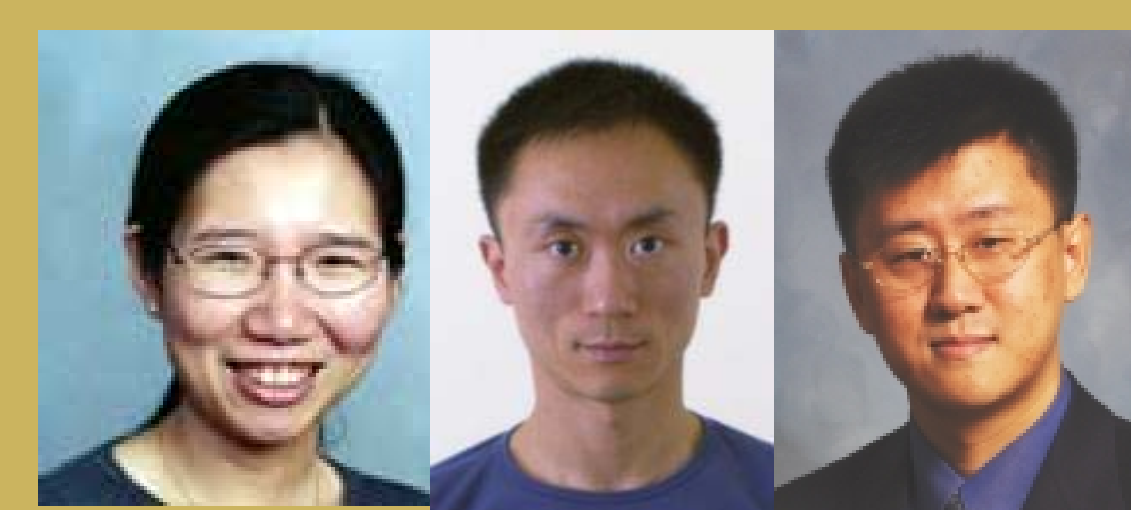


# Automatic Validation, Optimization, & Adaptation of Distributed Firewalls



Chen-Nee Chuah, Hao Chen, and Zhendong Su, <http://www.ece.ucdavis.edu/rubinet/fireman.html>

## Project Goals

- Policy checking and validation for distributed firewall configurations (same or multiple routes) to ensure security
- Traffic-aware optimization and adaptation of firewall configurations for improved performance and efficiency

## Real world applications

- Firewall is effective as network perimeter defense only if configured correctly. [Wool'04] study found multiple misconfigurations in 37 firewall rule sets.
- We develop **FIREMAN**, a static analysis toolkit to audit firewall configurations before deployment or rule-updating.
- We develop an adapt rule-placement based on real traffic statistics to minimize processing delay

Access Control List: core of firewall configs.

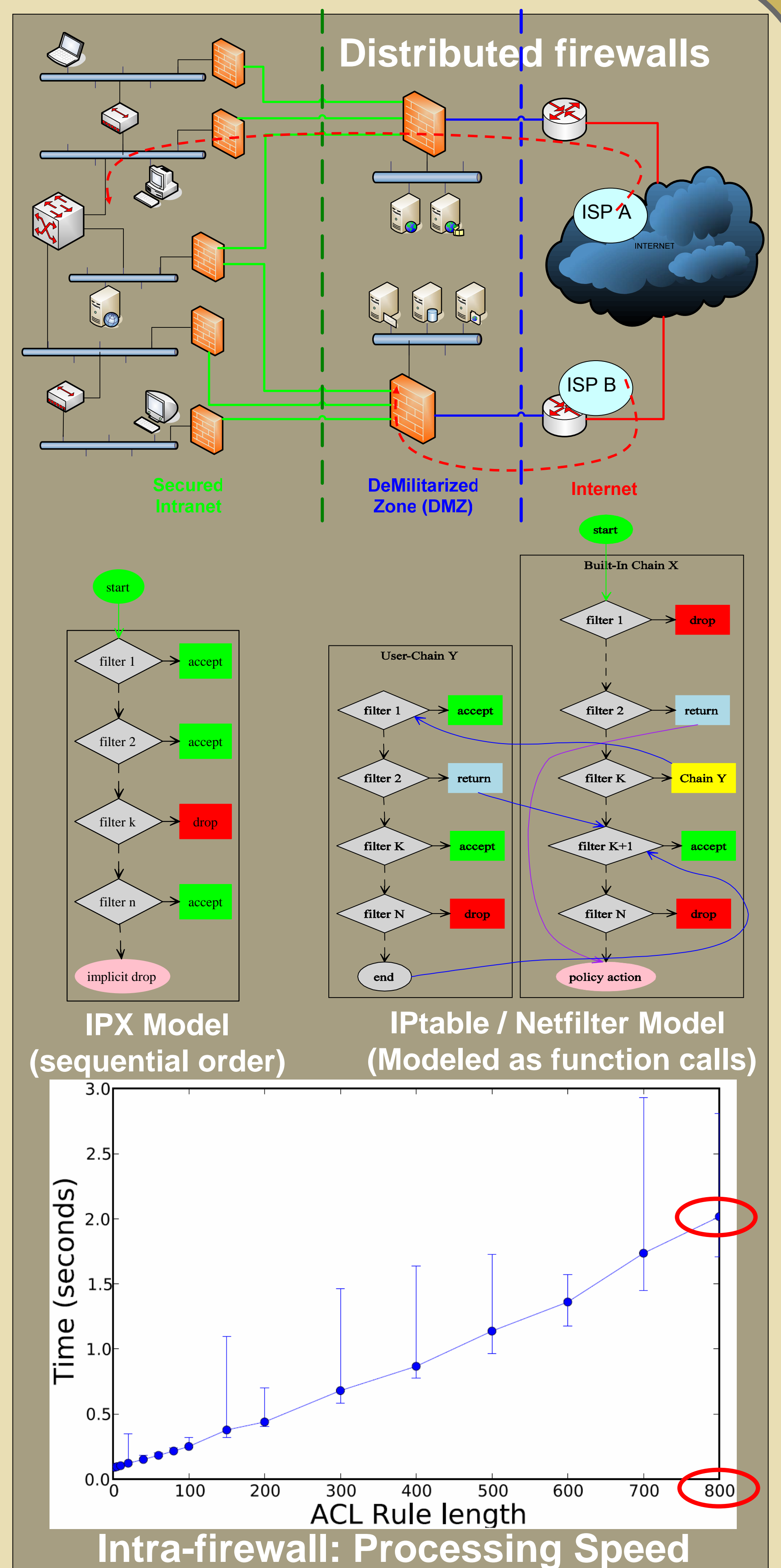
- Individual rules:  $\langle P, action \rangle$   
**P**: A predicate matching packets 5-tuple  $\langle proto, sip, spt, dip, dpt \rangle$   
**action**: accept, deny, chain-Y, return

Types of misconfigurations

- Type 1: Policy Violations
- Type 2: Inconsistencies  
 – Shadowing, Generalization, and Correlation
- Type 3: Inefficiencies

Static Analysis Algorithm & Implementation

- Control flow analysis (complex chain  $\rightarrow$  simple list; topology  $\rightarrow$  ACL graph)
- Check single firewall, inter-firewall, ACL root
- Implement using binary decision diagram
  - Efficient representation of random set of IP packets
  - Fast set operation



Intra-firewall: Processing Speed

FW	# ACLs	# Rules	# Violations Found		
			Policy	Inconsistency	Inefficiency
PIX1	7	249	3	16	2
BSD1	2	94	3	0	0
PIX2	3	36	2	0	5

## Approach and Impact

### New approach

- Model individual and distributed firewalls
- Classification of mis-configurations
- **Static analysis** algorithm to detect misconfigurations and an implementation based on **BDD - FIREMAN**
- Features: *full coverage, scalable, efficient*

### Research Impact

- Effective tool for network administrators to audit firewall configurations
  - transfer of technology to campus IT group
  - prototype used in security class at UCB
- Build the foundation for validating end-to-end reachability and other security policies