Parallelized Network Security Protocols

Erich Nahum, David Yates,
Sean O'Malley, Hilarie Orman, and Richard Schroeppel

University of Massachusetts
University of Arizona

Talk Outline

Motivation

Parallelism in Network Protocols

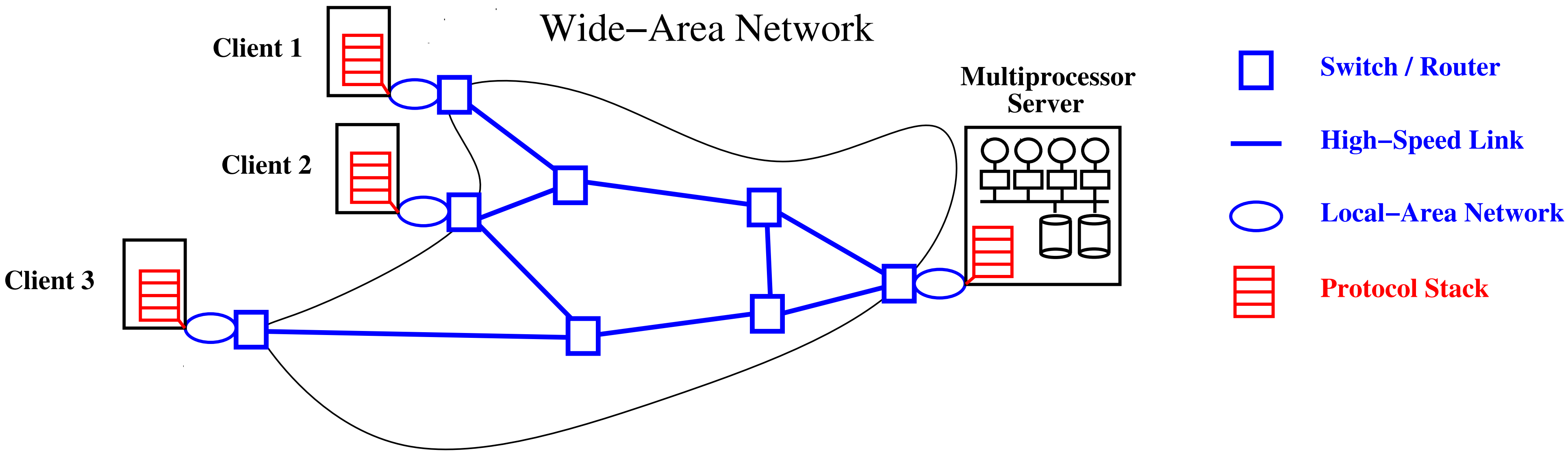
Implementation and Experiments

Packet-Level Parallelism

Connection-Level Parallelism

Summary

Motivation



Networked Information Servers

- World-Wide Web, Video, Image, File servers
- Large amounts of information

$\Rightarrow$ *Determine appropriate networking support for shared-memory multiprocessor servers*

Support for Secure Servers

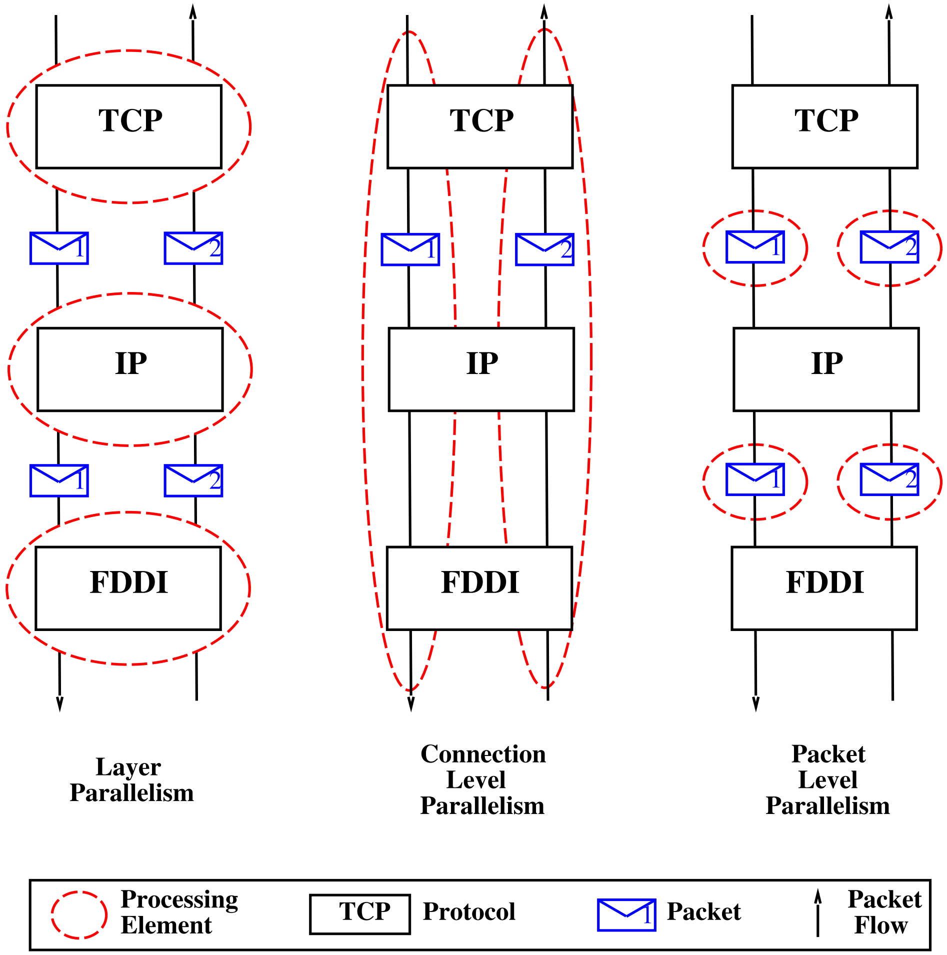
Security and privacy growing concerns

- Commerce on the Internet
- Multiple standards: secure IP, SHTTP, SSL

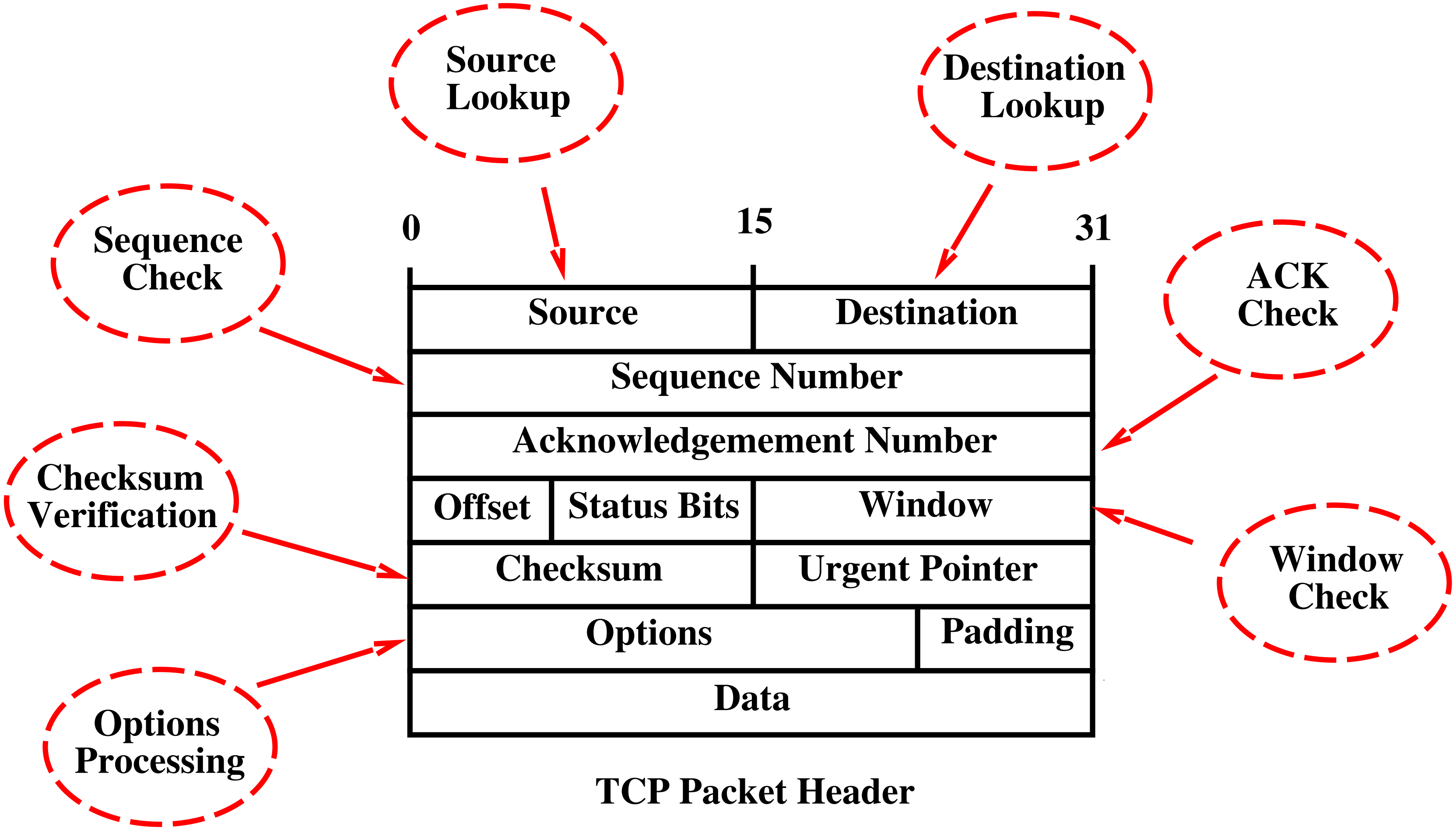
Crypto is slow, but still needs to be in software

- Multiple, evolving standards
- Multiple protocols in each standard
- Software cheaper, flexible
- Certain algorithms won't benefit from hardware

Exploiting Parallelism

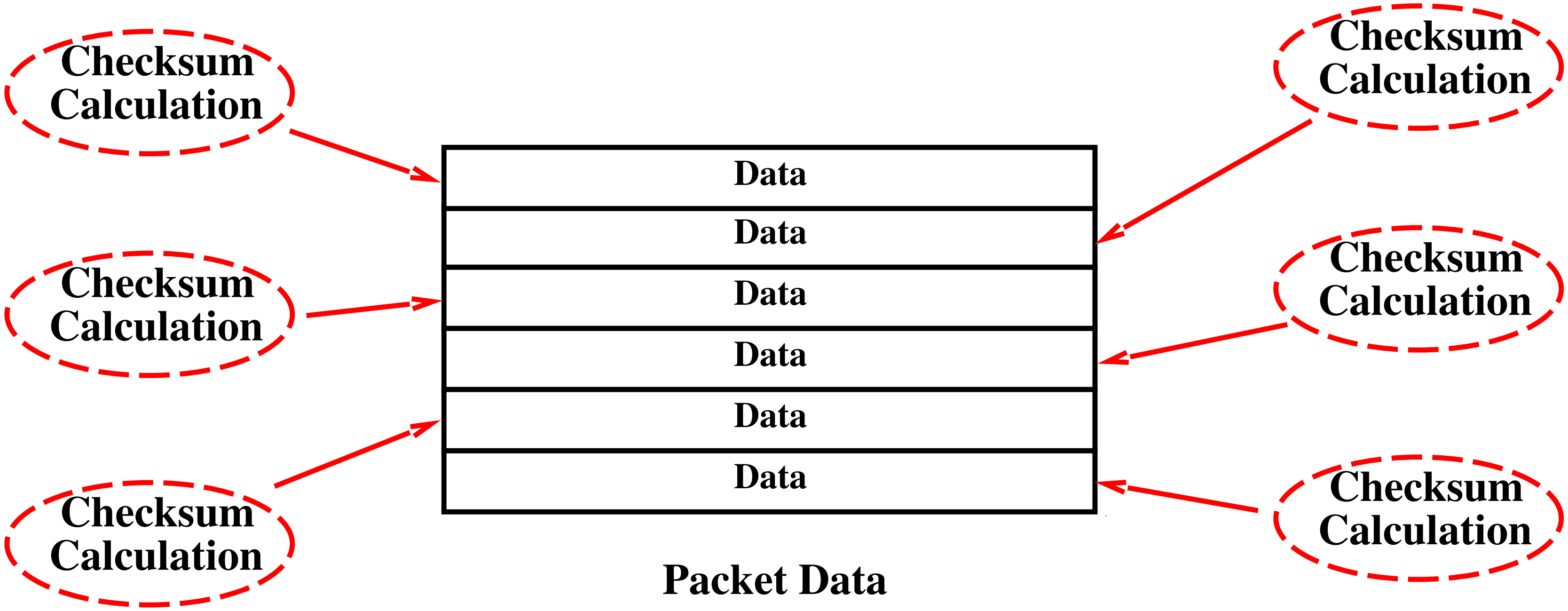


Functional Parallelism



TCP Packet Header

Data-Level Parallelism



Research Issues

What's the impact of cryptographic protocols?

What's the available parallelism?

- Packet-Level Parallelism (PLP)
- Connection-Level Parallelism (CLP)

Research Infrastructure

SGI Challenge multiprocessor (12 100 MHz R4400)

Parallelized x-kernels (PLP & CLP)

Parallelized Internet-based protocol stacks:

- TCP/IP
- TCP/MD5/IP
- DES/TCP/MD5/IP
- 3-DES/TCP/MD5/IP

In-memory drivers

Experimental Methodology

Throughput tests

Isolated machine

30 second runs, 30 second warmup

Avg. of 10 runs, 90 % conf. intervals

PLP: Single-connection tests

CLP: 12-connection tests

Packet-Level Parallelism (PLP)

Implementation:

- Access to data structures serialized via locks
- Threads contend for them

Advantages:

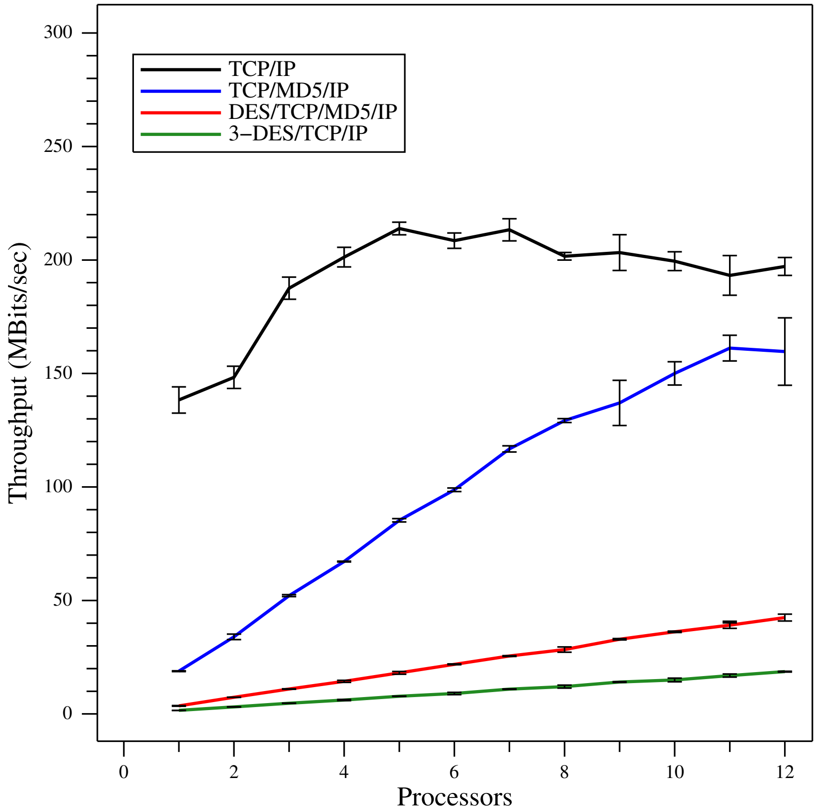
- No restrictions on packet processing
- Good available parallelism for UDP

Disadvantages:

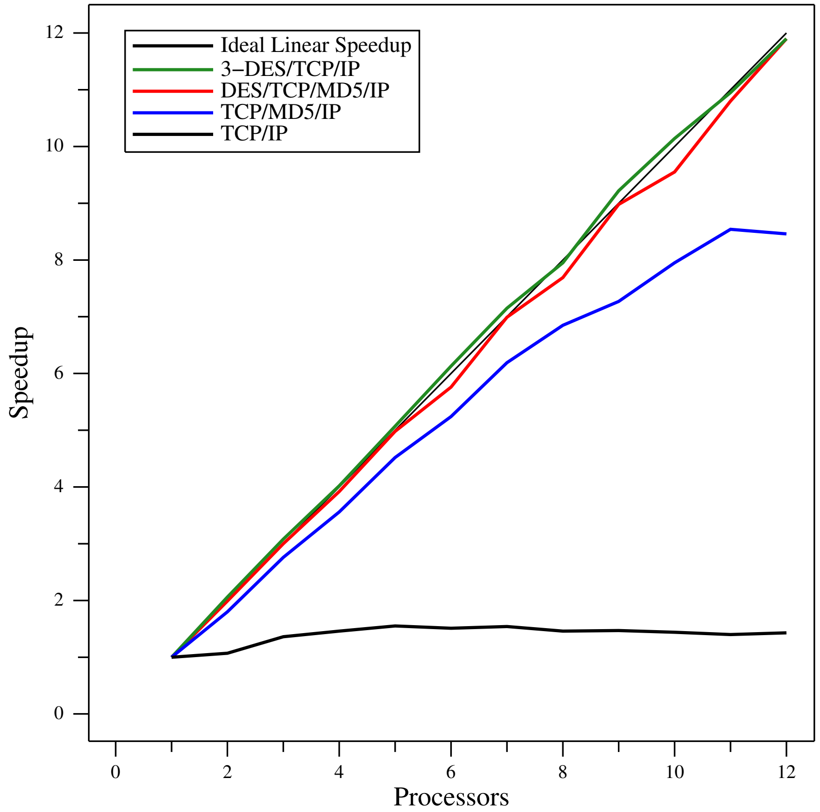
- Limited single-connection parallelism for TCP

PLP Results

Throughputs



Speedup



Much greater available parallelism

Why does speedup change?

Protocol Stack	Send Side	Inc. Cost	Recv Side	Inc. Cost
TCP/IP	236		189	
TCP/MD5/IP	1737	1500	1708	1519
DES/TCP/MD5/IP	8982	8746	9179	8990
3-DES/TCP/IP	21461	21225	21121	20932

Latency in usec.

Cryptographic processing happens outside scope of locks

Connection-Level Parallelism (CLP)

Implementation:

- Data structures replicated per-connection
- Demultiplexing done by packet filter

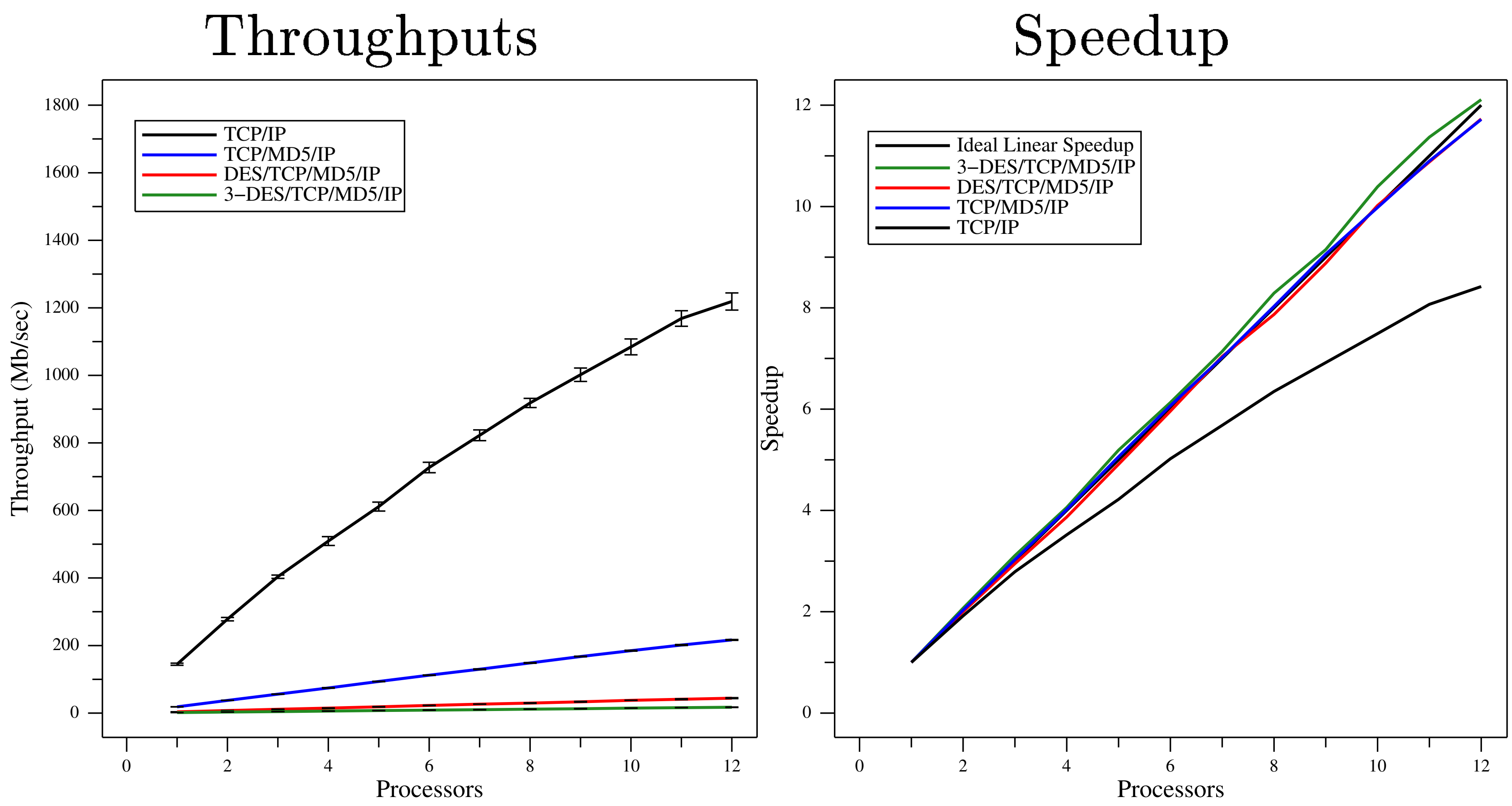
Advantages:

- Natural for large numbers of connections
- No synchronization on 'fast path'
- Good available parallelism for sufficient number of connections

Disadvantages:

- Traffic tends to be bursty

CLP Results



Greater available parallelism

Summary and Future Work

Results

- Parallelism is effective
- Available parallelism changes radically
- PLP exhibits linear speedup with DES
- CLP exhibits linear speedup with MD5

Future Work

- More fine-grained approaches to parallelism
- Connection setup and teardown