USC
UNIVERSITY
OF SOUTHERN
CALIFORNIA

Introduction to Intrusion Detection Systems

Zachary K. Baker and Viktor K. Prasanna
University of Southern California
June 22, 2004

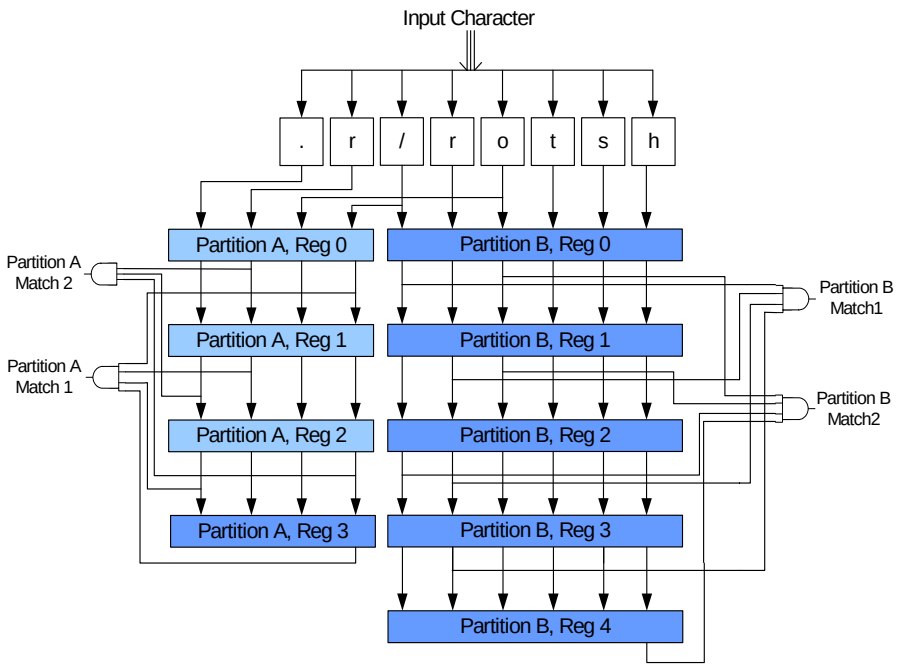
Introduction

- All incoming packets are filtered for specific characteristics or content,
- Databases have thousands of patterns requiring string matching

- We can achieve 10 Gb/s and higher rates desired
  - Provided by pipelined, streaming architectures,
  - Reduction of redundancy,
  - Efficient recoding,
  - Reduction of routing through pipeline partitioning

Efficient Matching Design

- Pre-decoding into individual characters allows for high time and area efficiency
- Pipelining allows for reduced interconnect latency and separation of related patterns into prefix-linked modules



Incremental Architecture Synthesis

- Module-based, partitioned pipelines allow for several independent modules connected only by controller
  - Changes in one module do not necessarily require recompilation of other modules
    - Significantly reduce place and route costs
    - Cost for changing rules in one of *k* partitions:
      overhead + 1/k