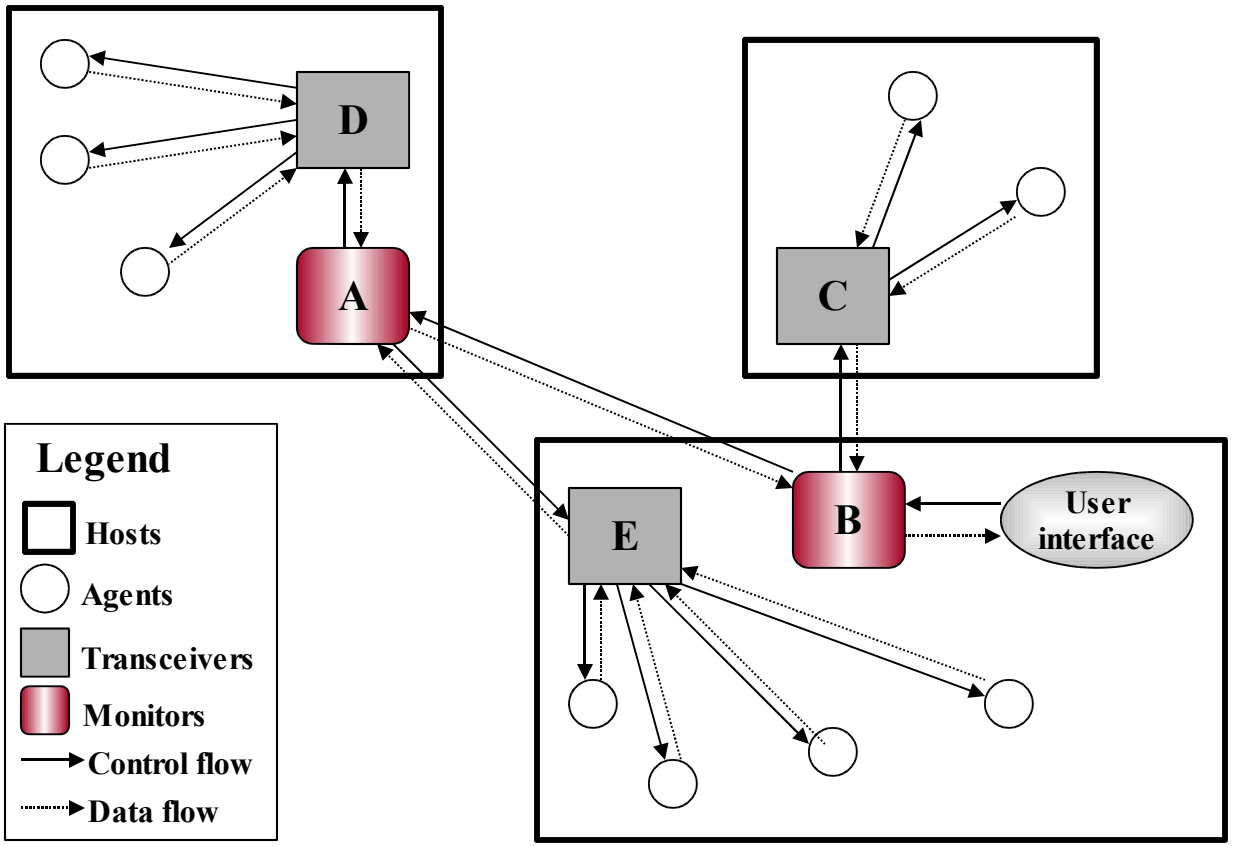
Agent-based IDS (EMERALD : SRI International)

- A scalable surveillance and response architecture for large distributed networks
- Statistical Anomaly Detection & Misuse Detection



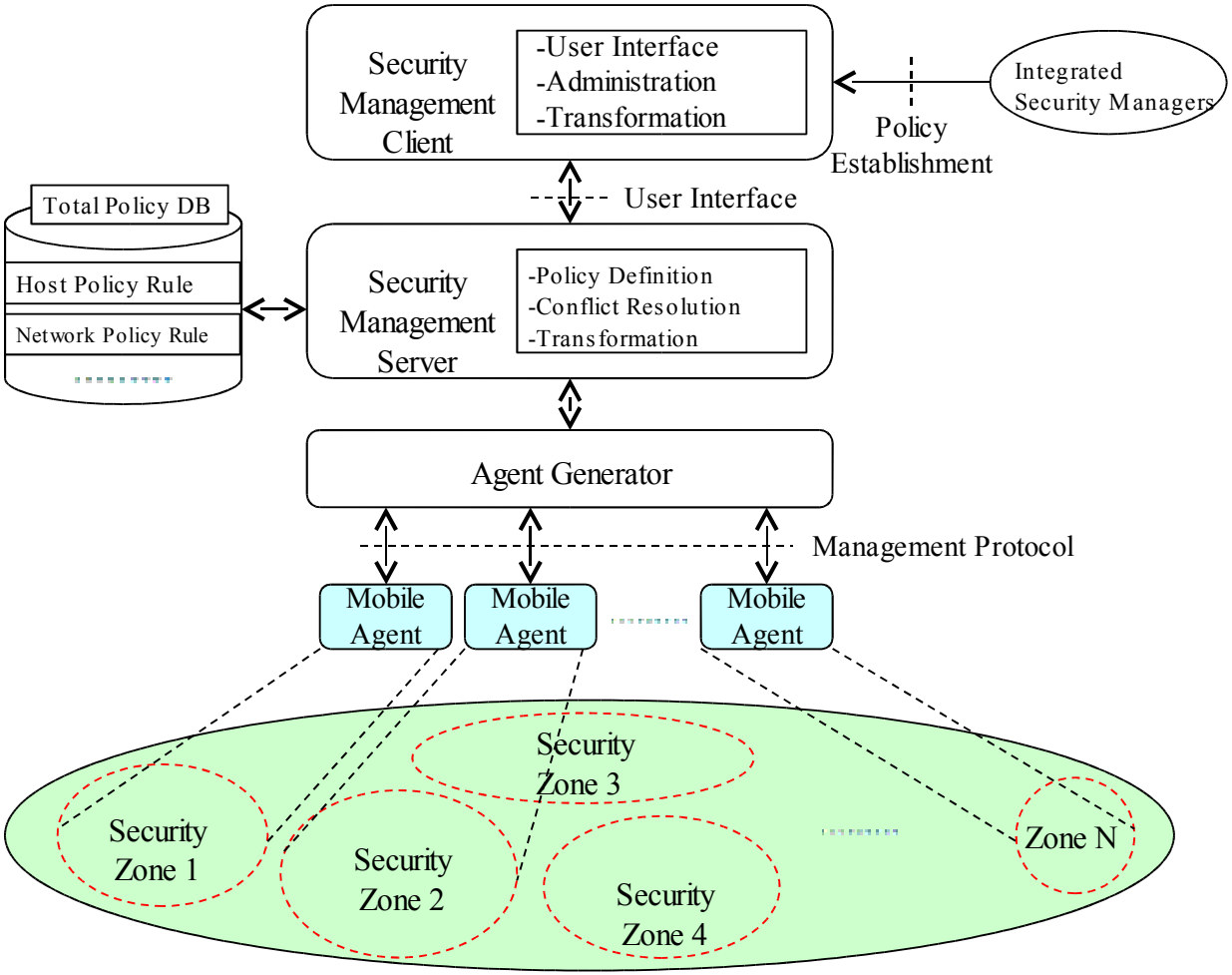
Agent-based IDS (AAFID : COAST Lab.)

- **A Distributed IDS based on Multiple Independent-running Entities (Autonomous Agent)**



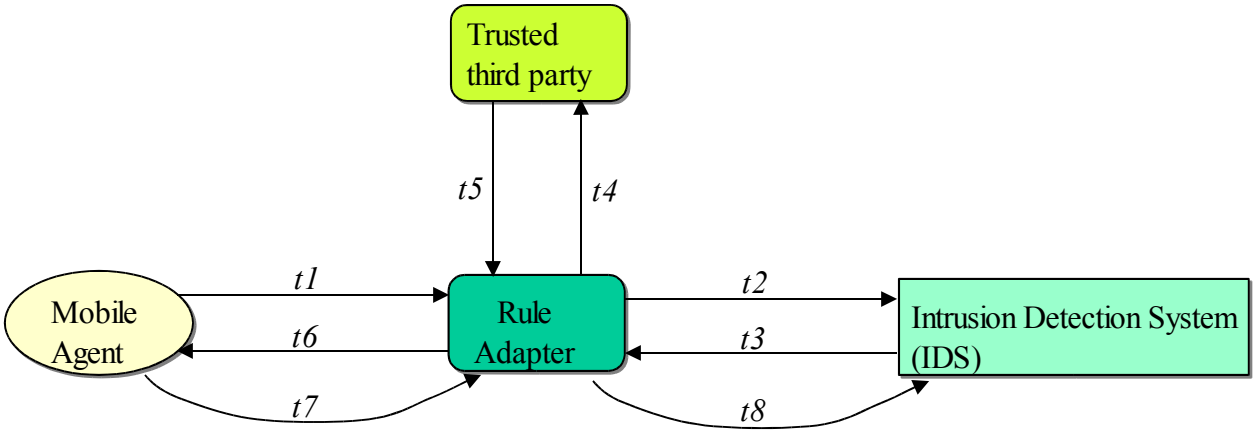
Design of Rule Propagation System

Conceptual Architecture of MARS



Design of Rule Propagation System

Conceptual Architecture of Rule Propagation



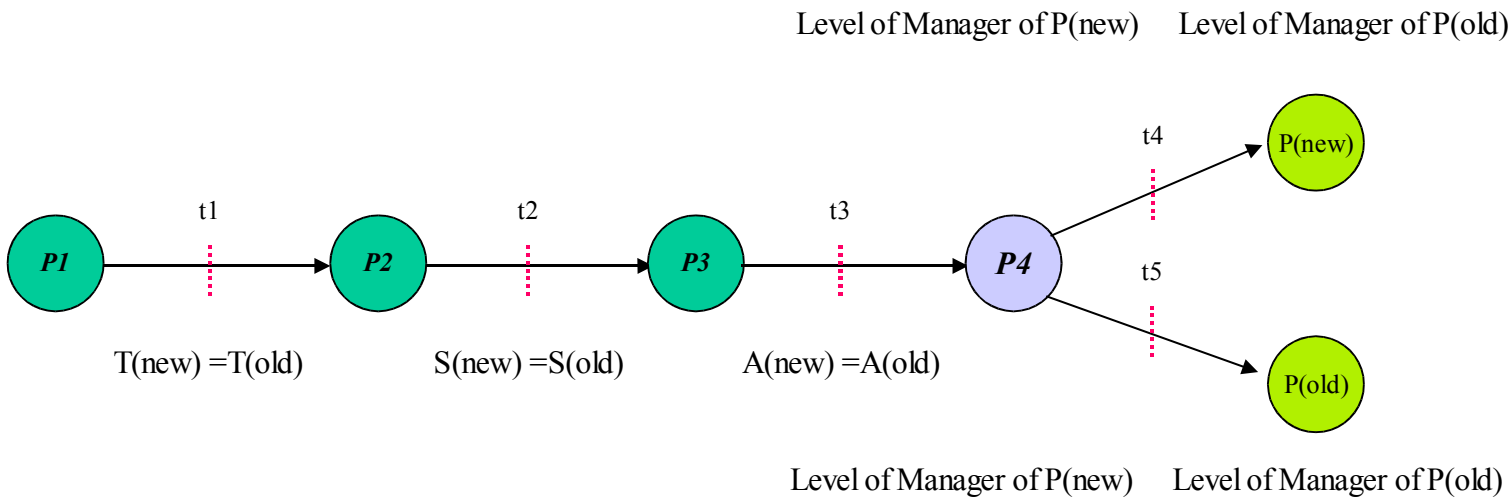
Negotiation Procedure of Security Rules

- **The primary function of the rule adapter is detecting and resolving policy conflicts**
- **The policy of IDS, P(x), is defined by the existing policy(old) and the newly propagated policy(new)**
  - P(x)
    - T(x) : Policy Target
    - S(x) : Policy Service
    - A(x) : Policy Action
    - P(new) = {T(new), S(new), A(new) }
    - P(old) = {T(old), S(old), A(old)}
- **Comparison factors for solving policy conflicts**
  - Level of Manager
  - Priority of security policy
  - Creation time of security policy

Negotiation Procedure of Security Rules

Condition 1 (Equivalence) of policy conflict

- Two policies have the same values of policy target T(x), service S (x) and the action of policy A(x)



P1 : Input P(new)

P2, P3 : No Conflict

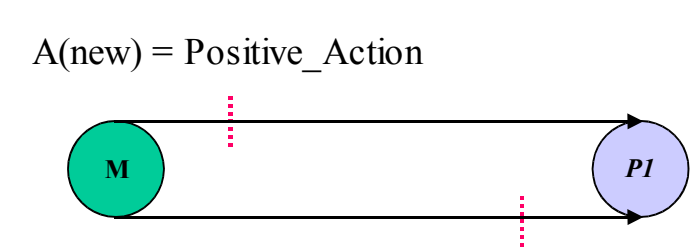
P4 : Policy Conflict Occurred

Negotiation Procedure of Security Rules

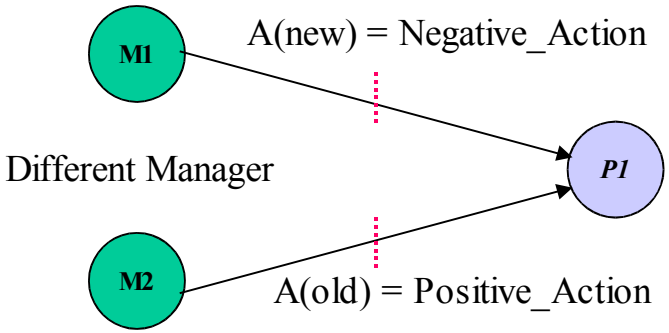
Condition 2 (Contradiction) of policy conflict

- Positive and negative policies exist to the same security zone

T(x): Target	S(x): Service	A(x): Action
T(old) = T(new)	S(old) = S(new)	A(new) = Positive_Action A(old) = Negative_Action
		A(new) = Negative_Action A(old) = Positive_Action



M(new) = M(old), T(new) = T(old), S(new) ↔ S(old)



M(new) ≠ M(old), T(new) = T(old), S(new) ↔ S(old)

Negotiation Procedure of Security Rules

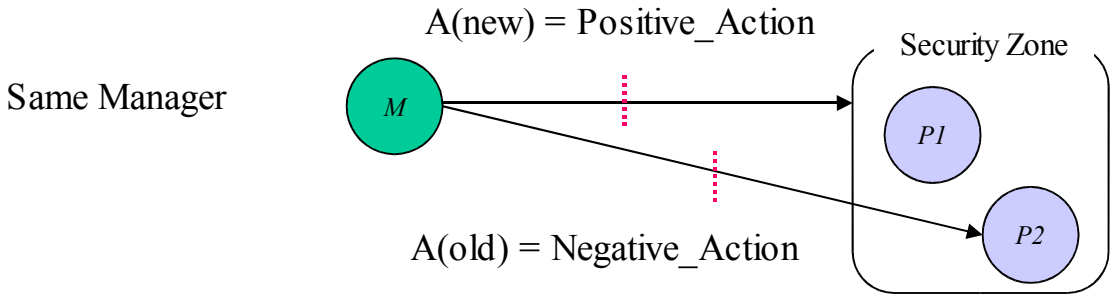
Condition 3 (Inclusion) of policy conflict

- Contradictable inclusive relationship between policy P(old) and policy P(new)

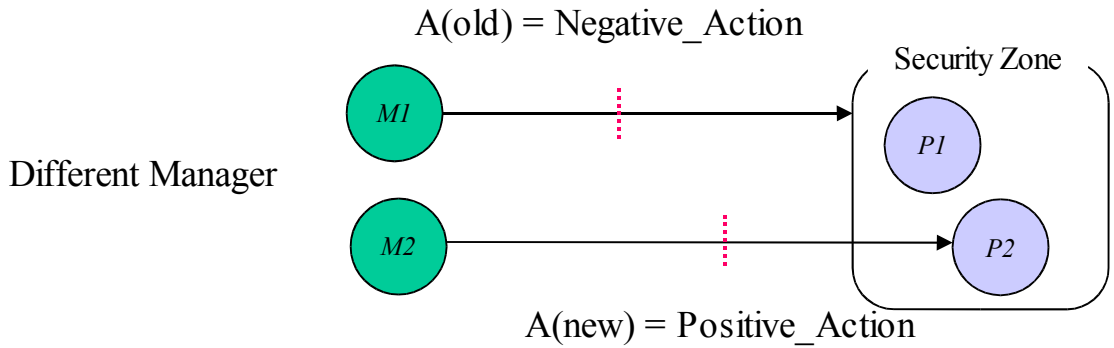
T(x): Target	S(x): Service	A(x): Action
T(old) = T(new)	S(new) S(old)	A(new) = Positive_Action A(old) = Negative_Action
		A(new) = Negative_Action A(old) = Positive_Action
	S(new) S(old)	A(new) = Positive_Action A(old) = Negative_Action
		A(new) = Negative_Action A(old) = Positive_Action

Negotiation Procedure of Security Rules

Condition 3 (Inclusion) of policy conflict



M(new) = M(old), S(new) S(old), A(new) ↔ A(old)

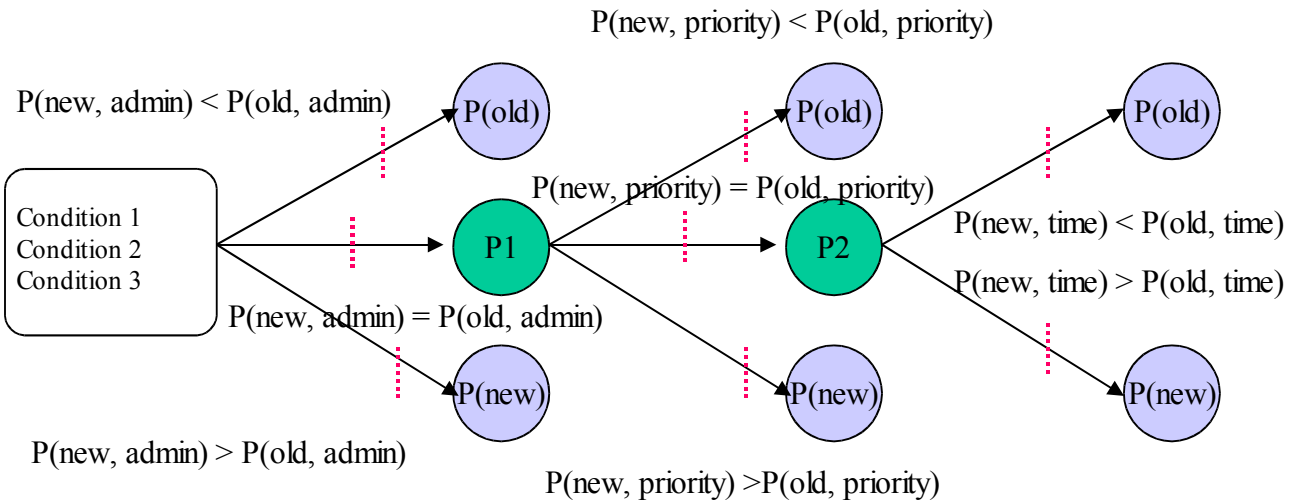


M(new) ≠ M(old), S(new) S(old), A(new) ↔ A(old)

Negotiation Procedure of Security Rules

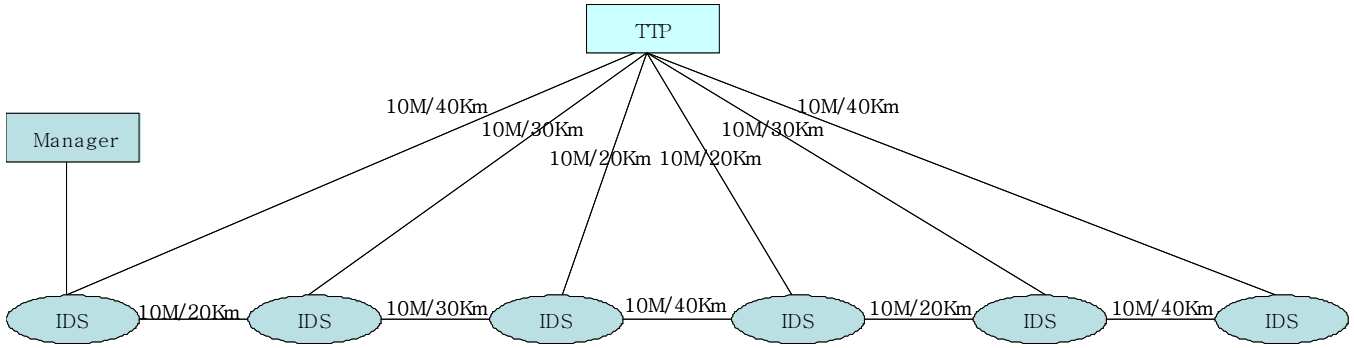
Solution of policy conflict

- Level of admin
- Priority of each policy
- Creation time of policy

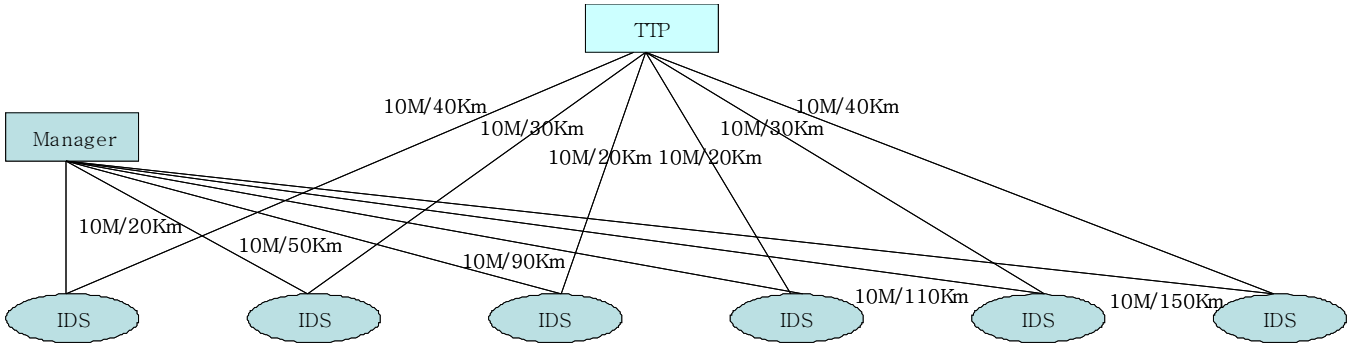


Comparison of Performance

Simulation Topology 1 using NS-2



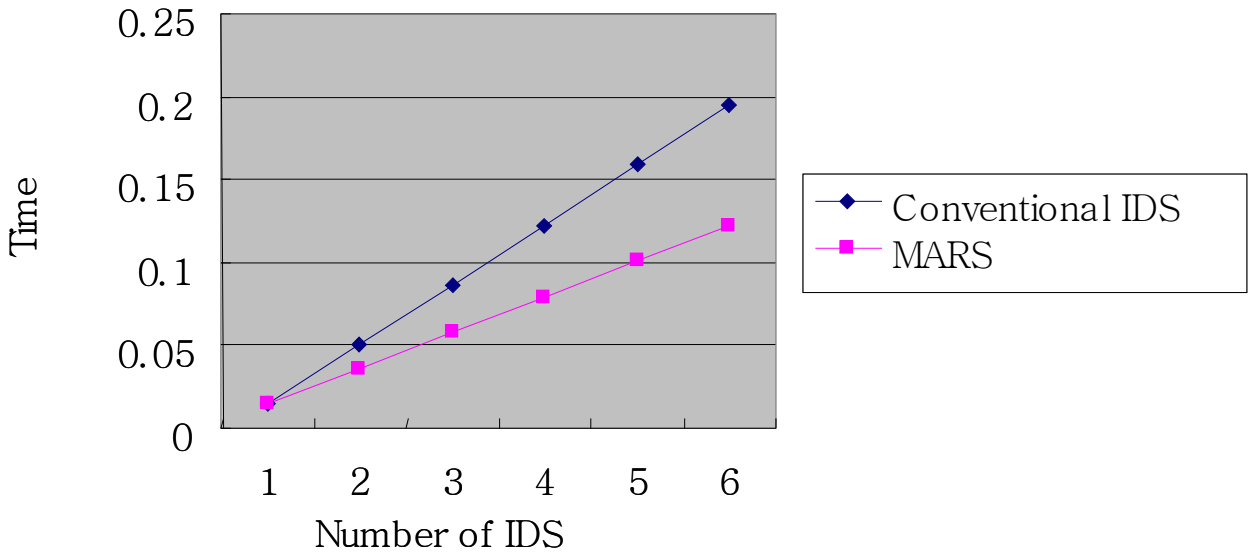
MARS



Conventional IDS

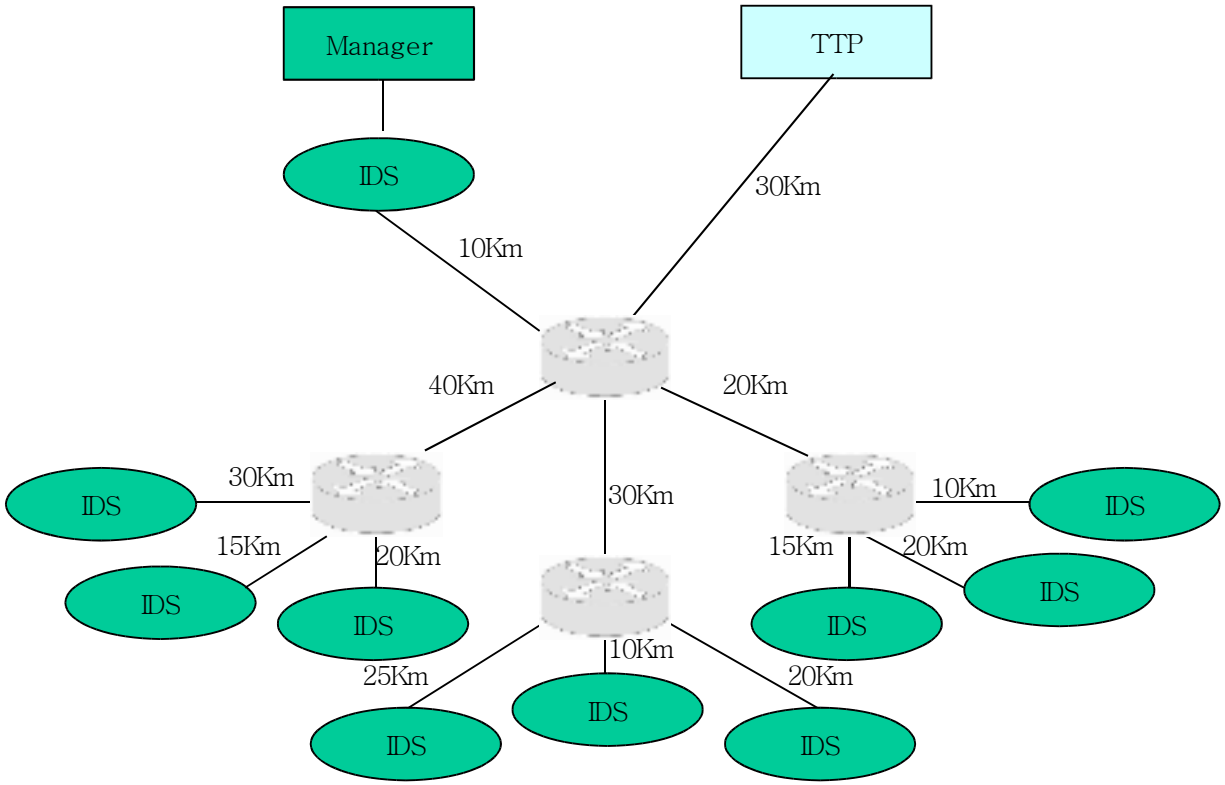
Comparison of Performance

- **Transmission elapsed time of Centralized approach and MARS**



Comparison of Performance

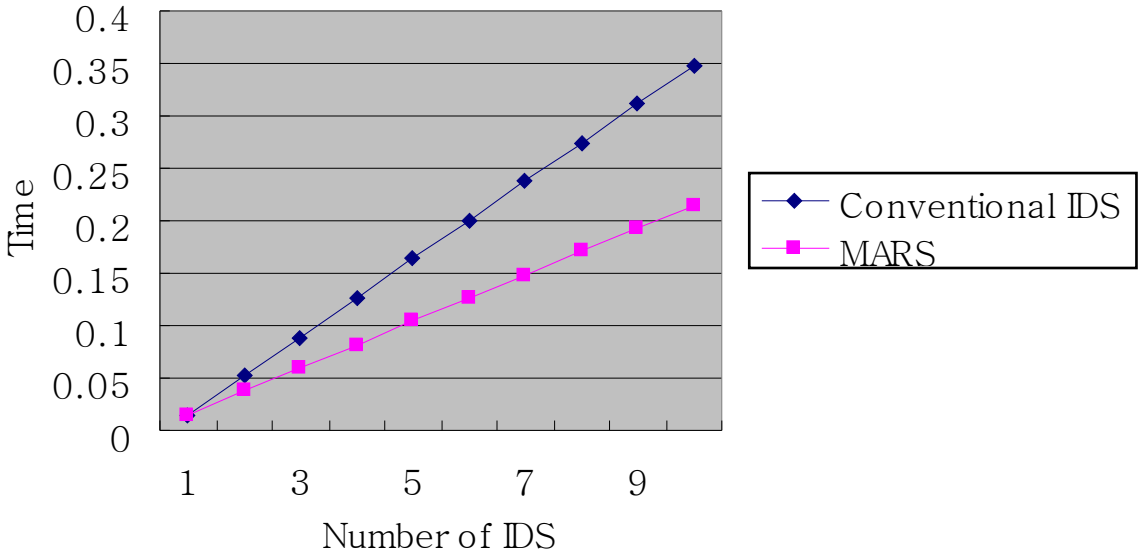
Simulation Topology 2 using NS-2



Simulation Topology 2

Comparison of Performance

- **Transmission elapsed time of Centralized approach and MARS in Tree topology**



Conclusion and Future works

Advantage of MARS

- Solve the security problem of mobile agent
- Suggest a more proactive mobile agent-based rule propagation and negotiation model
- Show the efficiency of the proposed model using NS-2 in various network topology in terms of transmission elapsed time
- Present advantages in terms of spreading rules rapidly and increasing scalability

Future Work

- Improve the functions of the mobile agent so as to cooperate with other security systems about security policies and intrusion detection