

Alternate representation of NIDS/NIPS signatures for fast matching



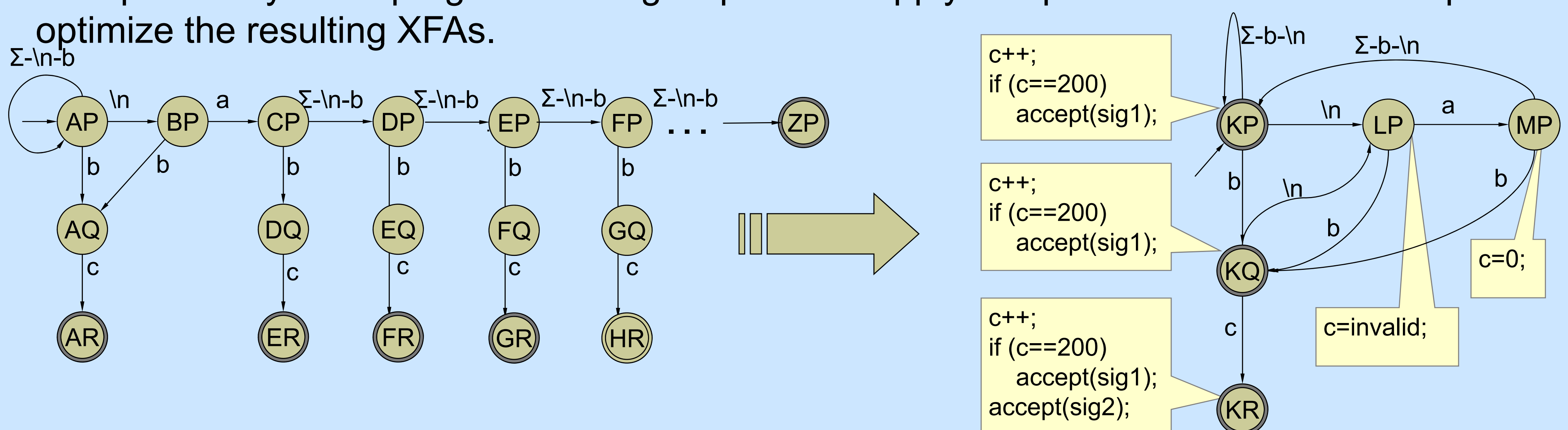
Cristian Estan (PI), Somesh Jha (co-PI) – University of Wisconsin-Madison

Motivation

Network Intrusion Detection Systems (NIDS) protect networked computing resources from unwanted or malicious traffic. NIDS are between a rock and a hard place: increasing traffic volume, increasing signature complexity, and increasing number of signatures means few cycles available for detection. Current matching techniques require too much time or too much memory (or both!). Goal: Develop signature matching mechanisms with smaller memory footprints and time requirements.

Approach

Use alternate signature representation that employs bits, counters, and other mechanisms to track inspection progress. Bit and counter values reside in an auxiliary “scratch memory” and are updated by small programs during inspection. Apply compiler construction techniques to optimize the resulting XFAs.



Results

Measure XFA space savings and performance penalty using commercial quality signatures. Experiments include 700+ signatures for FTP, SMTP, and HTTP protocols, drawn from Sourcefire and Cisco IPS rule sets. Compare XFAs to other inspection mechanisms: DFAs, NFAs, and multiple DFAs (mDFAs). For each inspection mechanism, combine signatures on a per-protocol-group basis.

XFA representation yields fast inspection with small memory usage. XFAs 10 times smaller and 5 times faster than best alternatives for most complex rules. Space-time tradeoff: perform more work per byte (we need more time) in exchange for a drastic reduction in space.

