Dependable Private Virtual Networks

Dr. D. R. Avresky

Network Computing Lab

avresky@ece.neu.edu

Motivation

Within five years, it will be common to encounter networks, dedicated to a single

enterprise, which will be composed of tens of thousands of computers. Some of these networks (banking, medical, e-business, military, transportations) will run critical - mission applications . Failures will be considered as “normal” properties of these networks.

Motivation

The economic cost of downtime to Internet providers is substantial –millions of dollars per hour for brokerages and cridit card companies, hundred of thousands of dollars for online retailers and services like eBay. Indeed, Internet Week recently reported that 65% of the sites they surveyed had experienced at least one customer -visible outage during the previous six months, while 25% had experienced three or more.

Recovery-Oriented Compting

The challenge is to build computer networks, based on COTS , that are inexpensive, scalable and dependable. Private virtual networks are created by composing a complex set of hardware and software components that are heterogeneous and subject to continuous upgrade, replacement, and scaling their numbers.

Recovery-Oriented Computing

The systems are too complex to model formally , and reducing the failure rate of individual components may not substantially reduced the rate of overall system failures due to unexpected interactions between components. One may consider that failures are inevitable.

Recovery –Oriented Computing

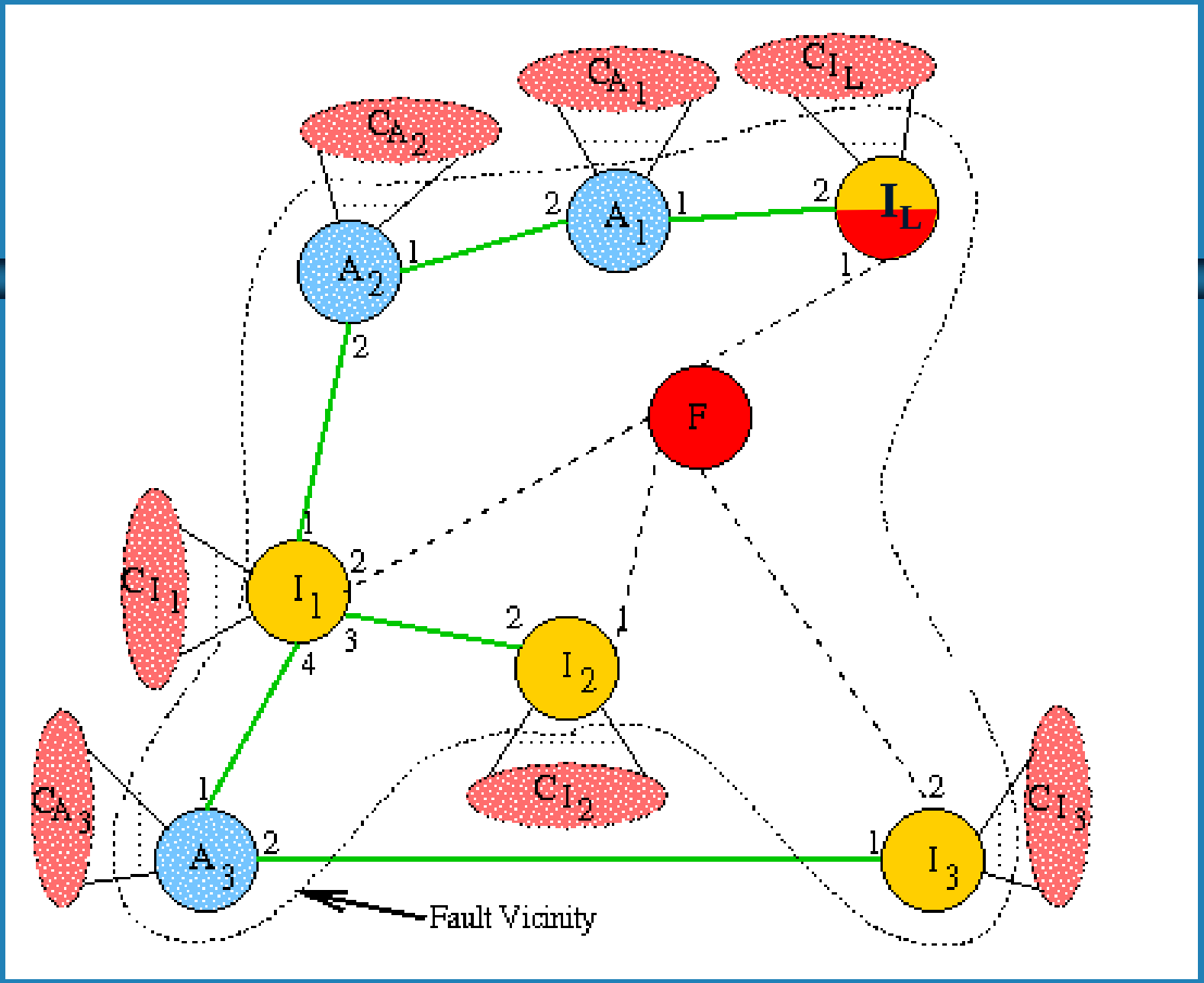
Having this in mind, we have to consider

detection and recovery-oriented computing, a technique for achieving high

availability that focuses on detecting and recovering from failures rather than preventing them entirely. The following techniques can be considered as a basis for this computing: redundancy and isolation; online self-testing and verification; support for problem diagnosis; and concern for human interaction with the system.

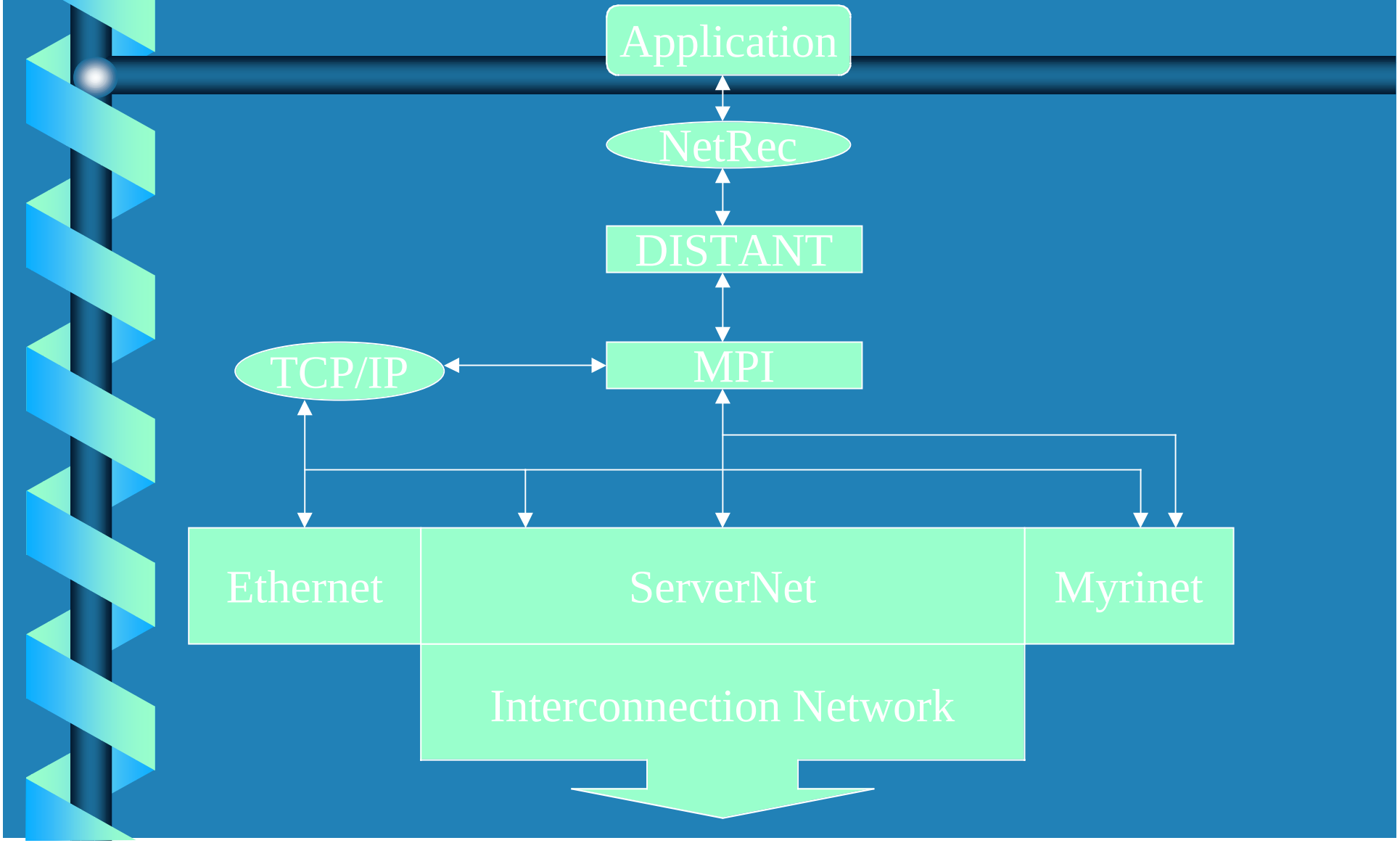
Motivation

High-speed computer networks (LAN, WAN or SAN) may change their topology due to switching off/on of routers and hosts or due to component failures. The purpose of this work is to specify and validate a novel approach for reconfiguring arbitrary network topology in a user transparent way, when node or links faults occur. The approach is applicable for private virtual high-speed computer networks (LAN , WAN), including wormhole-based system-area networks SAN.



Reconfiguration Example – F faulty node

Distributed Reliable Computing System Based on COTS



Seamless tasks execution

Based on the new NetRec approach, any application written in C++ can be executed correctly in the presence of failures. Without any changes , the application can use either TCP/IP or ServerNet , Myrinet , Giganet drivers and can be accomplished within Ethernet or SAN environment.

Validation with a real-life application

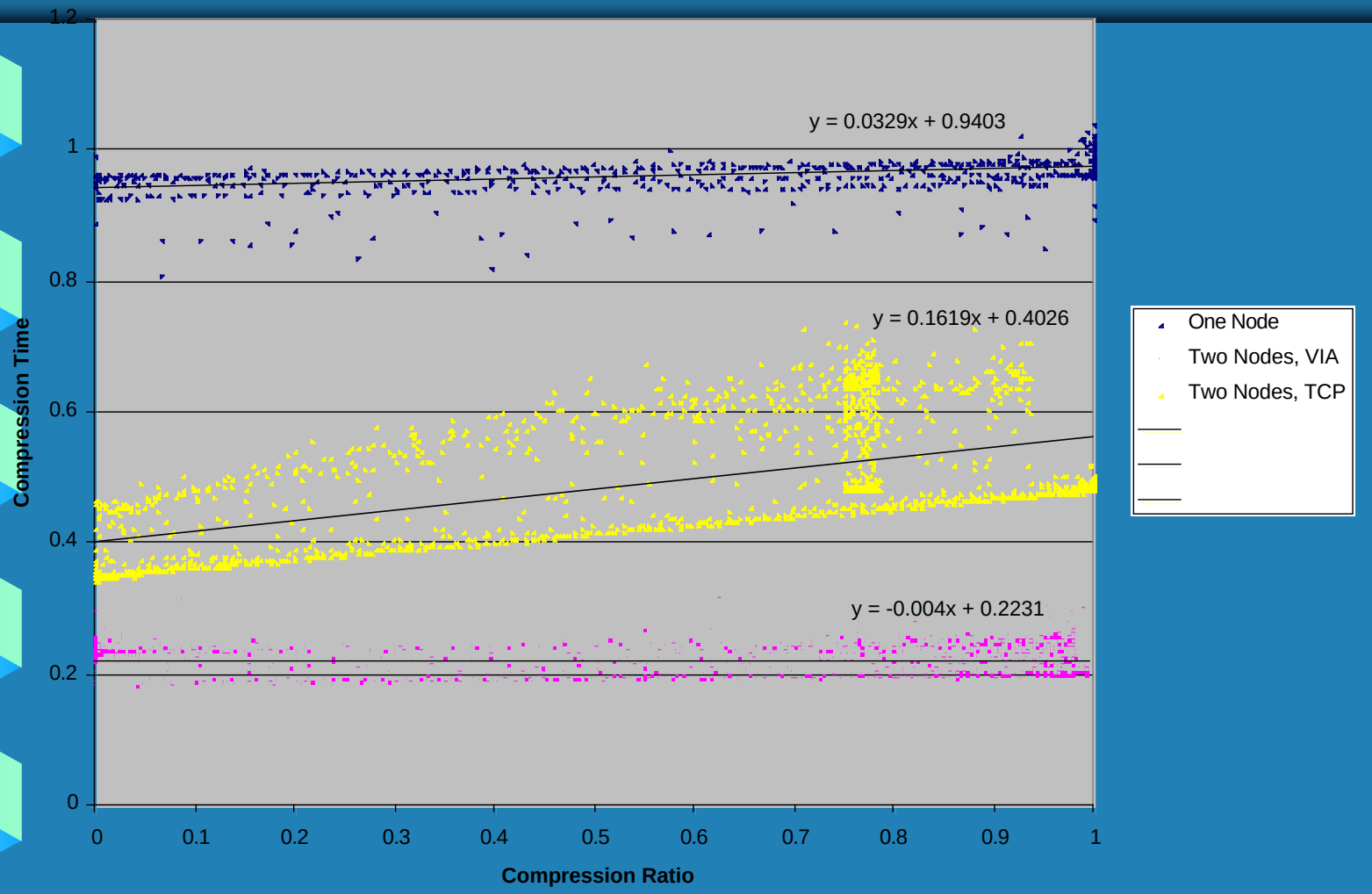
- Mapping of the Quad-Tree Data Compression algorithm onto fault-free topology –

{root II, leaf1-A1, leaf2-F,leaf3-I2 and leaf 4-I3}

- Mapping of the Quad-Tree Data Compression algorithm onto faulty topology (node F) –

{root-II, leaf1-A1, leaf2-A2,leaf3-I2 and leaf 4-I3}

Quad-tree Compression Algorithm (compression ratio vs. time)



Dependable Task Execution

The application can completely recover from the single and multiple process faults and deliver correct results by replacing the faulty process with one of the spare process and reassigning the lost task to it when it is necessary.

Dynamically Scaling Computer Networks

The NetRec approach does not stop the user traffic when new nodes are joining

the networks. The protocol only updates the routing tables of a small number nodes

and it is completely decentralized. Thus , the size of the Dependable Private Virtual Network can be scaled dynamically in order to meet the QoS requirements or in the case, when the node is

rejoining the network after recovery.