Distributed Security Enforcement for Trusted Cluster and Grid Computing

Keynote address at the IEEE
International Conference on Cluster Computing
(Cluster 2003), Hong Kong, Dec. 2, 2003

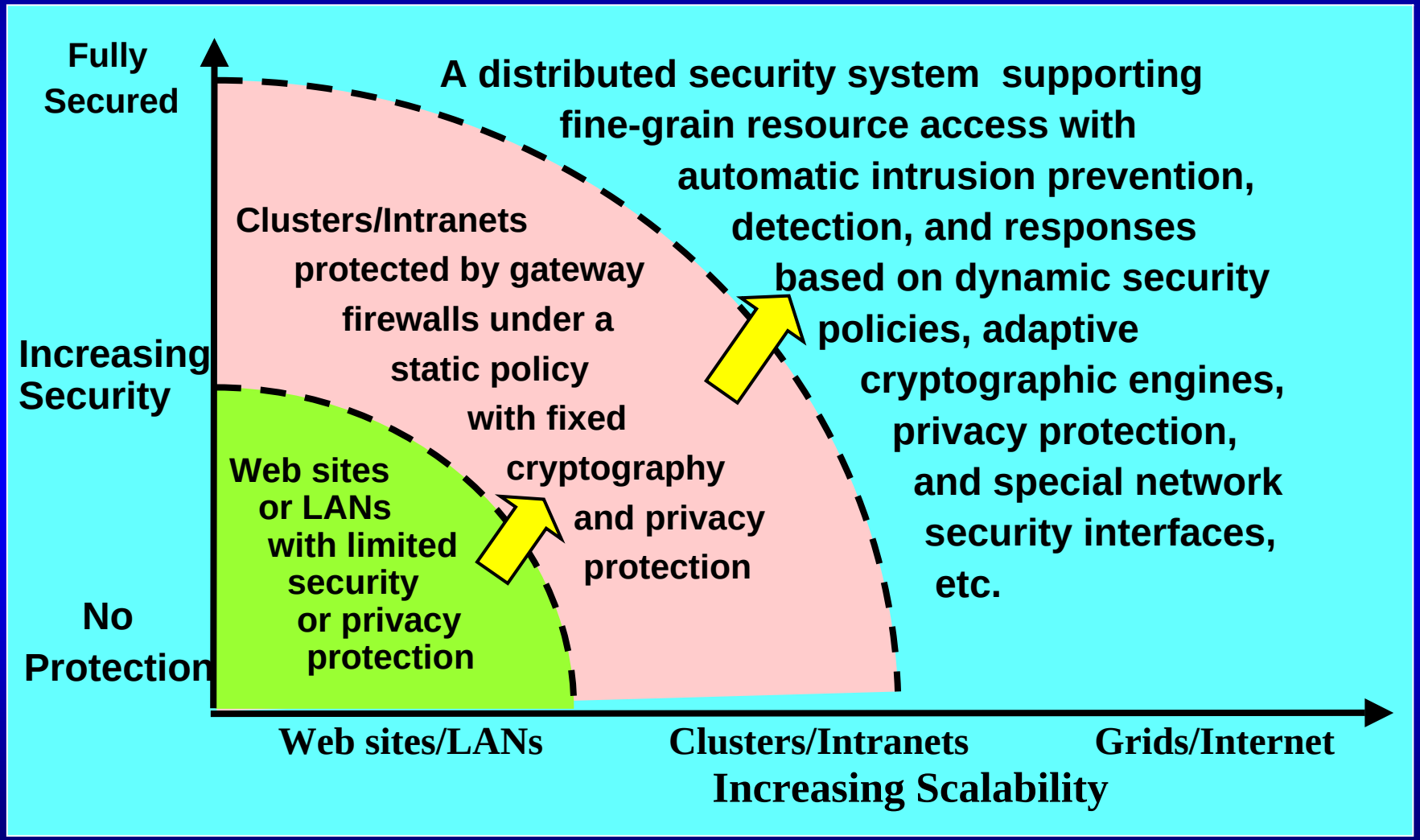
Kai Hwang

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

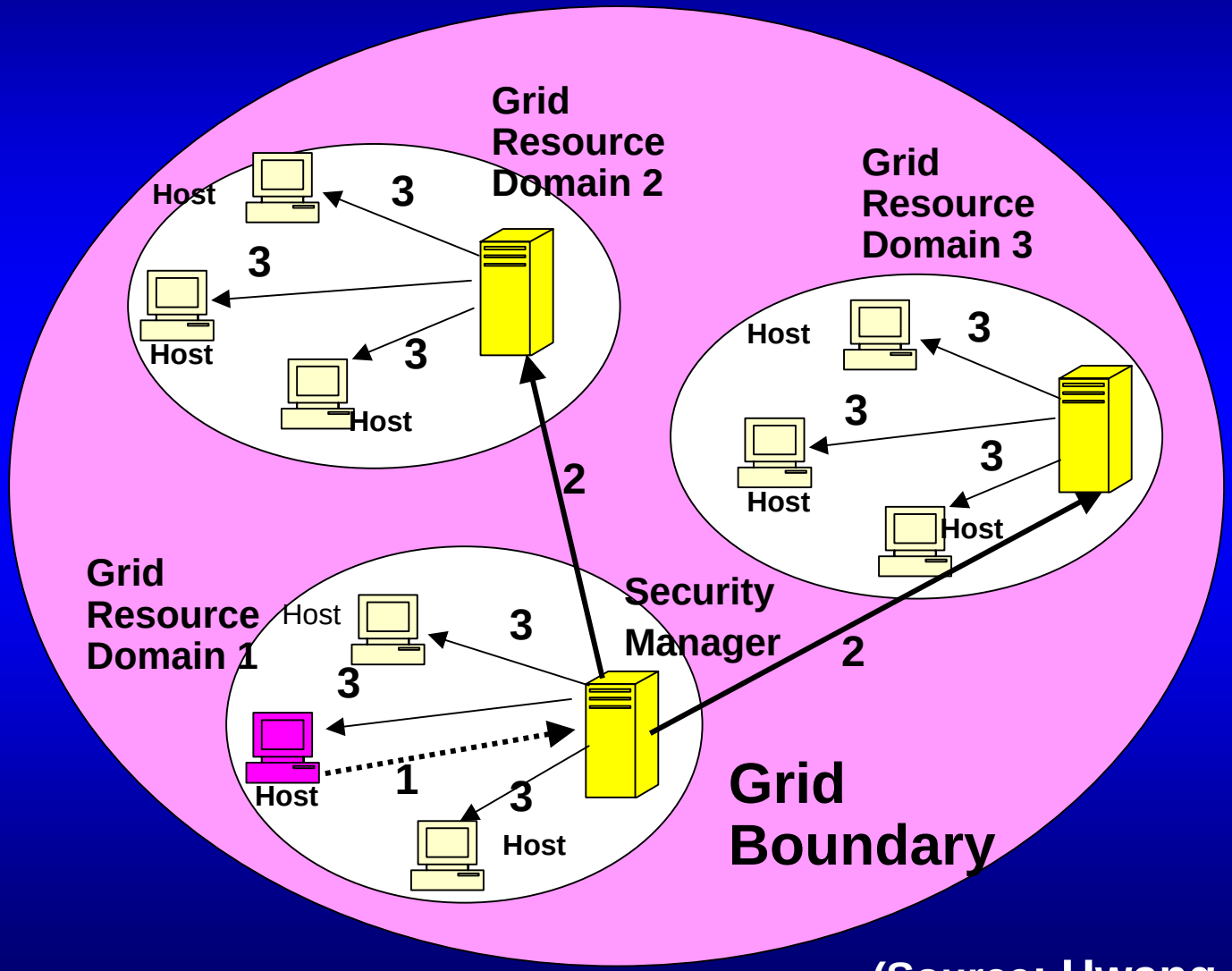
Presentation Outline:

1. Distributed GridSec Architecture
2. Virtual Private Networks for Distributed Security Enforcement
3. Anomaly Intrusion Detection with Datamining
4. Defense Strategies against DDoS Attacks
5. Secure Management and Access Control in Distributed Shared Resources

Security vs. Scalability



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.

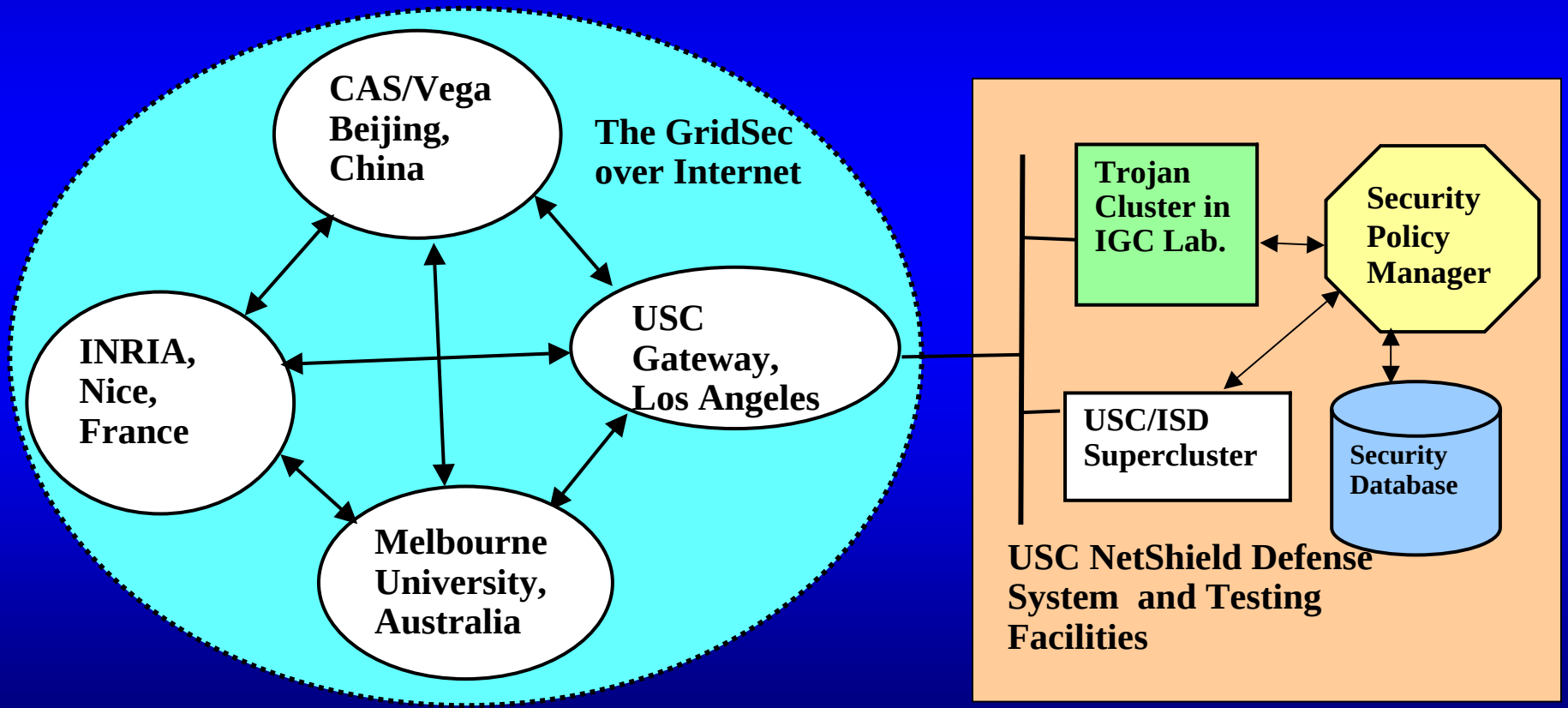
(Source: Hwang, et al [1])

GridSec Design Objectives:

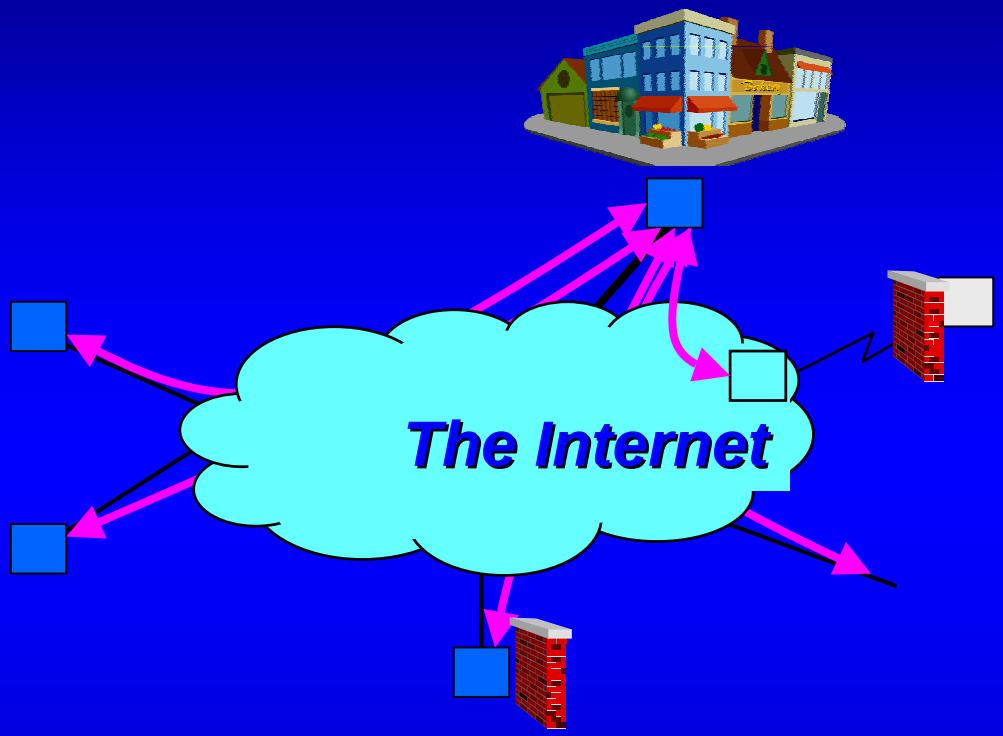
- Remove the security barrier hindering distributed grid computing - Offering a new trust model
- GridSec offers distributed intelligence in trust management on top of Globus, AppLes, NimRod etc.
- Dynamic grid resource allocation optimized with respect to computing power, security demand, and cost limit
- Benefiting E-commerce, digital government, public safety, and global economy over the Internet using GridSec-based VPN tunneling

Global GridSec Testing Environment

International Collaborators in USA, France, China, and Australia



GridSec VPN : Combining both IPSec and MPLS Features for Federated Security



Grid Resource Sites

A VPN specially configured on a public Infrastructure based on tunneling at the IPSec network layer. Same policies as a private network supported by service provider and using **IPSec, MPLS, PKI, GridSec, attribute certificates, etc.**

NPN-Secured Grid Resource Management

Step 1: Two-way authentication and User request submission to resource manager (RMgr) in Grid site *F*.

Step 2: RMgr in GRS F broadcast request to other GRSs.

Step 3: RMgrs in other GRSs send reply with available resources.

Step 4: RMgr generates resource allocation solutions based on received information, and sent back to user.

Step 5: User selects one solution based on computing demand and budget constraints

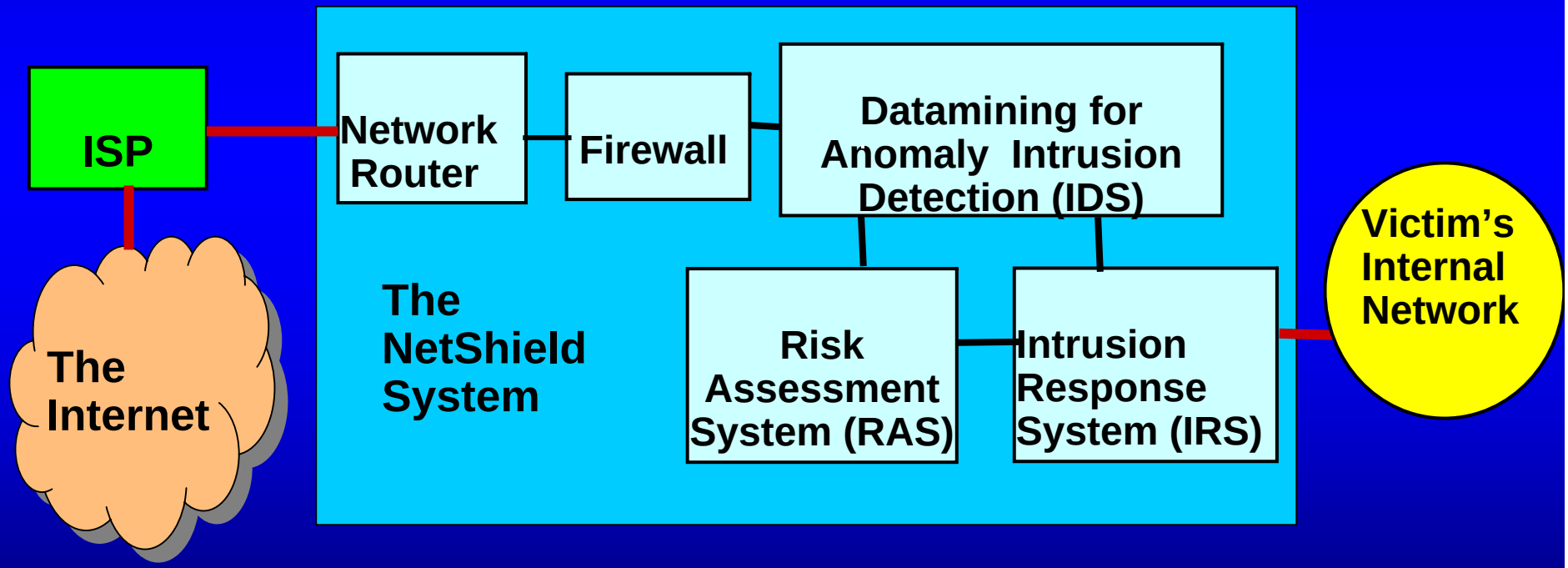
Step 6: Allocate resources {*A*, *E*, *F*}, establish VPN connections , and

Developing Virtual Private Networks for Trusted Grid Computing

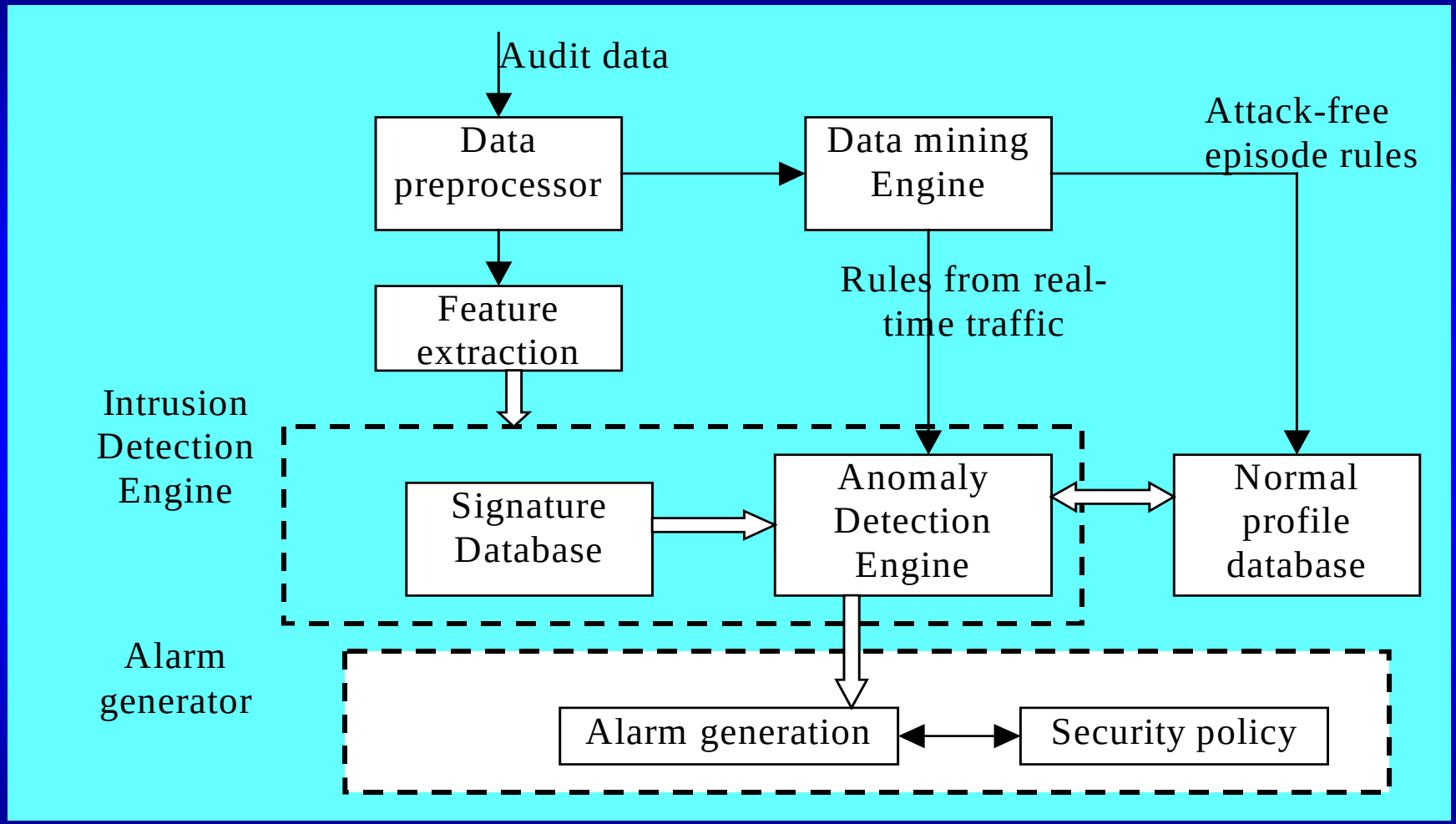
- Create encrypted tunnels between private networks used to form the Grid computing infrastructure
- The GridSec project chooses an approach combining the advantages of both IPsec-based and MPLS-based VPNs
- Aimed to satisfy the IPv6 standards proposed for both wired and wireless networks for the next-generation Internet

USC NetShield Defense System

Protecting Cluster or Grid Resources



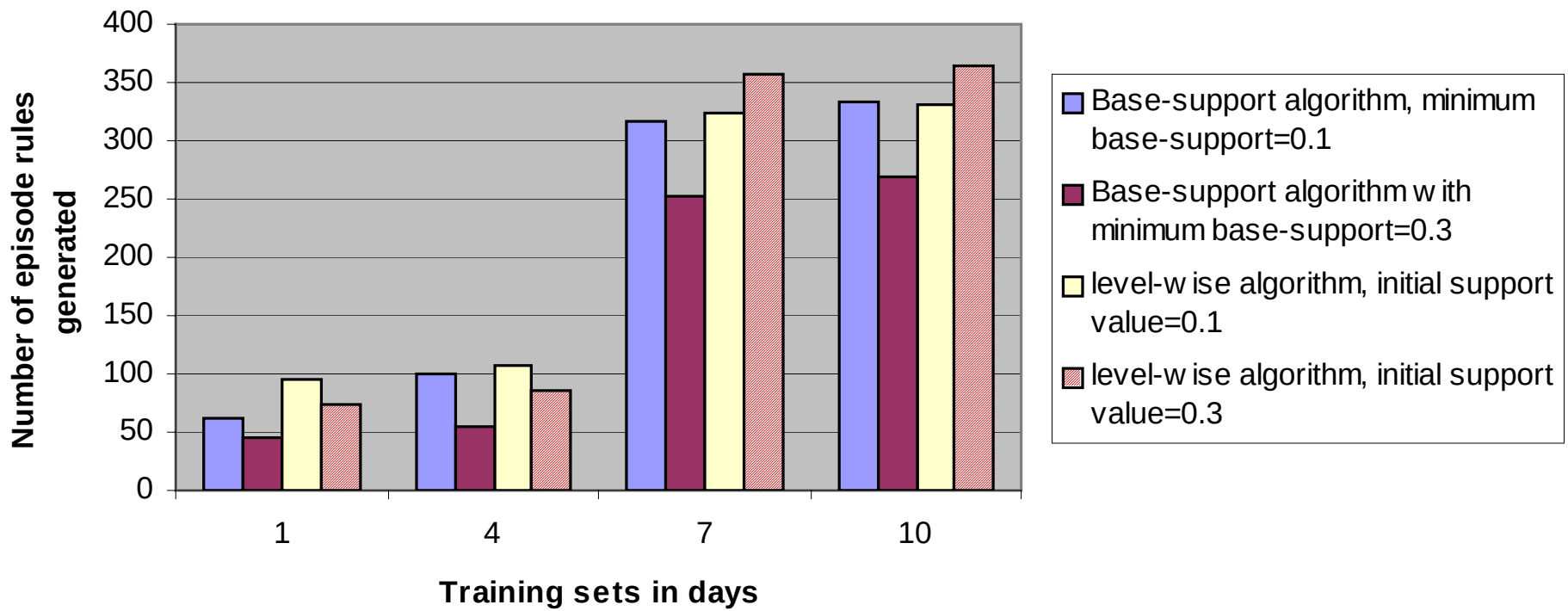
Anomaly-based IDS Architecture



(Ref.: Qin and Hwang [3])

Testing of the Base-Support Mining Algorithm on Normal TCP Traffic Connections

from the 1999 DARPA Intrusion Detection Evaluation Data Sets collected in the first 10 Days



Using our base-support mining algorithm with a minimum confidence value of 0.6 and a window size of 30 sec, compared with using Lee's Level-wise mining algorithm

Pruning of Ineffective Episode Rules

- **Transposition Law: The rule:** $L_1, L_2, \ldots, L_n \rightarrow R_1, \ldots, R_m$

  is more effective than using the rule:

  $$L_1, L_2, \ldots, L_{n-1} \rightarrow L_n, R_1, \ldots, R_m$$

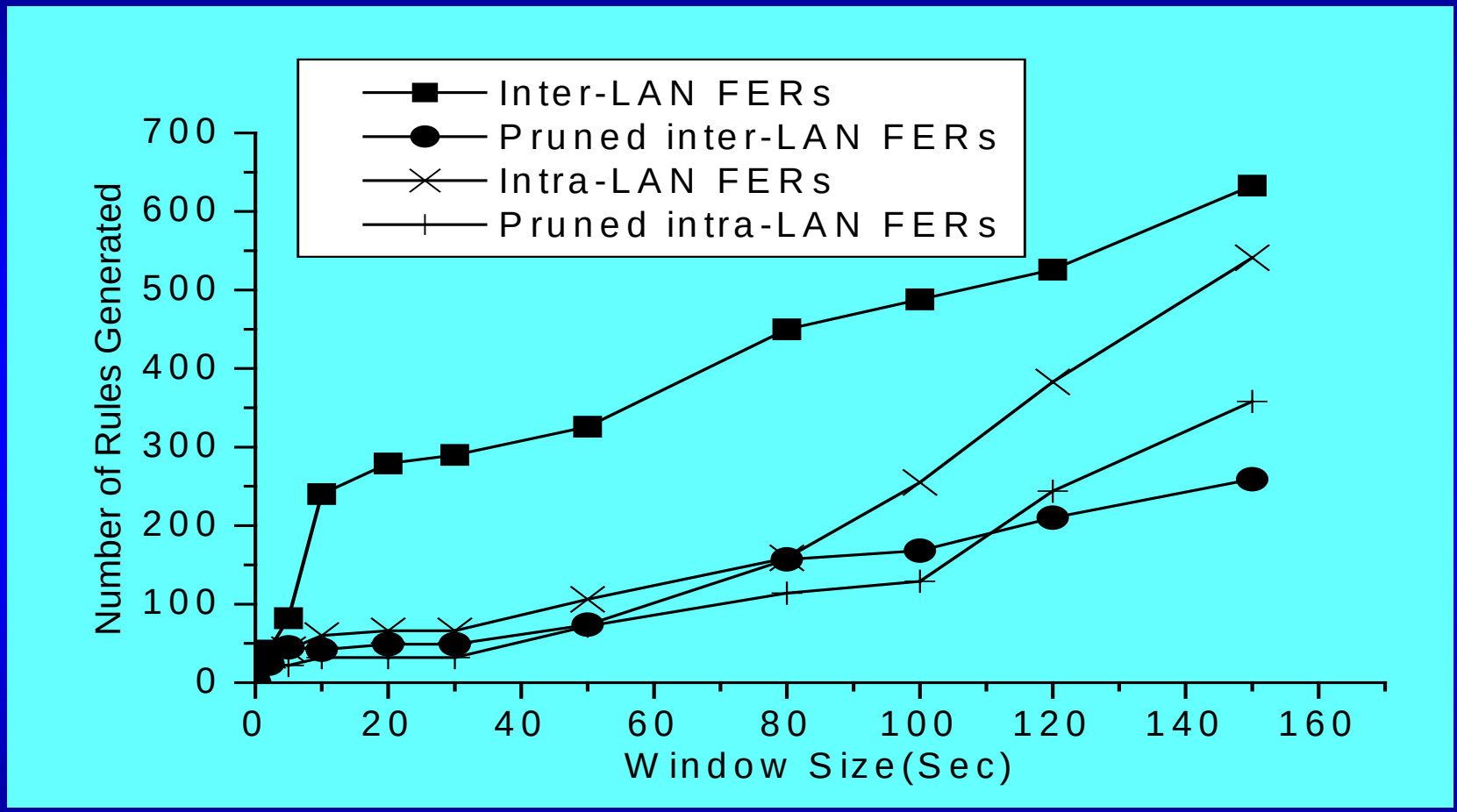
- **Elimination Law: The rule** $L_1, L_2 \rightarrow R_1$ (c_1, s_1) **is less effective than using :** $L_2 \rightarrow R_1$ (c_2, s_2), **if** $c1 \approx c2$

- **Transitive Reconstruction Law: The rule:** $L_1 \rightarrow R_1, R_2$

  becomes ineffective, if we have the following rules

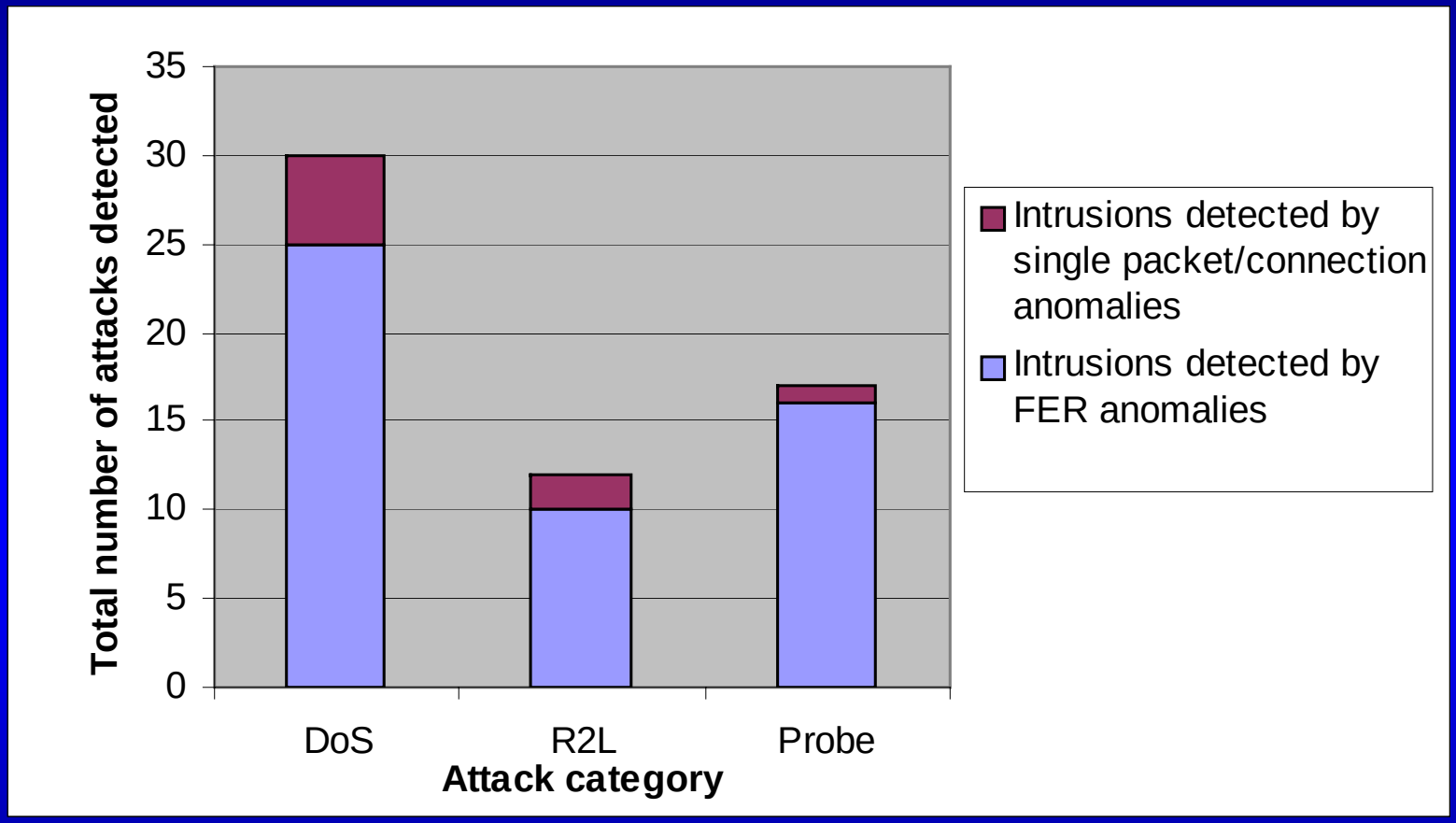
  $L_1 \rightarrow R_1$ **and** $R_1 \rightarrow R_2$ **already in the rule set**

Effects of Pruning on the Growth of Frequent Episode Rules for Inter-LAN and Intra-LAN Traffic Events



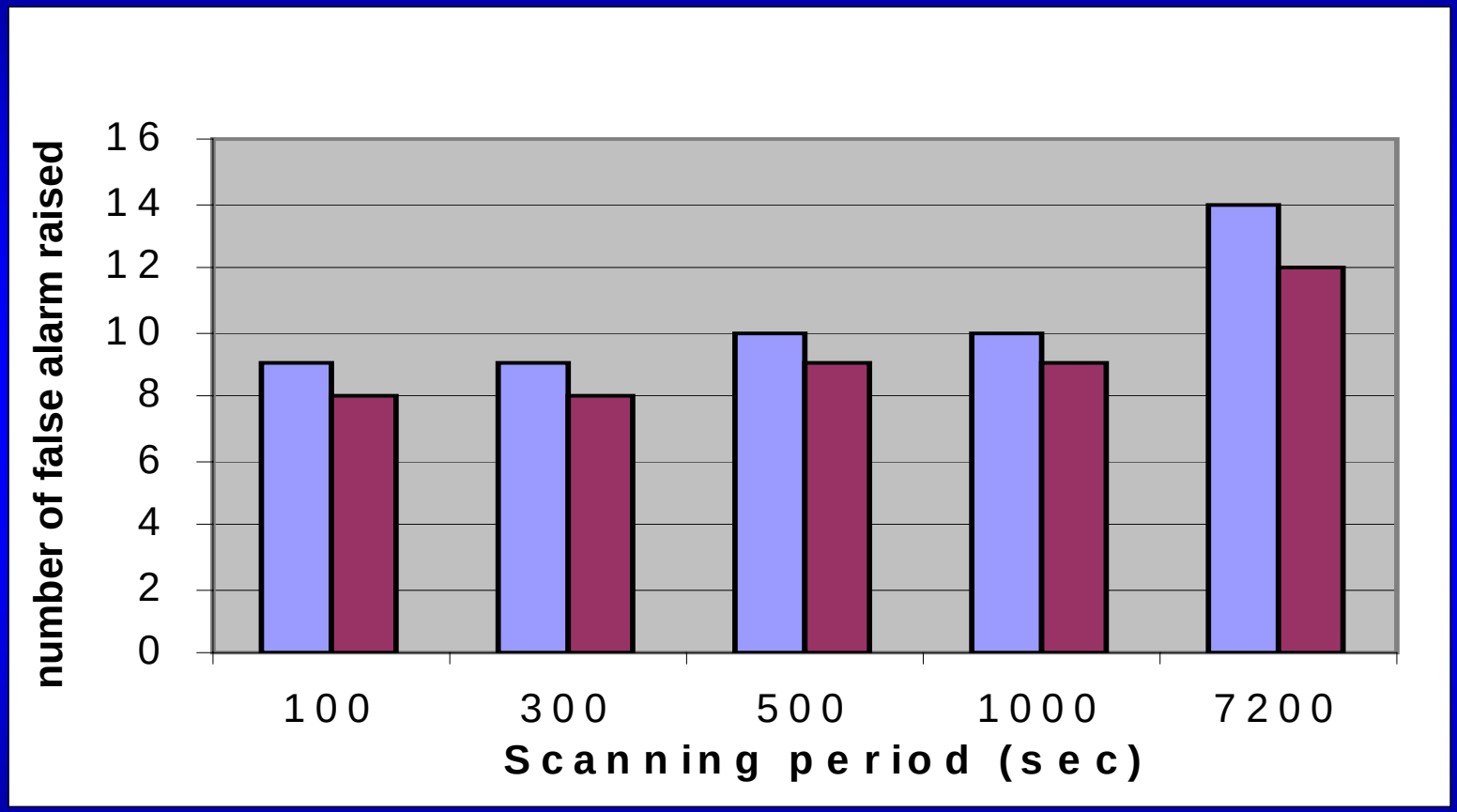
The base-support = 0.1, the minimum confidence = 0.6, the reference attributes = destination, and axis attributes = service

Anomaly Intrusion Detection Rate



Intrusive attacks detected by single packet per connection versus checking the frequent episode rules

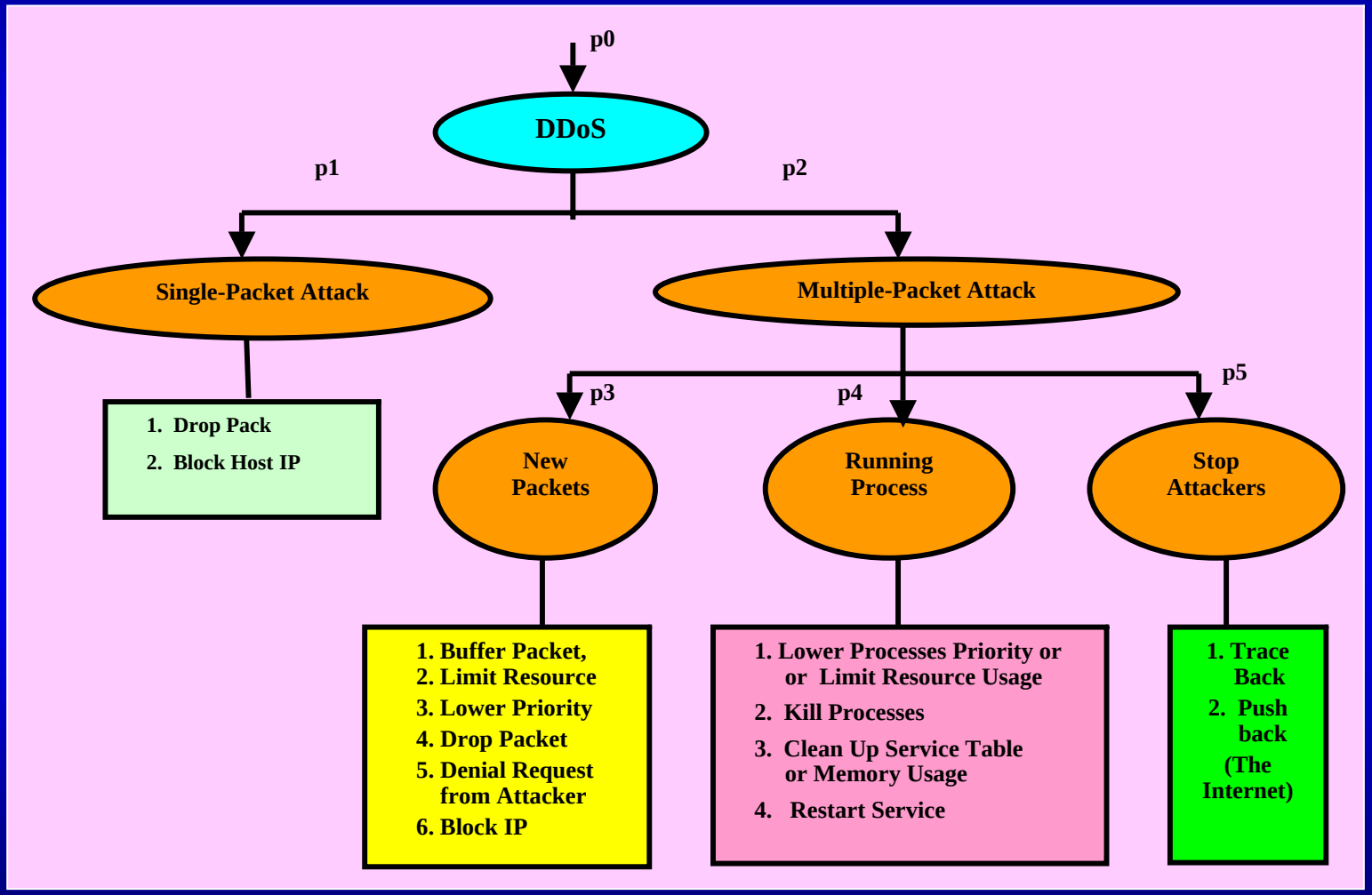
Effect of Pruning on Reducing the False Alarm Rate in Anomaly Intrusion Detection



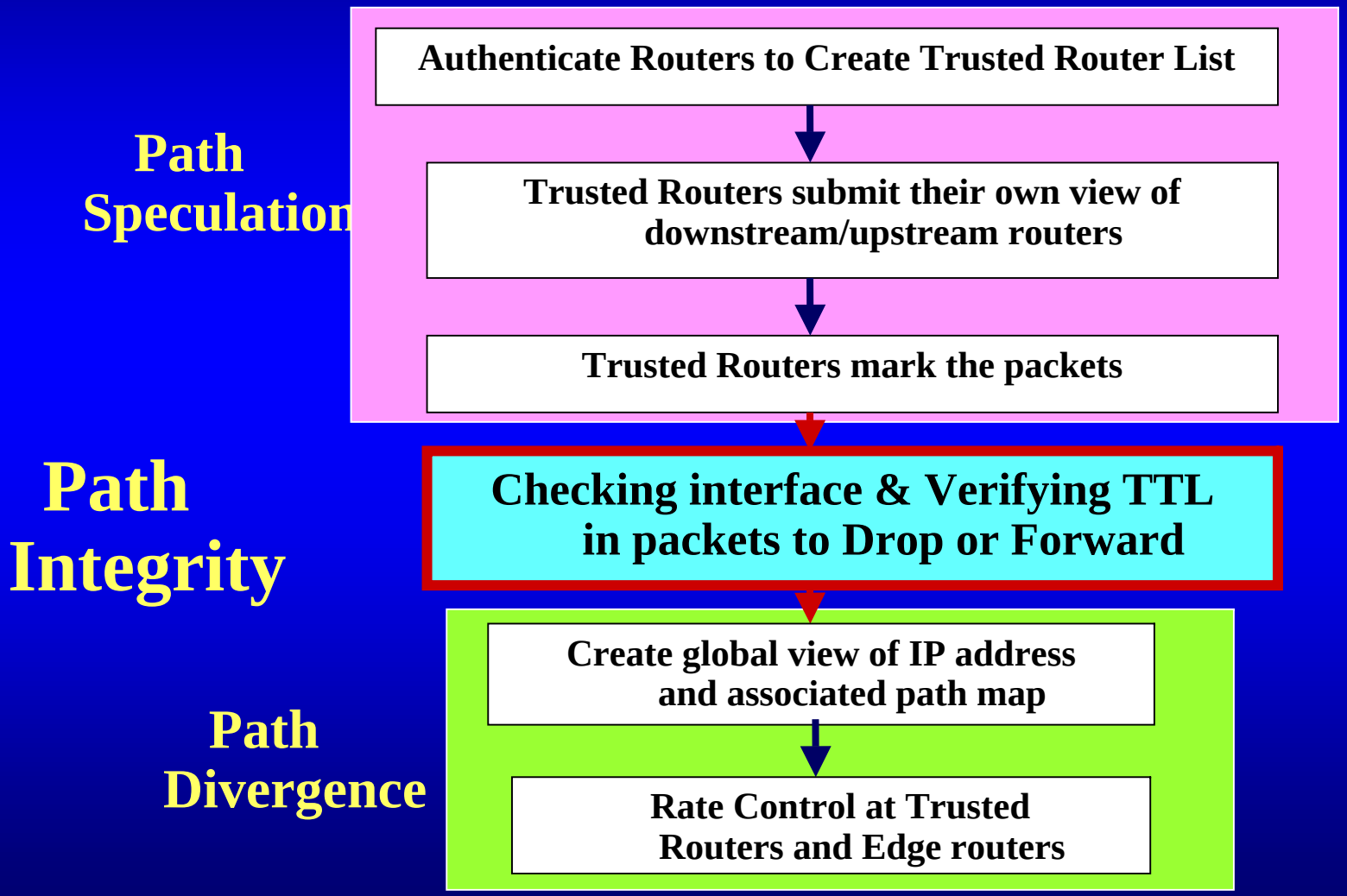
Blue bar: Detection without rule pruning

Purple bar: Detection with rule purning

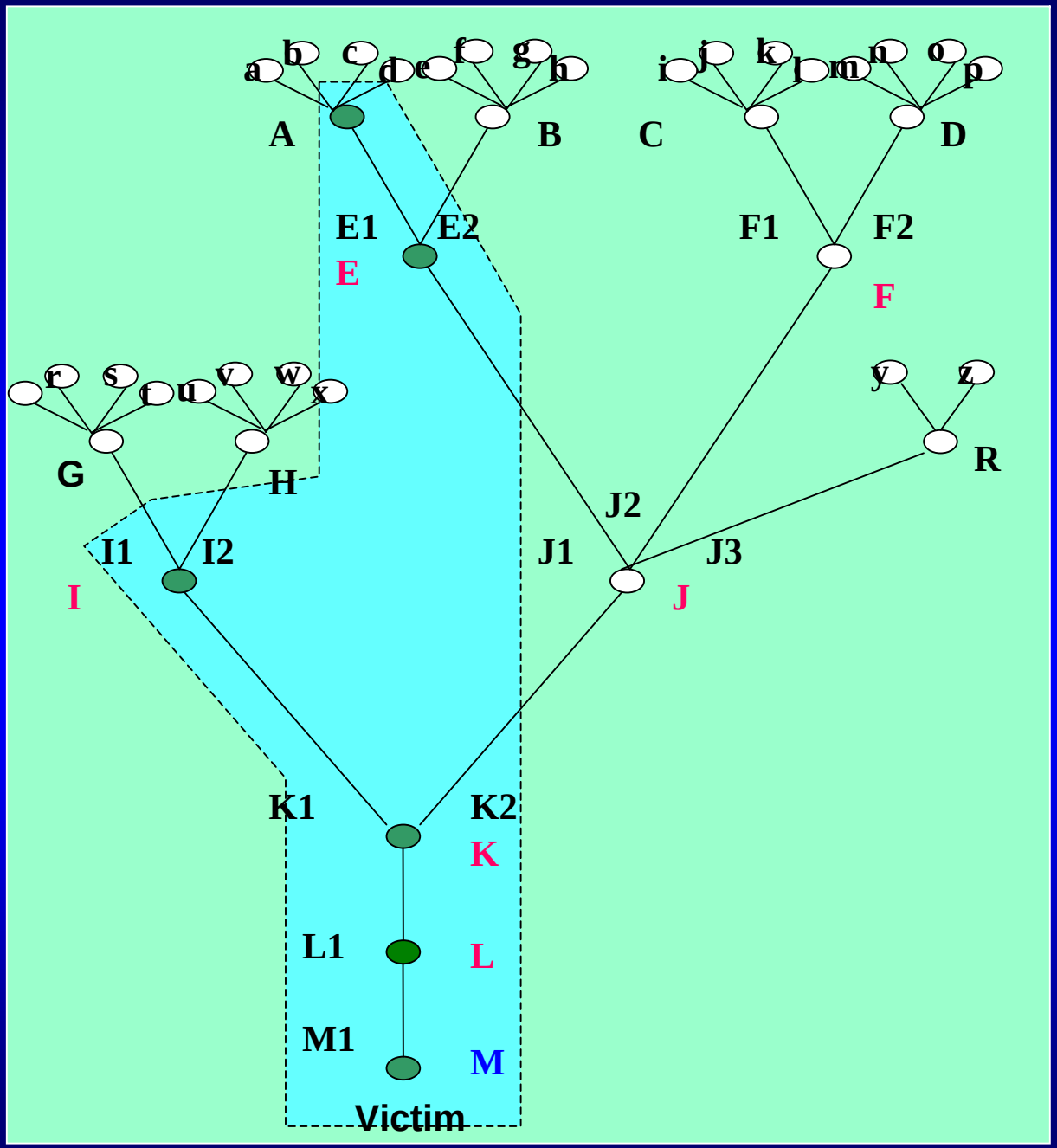
Intrusion Response Strategies for Defending against DDoS Attacks



Verifying IP Path Integrity to Filter Out Packets from DDoS Attacks



Edge Pushback Against DDoS Flood Attacks



A, B, C, D,
G, H, R : Edge Routers

E, F, I, J,
K, L : Intermediate Routers
a-z : End hosts

E1,E2 : E Interface
F1,F2 : F Interface
I1,I2 : I Interface
J1,J2, J3 : J Interface
K1,K2 : K Interface
L1 : L Interface
M1 : M Interface

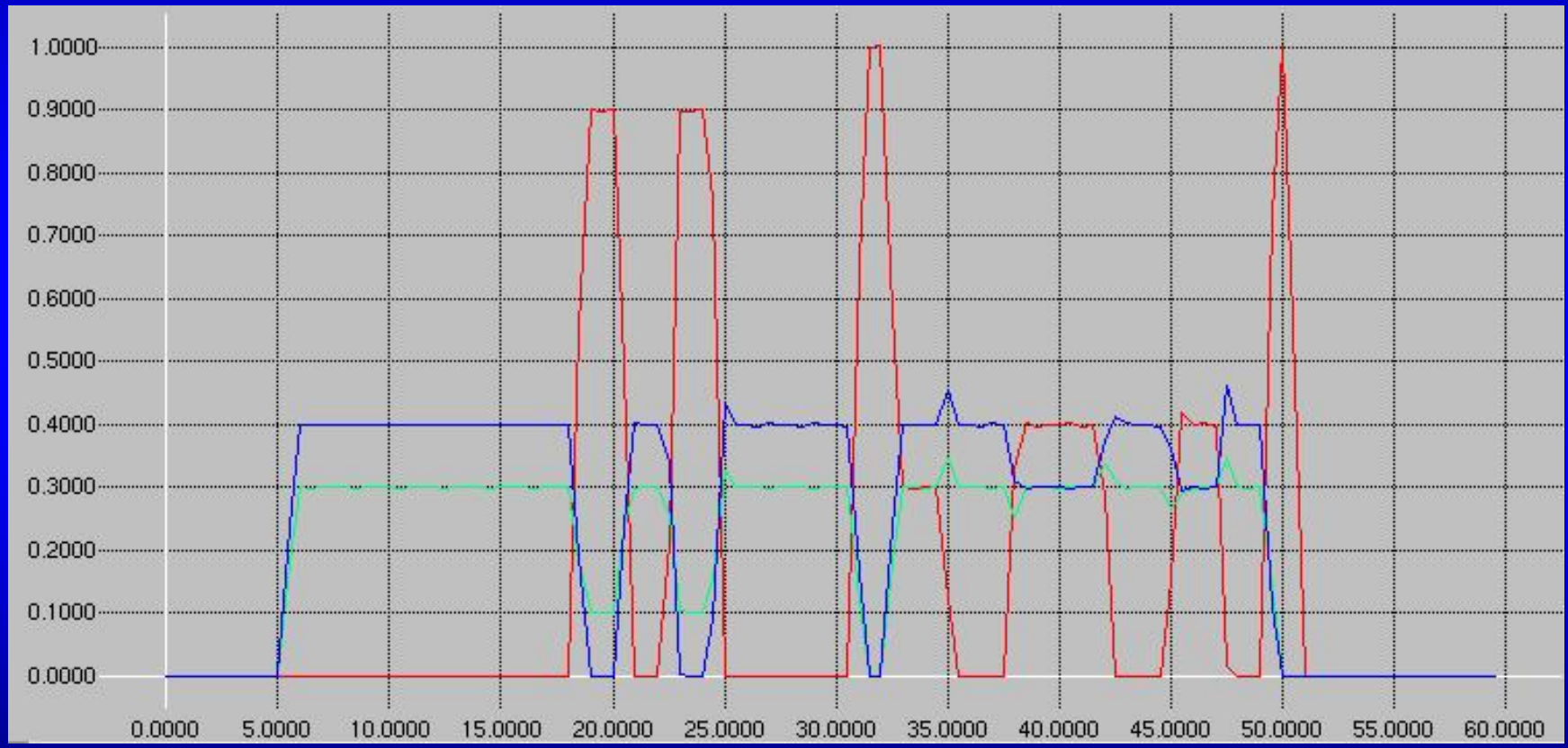
: Trusted Routers

NS-2 Simulation Results

- Implement first prototype in ns-2
- Random spoofed IP and random spoofed TTL Generator
- Only filter based on TTL and IP range
- Type of Attacker
  - Single source (1 Mbps)
  - Multiple sources (6 of 160 Kbps)
- Two flow of normal traffics (400 Kbps and 300 Kbps)

Single Attack Filtering
(NS-2 Simulation Results)

Traffic (Mbps)

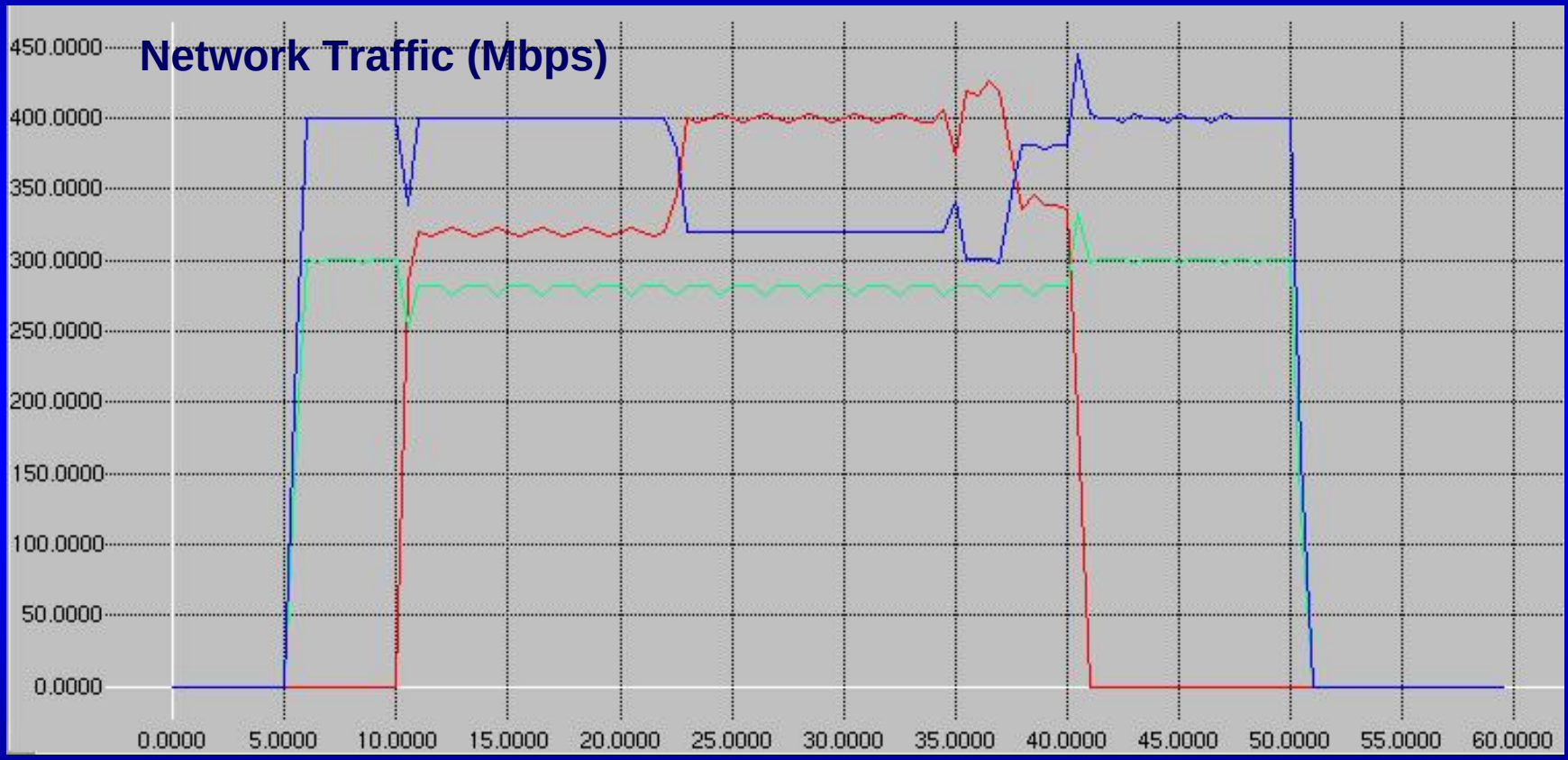


Time (Seconds)

Red: DoS Traffic

Blue/Green: Normal Traffic

Filtering of DDoS Attacks from Multiple Sources (Simulated Results)

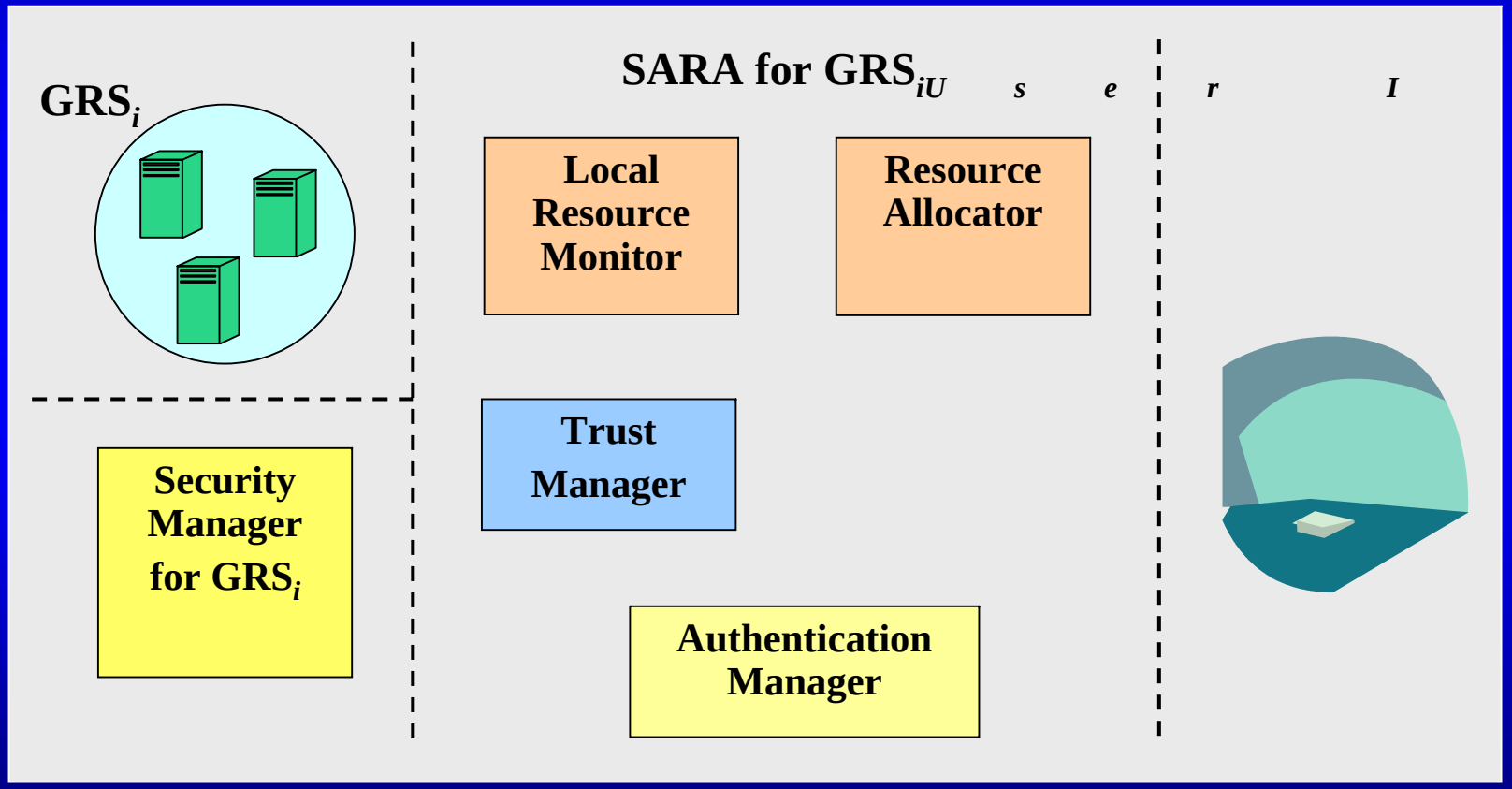


Time (Seconds)

Red: DDoS Traffic

Blue/Green: Normal Traffic

SARA: A Trust Model for Securing Grid Resources Allocation



Example: Allocating Resources from Two Grid Sites

Application Demand: (P_o, T_o, C_o) = (4Tflops, 0.6, $2.25M)

Resource Sit No. 1: R_1 = (1.6Tflops, 0.8, $500K, 6 hosts)

Resource Sit No. 2: R_2 = (1.2Tflops, 0.7, $220K, 5 hosts)

Objective function (Integer Programming):

$$P = t_1 p_1 x_1 + t_2 p_2 x_2 = 0.8 \times 1.6 x_1 + 0.7 \times 1.2 x_2 = 1.28 x_1 + 0.84 x_2$$

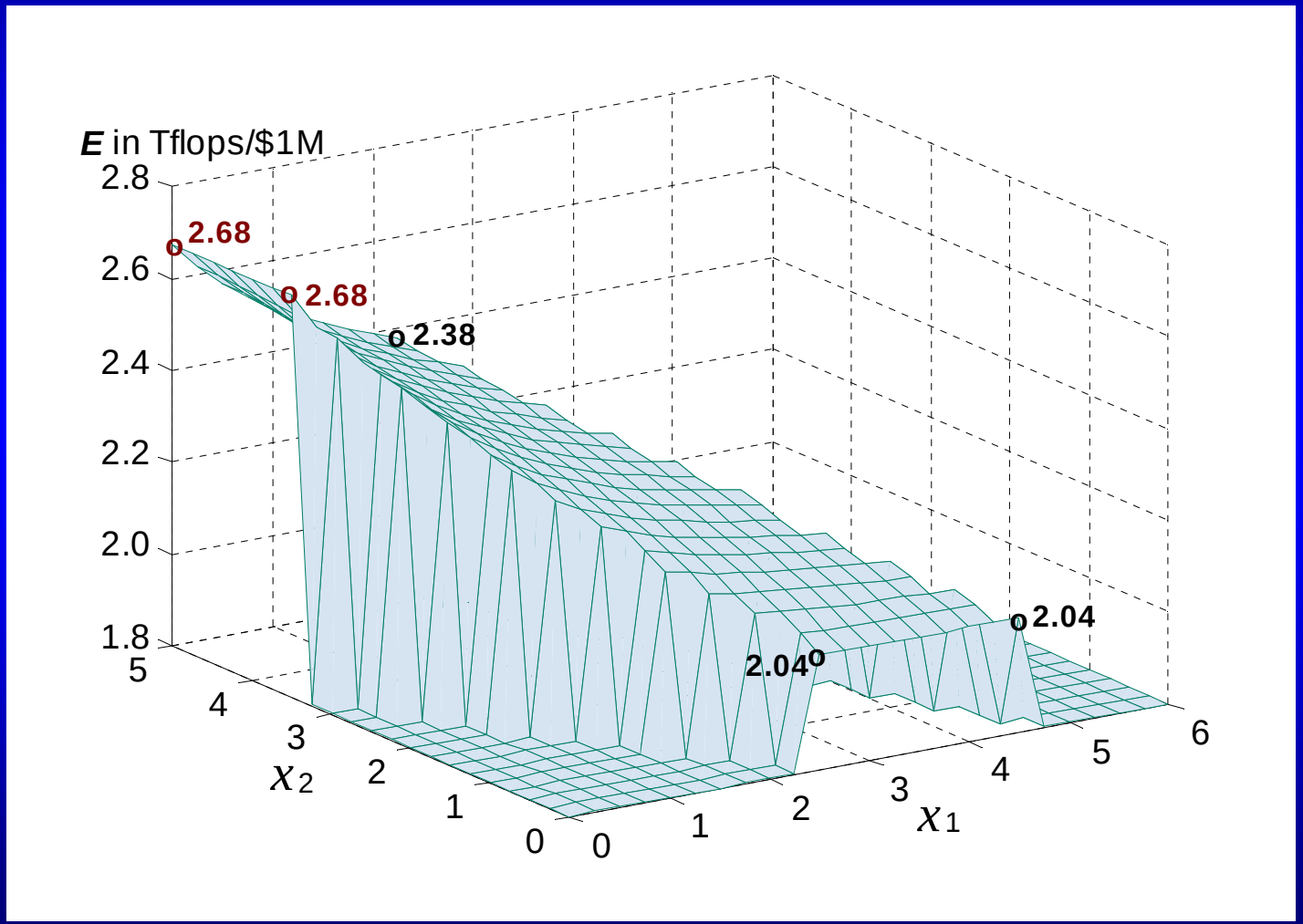
Subjective to the following constraints:

$$c_1 x_1 + c_2 x_2 = 500 x_1 + 220 x_2 \le \$2,250K$$

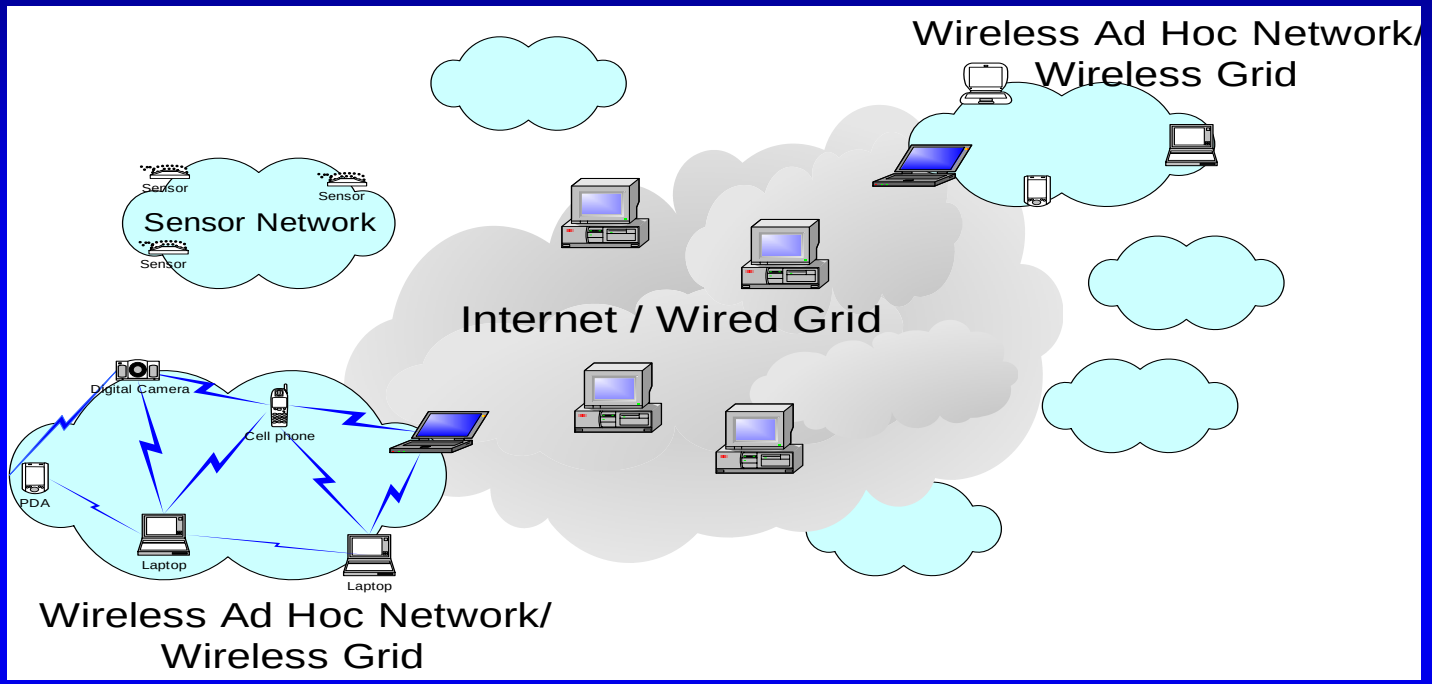
$$p_1 x_1 + p_2 x_2 = 1.6 x_1 + 1.2 x_2 \ge 4\text{Tflops}$$

$$0 \le x_1 \le 6 \text{ and } 0 \le x_2 \le 5$$

Plot of the performance/cost ratio *E* for allocation of server hosts from two resource sites. Two optimal allocations result in a peak *E* = 2.68 Tflops/$1M

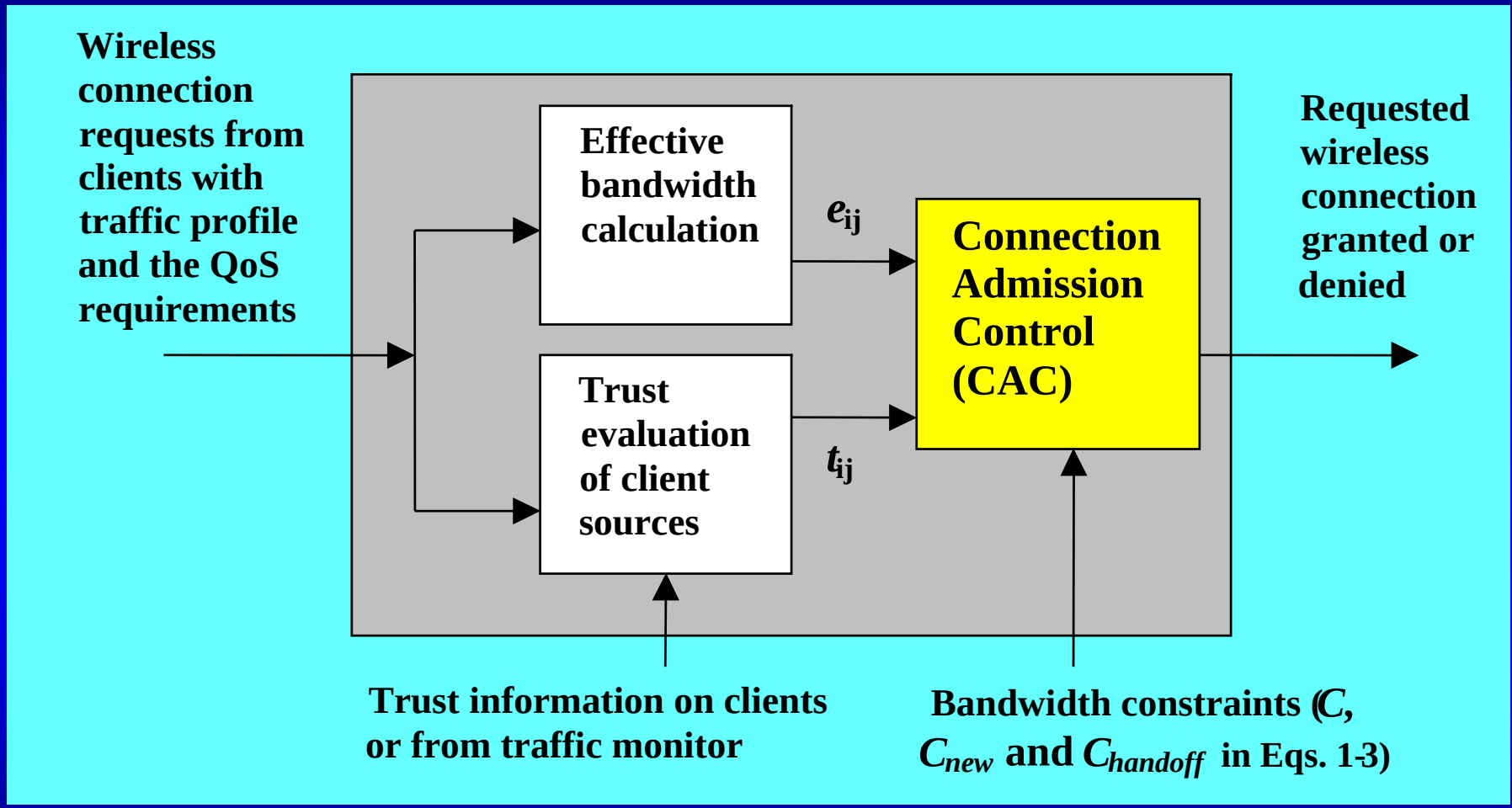


Wireless Access Control of Grid Resources



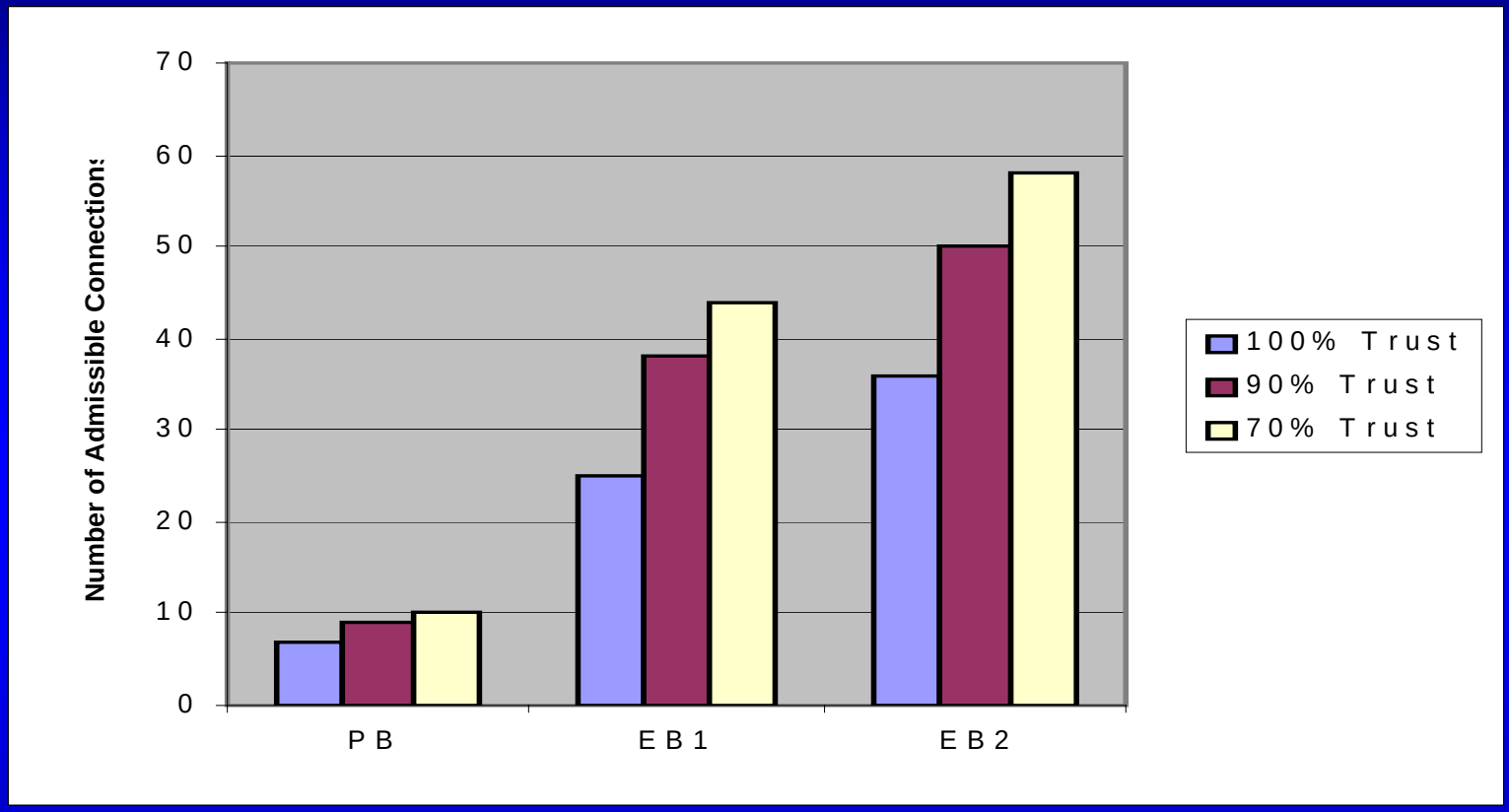
- Air interfaces, admission control, disconnection handling, wireless PKI, security binding, and QoS all demand extensive R/D
- The GridSec VPN supports both wired and wireless communications in distributed cluster, grid , and pervasive applications

The Architecture for Wireless Connection Admission Control



Allocate the bandwidth to satisfy the given QoS and security requirements

Maximum Number of Admissible Connections



EB1: Effective bandwidth method with 0.1% loss probability and EB2: Effective bandwidth method with 1% loss probability), PB: Peak bandwidth allocation method

Integrating Network-Based Distributed Computing Paradigms

Attributes	Cluster Computing	Grid Computing	Pervasive Computing
Networking	**System- or Local-Area Networks**	**Internet or Wide Area Network**	**Wireless LAN, GSM, CDMA Networks**
Communication Protocols	Mostly TCP/IP	IP/ATM, DNS, PKI, VPN	WAP : Wireless Application Protocol
Operating System	Most UNIX and Windows variants	Most UNIX, Windows variants	Windows CE, Palm OS, JavaCard
Environment and Software	**MPI, PVM, Score, Codine**	**GLOBUS, CONDOR, NetShield**	**Jini, UPnP, Bluetooth,**

Conclusions:

- GridSec for protecting distributed resources
  - Security-assured resource allocation (SARA)
  - Local resources fortified with NetShield library
  - Remote processing through GridSec VPN tunneling
- Automated intrusion detection and response
  - Generating anomaly detection rules to build IDS
  - Adaptive intrusion response through risk assessment
  - Priority defense against DDoS and flood attacks
- Continued research tasks and future directions:
  - Testing SARA and NetShield on GridSec testbed
  - Optimize the GridSec VPN architecture
  - Explore wireless Grid computing technology
  - Integrating pervasive, cluster, and Grid computing

Recent Reports and GridSec Papers:

1. K. Hwang, et al, " GridSec: A Distributed VPN/IDS Architecture for Securing Grid Computing ", Tech. Report, Internet and Grid Computing Lab., Univ. of S. Calif., Dec. 2003 (in preparation)
2. S. Song, K. Hwang, and R. Rajbanshi, "Security-Assured Resource Allocation for Trusted Grid Computing", submitted to *IPDPS- 2004*, October 16, 2003
3. M. Qin and K. Hwang, "Effectively Generating Frequent Episode Rules for Anomaly-based Intrusion Detection", submitted to *IEEE Symposium on Security and Privacy*, Nov.3, 2003
4. Y. Kim and K. Hwang, "Secure Admission Control for Resolving Wireless Congestion in Grid Computing ", submitted to *IEEE Internet Computing Magazine*, Nov.27, 2003

GridSec Research Team at USC and our International Collaborators:

- Sponsored by a NSF/ITR Research Grant in the USA
- Principal Investigator: Kai Hwang at USC

  Co-PI: Clifford Neuman at Information Science Institute, USC
- Post-doctorial Researchers at ISI/USC

  Dr. Tatyana Ryutov and Dr. Dongho Kim
- Research Assistants at USC EE and CS Departments:

  Min Qin, Shanshan Song, Yongjin Kim, Rakesh Rajbanshi, Ching-Hua Chuan, Gurpreet Grewal, Mikin Macwan, Narayana Jayaram, Yushun Zhang, Rohil Tripathi, ...
- International Collaborators:

  Prof. Michel Cosnard of INRIA, France

  Dr. Zhiwei Xu of Chinese Academy of Sciences

  Dr. Rajkumar Buyya of Melbourne Univ., Australia