USC GridSec Project

Trusted Grid Computing with Distributed Security Control and Defense against Intrusions

Kai Hwang

Internet and Grid Computing Laboratory,
University of Southern California
Los Angeles, CA. 90089 USA

Research Meeting on February 10, 2004

Meeting Agenda :

1. The GridSec Project at USC
   – Hwang and Team
2. Grid Resource Access-Control and Policy Management
   - Neuman and Ryutov
3. FPGA-based Network Security Support
   - Prasanna and Baker
4. Discussions on Planned Future Work

The GridSec Project at USC:

- Sponsored by a NSF/ITR Research Grant ACR-0325409
- PI and Project Director: Kai Hwang

  Co-PIs: Clifford Neuman and Viktor Prasanna
- Post-doctorial and Foreign Collaborators:

  Dr. Tatyana Ryutov of USC/ISI

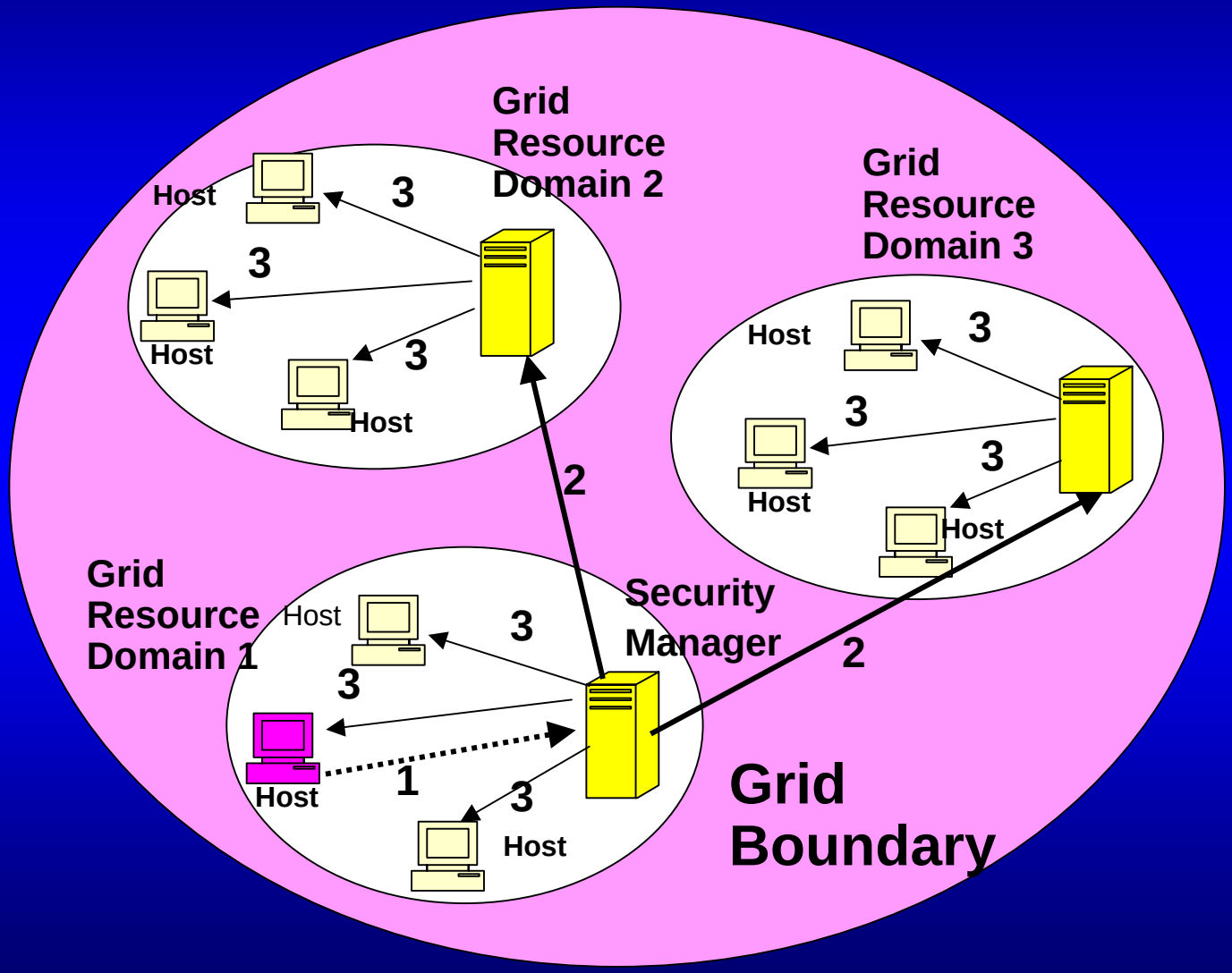
  Prof. Michel Cosnard of INRIA, France

  Dr. Zhiwei Xu of Chinese Academy of Sciences
- Ph.D.-bound Research Assistants:

  M. Qin, S. Song, Y. Kim, Z. Baker, L. Zhou,

  Y. Zhang, R. Tripathi, C. Chuan, …….

Distributed GridSec Architecture



Step 1: ·····▶
Intrusion detected by a local micro-firewall

Step 2: ⟶
All security managers alerted with the intrusion

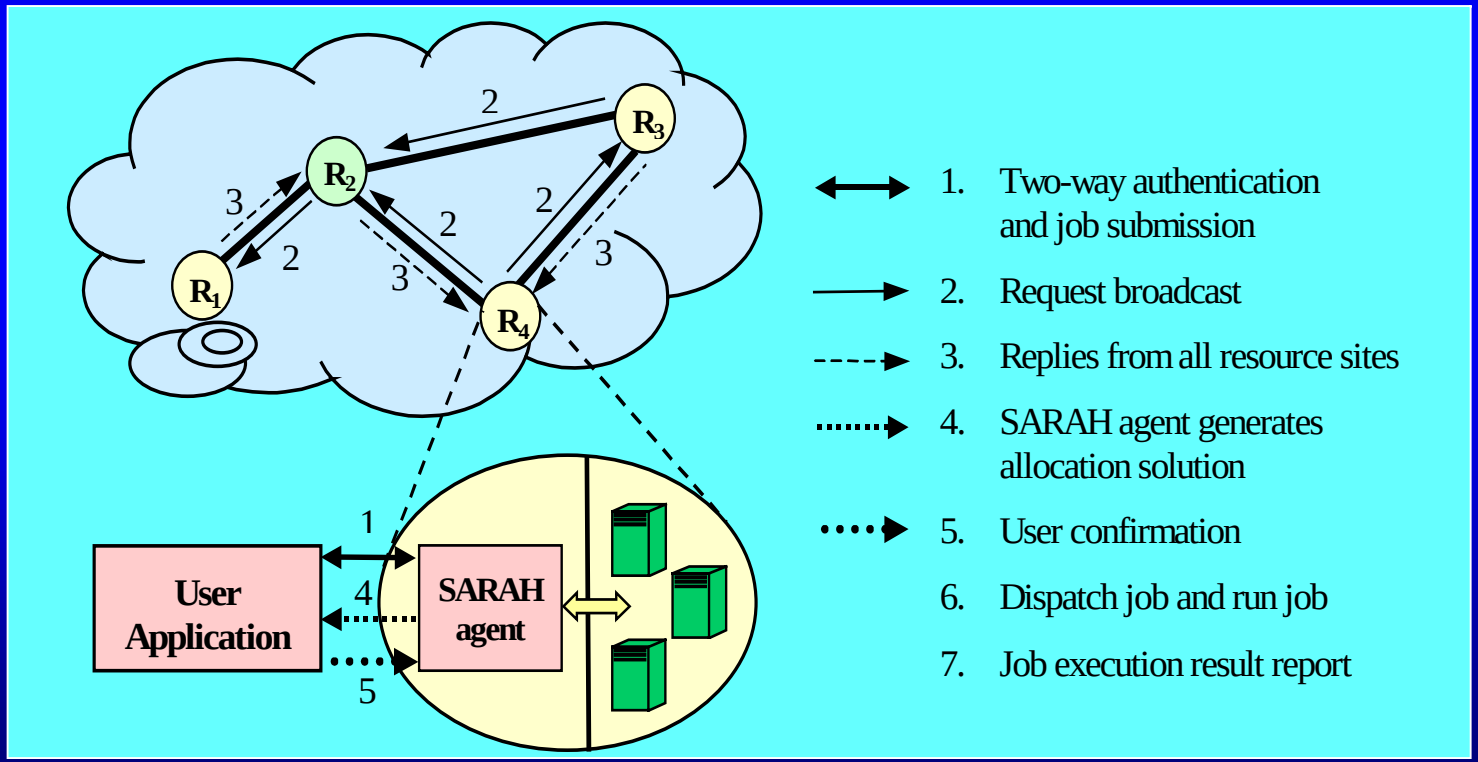
Step 3: ⟶
Security managers broadcast response command to all hosts under their jurisdiction.

Building Encrypted Tunnels between Resource Networks or Clusters for Trusted Grid Computing

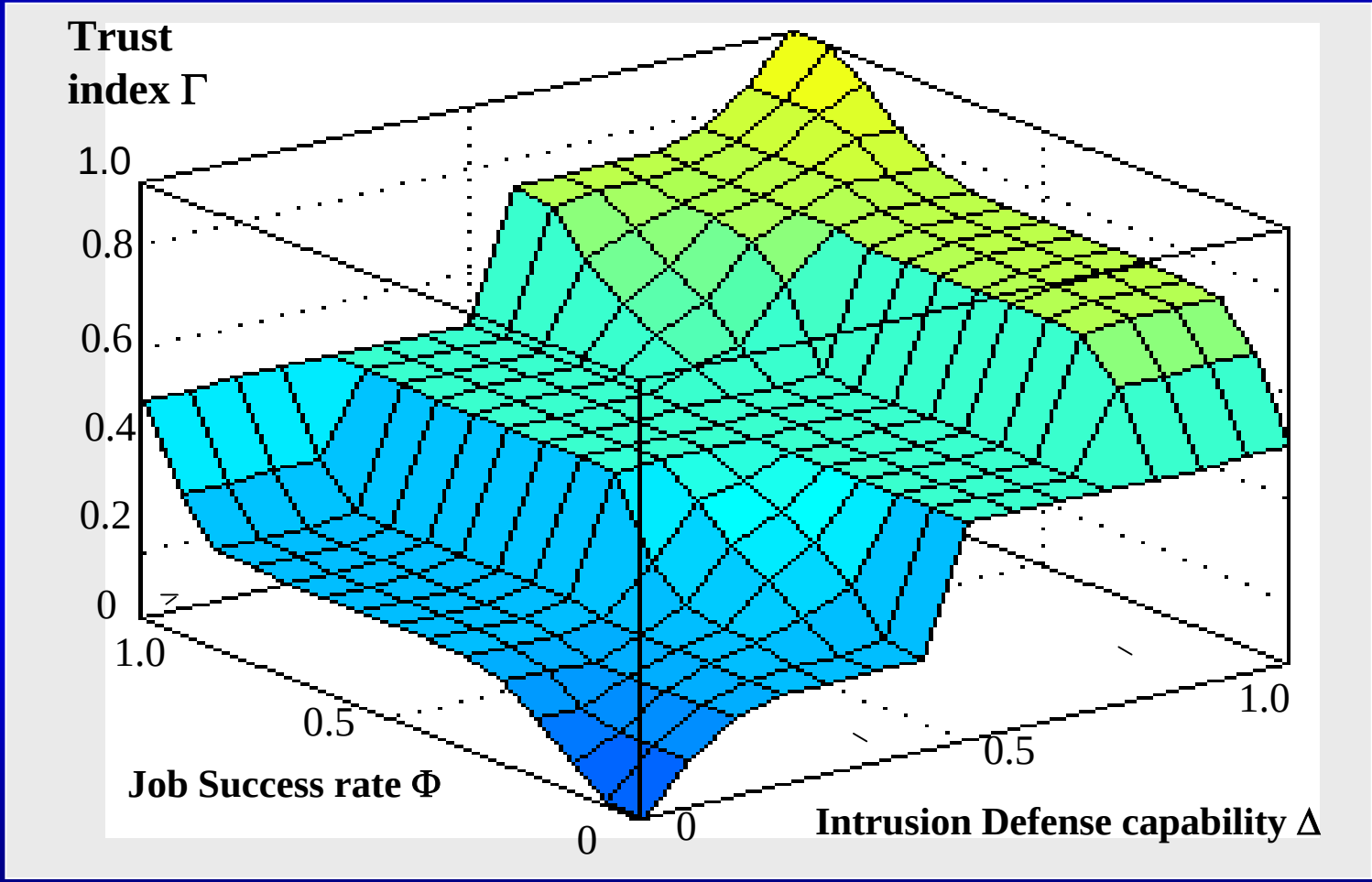
- With *n* nodes, the required number of tunnels grows with $O(n^2)$
- By using Dijkstra algorithm (All-source shortest path) in building VPN with minimum number of tunnels which grows with O (*n* log *n*) complexity (Yongjin Kim)
- Upon shortest path, security policy is generated to satisfy special Grid requirements, automatically if possible.
- How to integrate security policies from various private networks through the public network ? (Gurpreet Grewal)
- How to resolve policy conflicts among hosts, firewalls, switches, routers, and servers, etc. in a Grid environment ?

Security-Assured Resource Allocation
(Shanshan Song and Mikin Macwan)

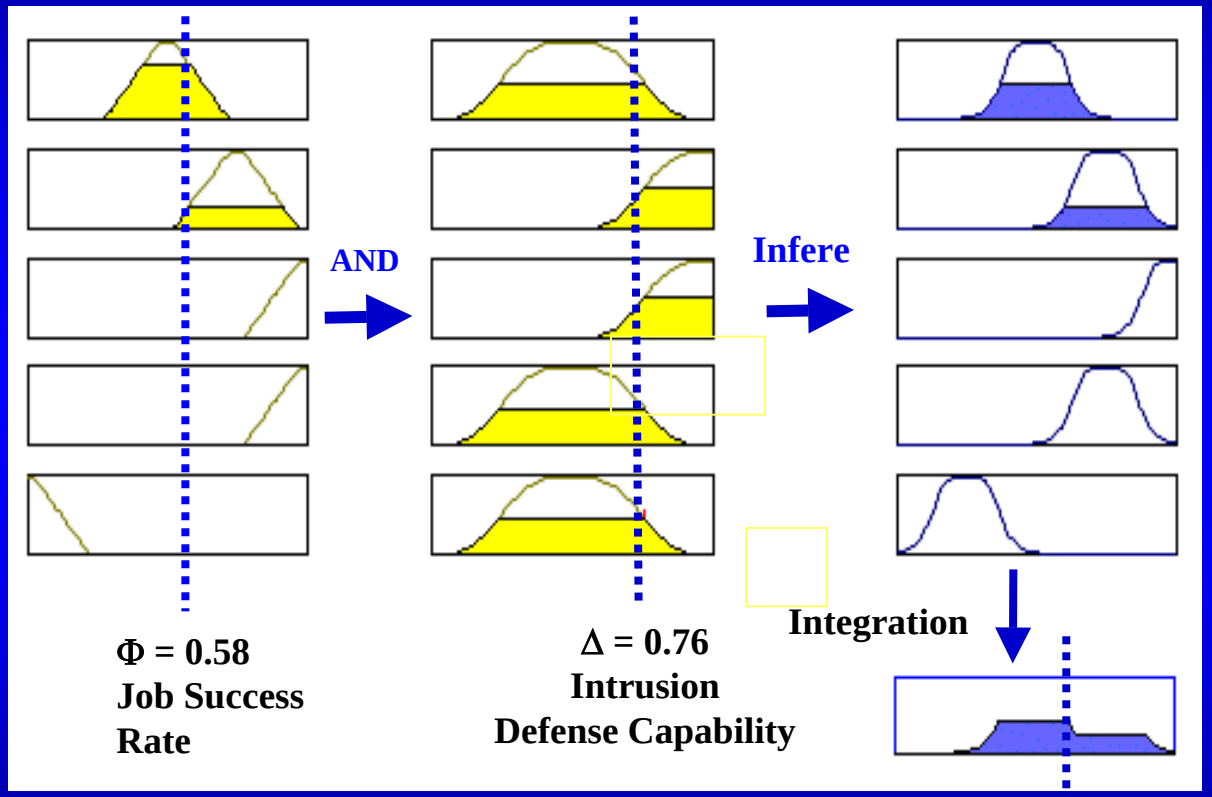
- Fuzzy logic for trust management over multiple Grid resource sites
- Linear programming model for trusted resource allocation (Sarah)



Trust Index of Grid Resource Site:
derived from job success rate and intrusion defense capability at resource site periodically



Fuzzy Logic Inference for Assessing Trust Index at Grid Resource Site



Security-Assured Resource Allocation

Algorithm: Dual-objective linear programming for secure resource allocation

Inputs: (1) A Grid job $J = (P_o, T_o, C_o)$, submitted to the **j**-th resource site R_j

(2) P_i and C_i (**i** = 1, 2, …, k) for k resource sites and trust vector V_j in R_j.

Output: The resource allocation vector $X = (x_1, x_2, \ldots, x_k)$.

Objective Function: Maximize $P = \sum_{i=1}^{k} x_i P_i t_{ij}$ and minimize $C = \sum_{i=1}^{k} x_i P_i C_i$ simultaneously.

or equivalently, maximize the performance/cost ratio E defined in Eq. (6).

Subject to the following constraints**:**

$$\sum_{i=1}^{k} x_i P_i \geq P_o, \quad \sum_{i=1}^{k} x_i P_i C_i \leq C_o, \quad \text{and} \quad t_{ij} \geq T_o \qquad (7)$$

where $0 \leq x_i \leq 1$ for **i** = 1, 2, …, k.

A SARAH Resource Optimization Example

V_1	V_2	V_3	V_4
0.5	0.5	0.4	0.4
0.8	0.8	0.7	1.0
0.9	1.0	0.8	0.8
0.7	0.7	0.6	0.6

(a) Trust Matrix

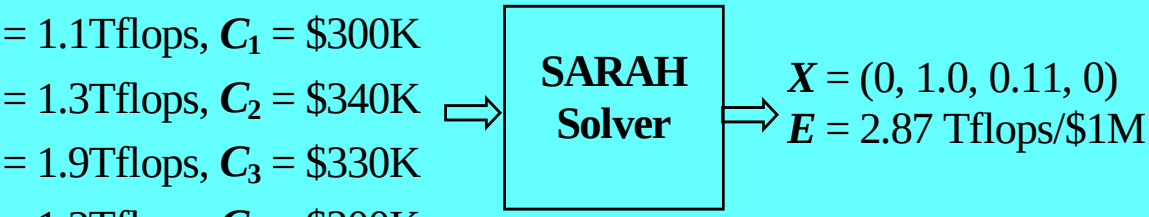
J_1 = (1.5Tflops, \$600K, 0.6)

P_1 = 1.1Tflops, C_1 = \$300K

P_2 = 1.3Tflops, C_2 = \$340K

P_3 = 1.9Tflops, C_3 = \$330K

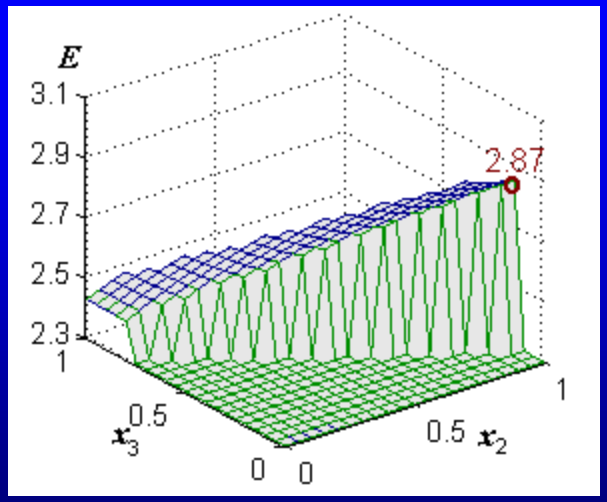
P_4 = 1.2Tflops, C_4 = \$300K

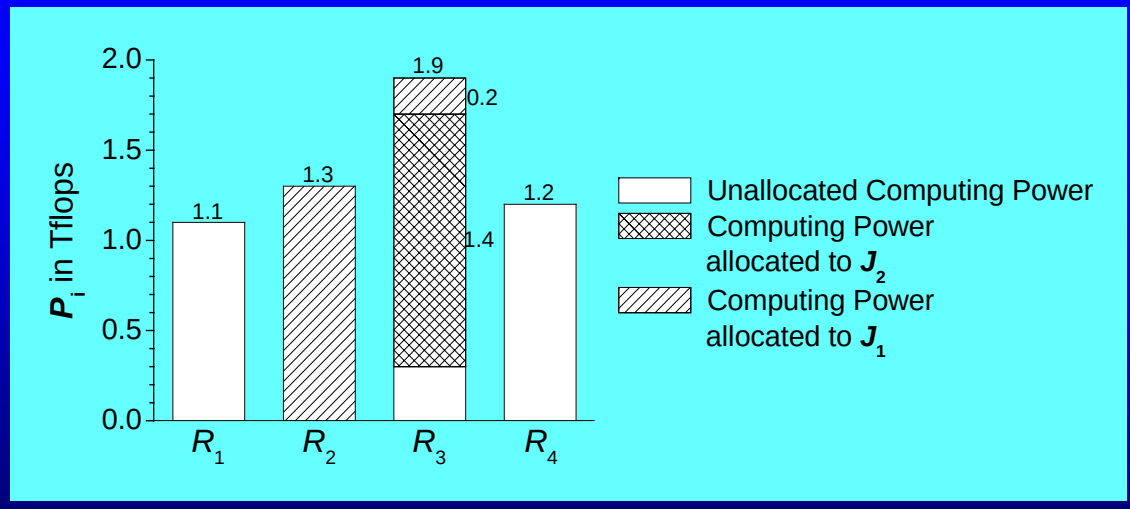


X = (0, 1.0, 0.11, 0)

E = 2.87 Tflops/\$1M

(b) Inputs and outputs

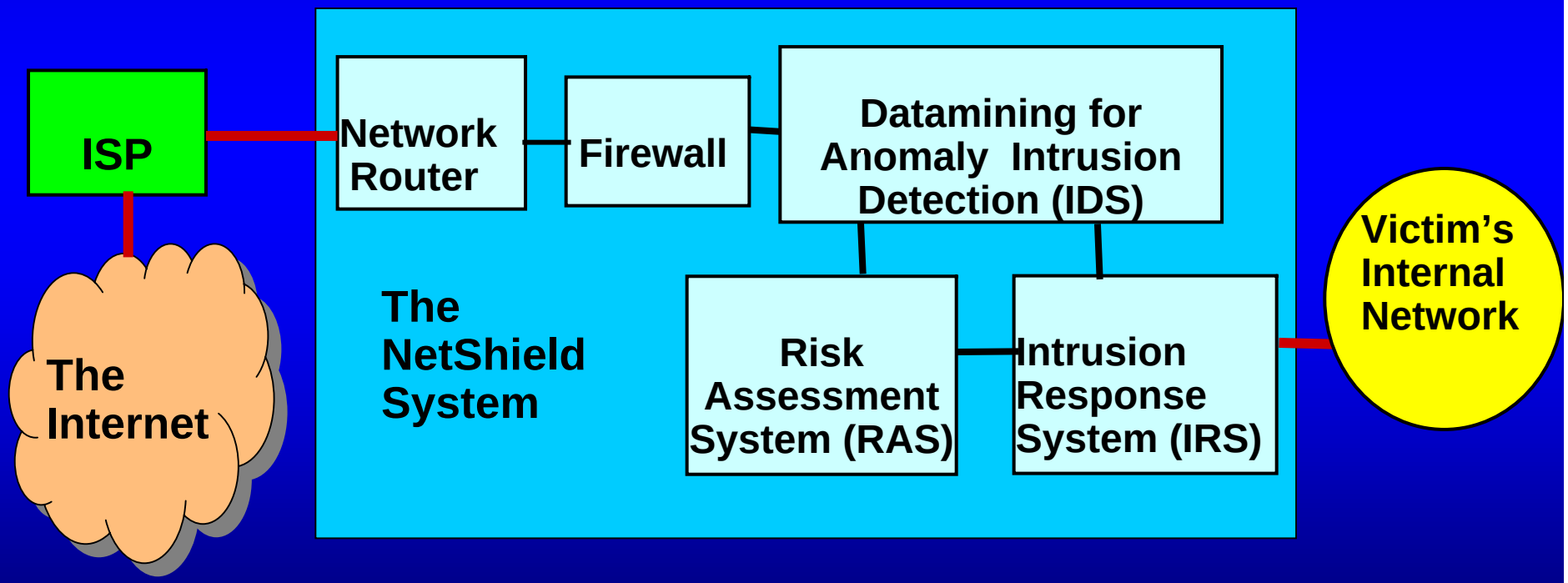




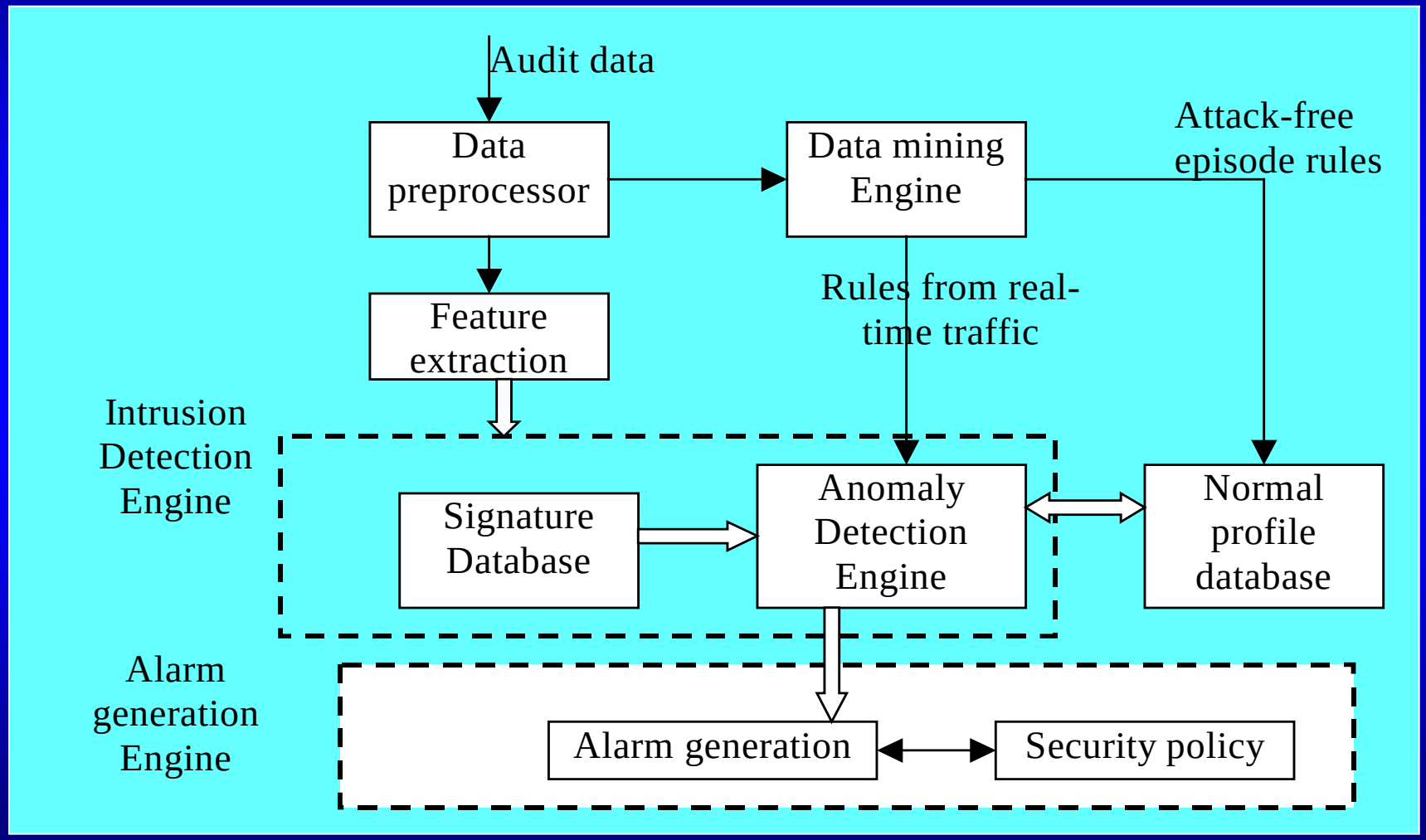
USC NetShield Intrusion Defense System

for Protecting Grid Computing Resource Sites

(Narayana, Chuan, and Qin)



Data mining Architecture for Network Anomaly Detection (Min Qin)



Datamining For Intrusion Detection

Trace TCP/UDP/ICMP connection events

to derive frequent episode rule (FER)

on traffic patterns. The SYN flood attack is

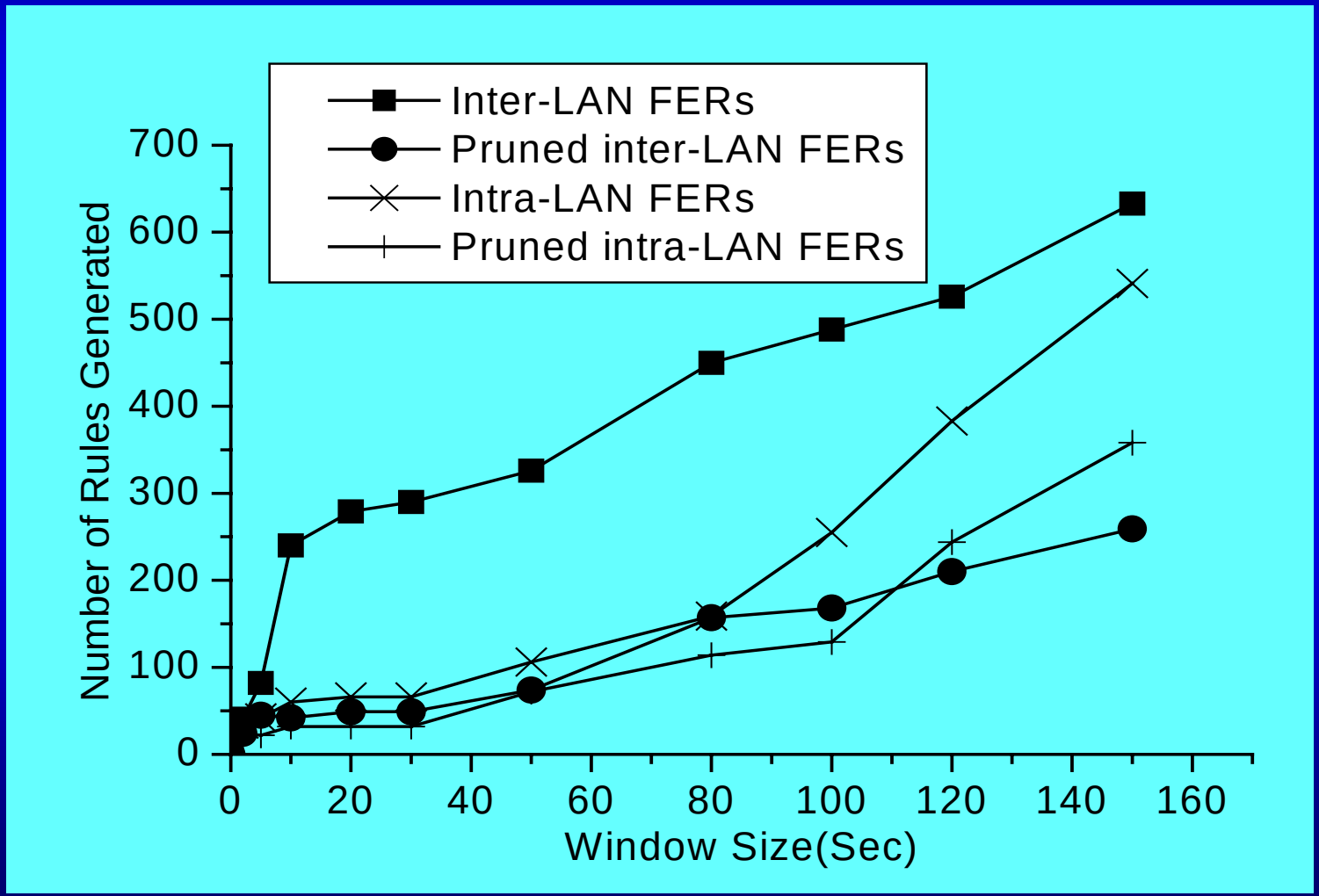
specified by the following rule:

(service = http, flag = S0) (service = http, flag = S0)

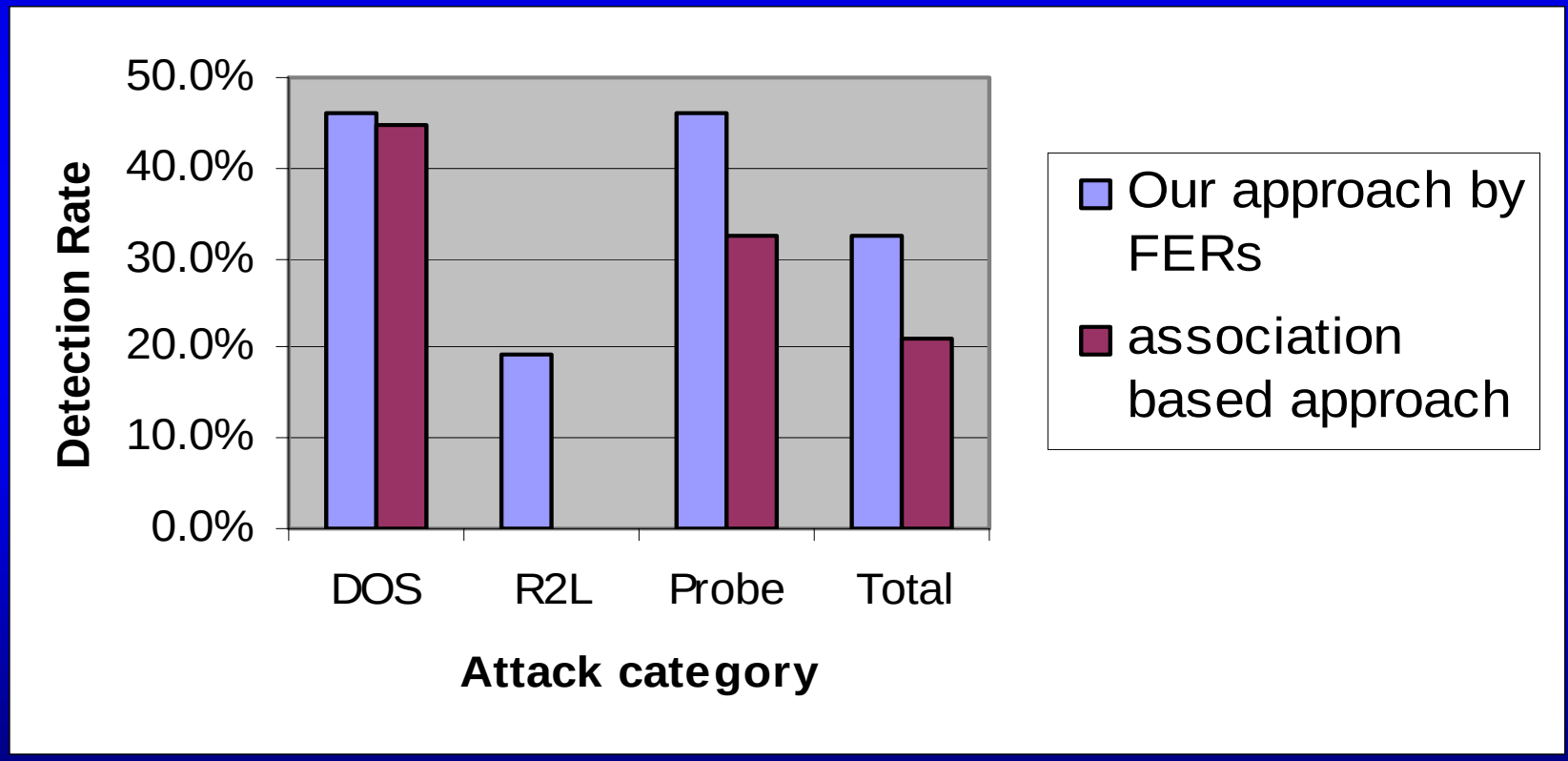
→ **(service = http, flag = S0)**

Reduction of Rule Search Space

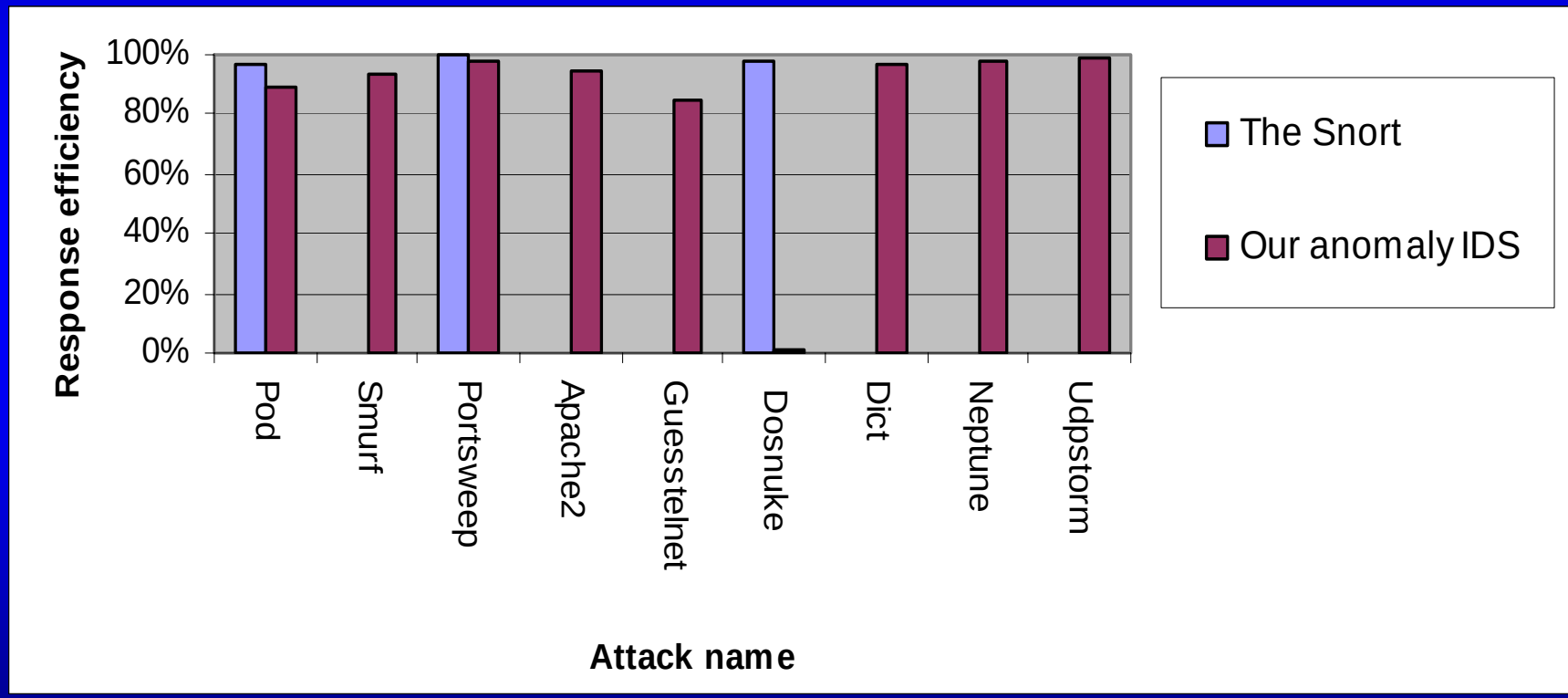
after pruning of ineffective FERs



Anomaly Detection Results
using Frequent Episode Rules



Intrusion Response Efficiency



DDoS Detection and Defense

(Y. Zhang and R. Tripathi)

- Internet traffic flow analysis for packet filtering, rate limiting, priority queuing, etc.
- Smart filtering for countering DDoS attacks based on traffic history analysis
- Use the Georgia Tech Network Simulator
- Test on the USC Internet trace data sets

Recent Papers and Technical Reports :

1. M. Qin and K. Hwang, " Frequent Episode Rules for Intrusive Anomaly Dtection with Internet Datamining", *USENIX Security Symposium*, submitted Jan.27, 2004
2. S. Song and k. Hwang, " Integrated Trust and Resource Optimization for Security-Assured Grip Computing", *International Symposium on High-Performance Distributed Computing*, (HPDC-13), submitted Feb. 7, 2004
3. Z. Baker and V. Prasanna", A Methodology for Synthesis of Efficient Intrusion Detection Systems on FPGAs", *IEEE Field-Programmable Custom Comuting Mechanism* (FCCM), submitted Jan. 19, 2004
4. K. Hwang, et al, " GridSec and NetShield Architecture for Securing Grid Computing", *Tech. Report 2003-1*, USC Internet and Grid Computing Lab., (under revision)