GARR

The Italian Academic & Research Network

www.garr.it

University of Rome "Tor Vergata"
Department of Electronics Engineering

NETWORKING GROUP

FairVPN, overlay topology construction tool to maximize TCP fairness

A framework for packet droppers mitigation in OLSR Wireless Community Networks

Francesco Saverio Proto

Giornata di incontro con i borsisti GARR, Roma, 23.02.2011

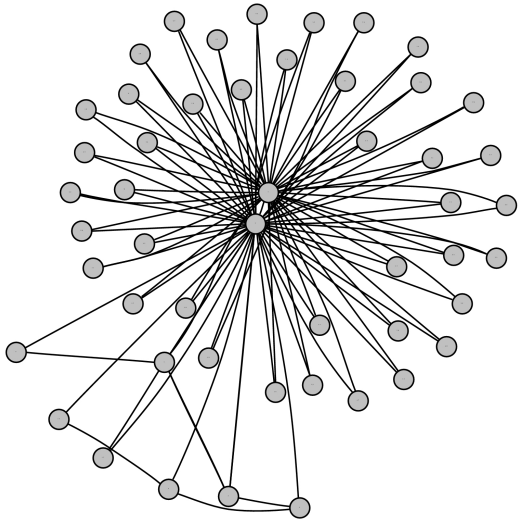
Consortium GARR

FairVPN

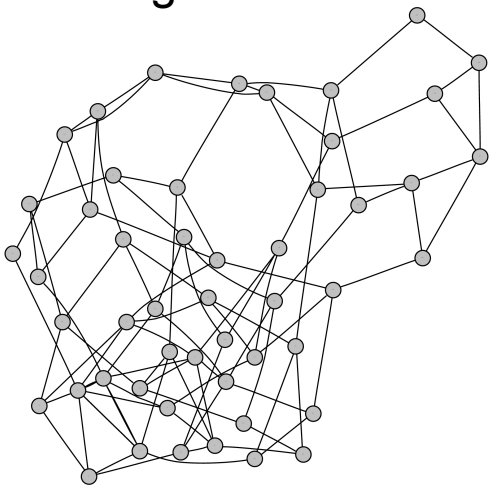
Overlay Networks: FairVPN

- Topology for Overlay VPN
- Goals:
  - Provide TCP fairness
  - Low Memory Consumption
  - Develop Prototype

- Roadmap:
  - Emulation (Netkit) ✓
  - Small real testbed (LiveCD) ✓
  - Large PlanetLab Testbed ✗
    - Virtual Distributed Ethernet ?



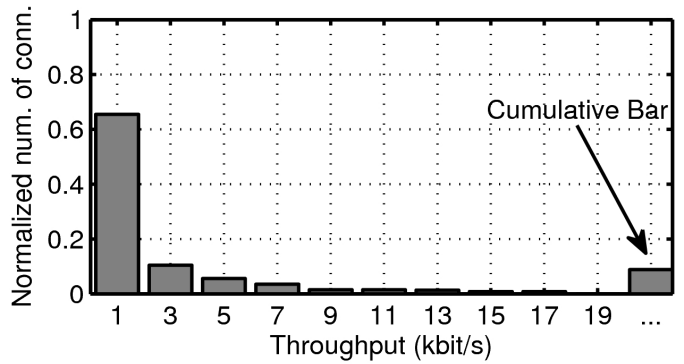
Short neighbor-selection

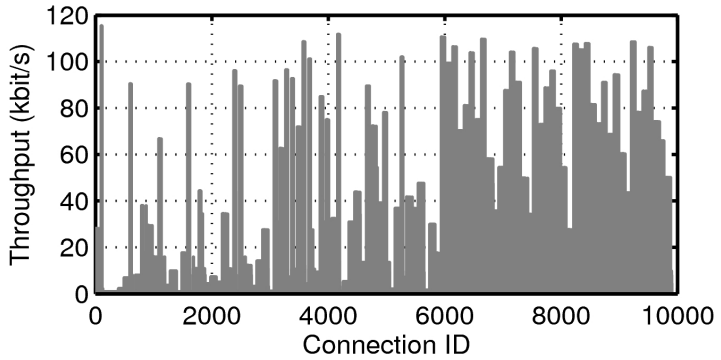


Short neighbor-selection

Throughput unfairness of short overlay

- Hub and Spoke or Full Mesh are unfeasible
- Building a partial mesh overlay with incremental approach
- How to build overlay ?
  - Short Overlay is unfair
  - Few very fast TCP connections
  - A lot of very slow TCP connections



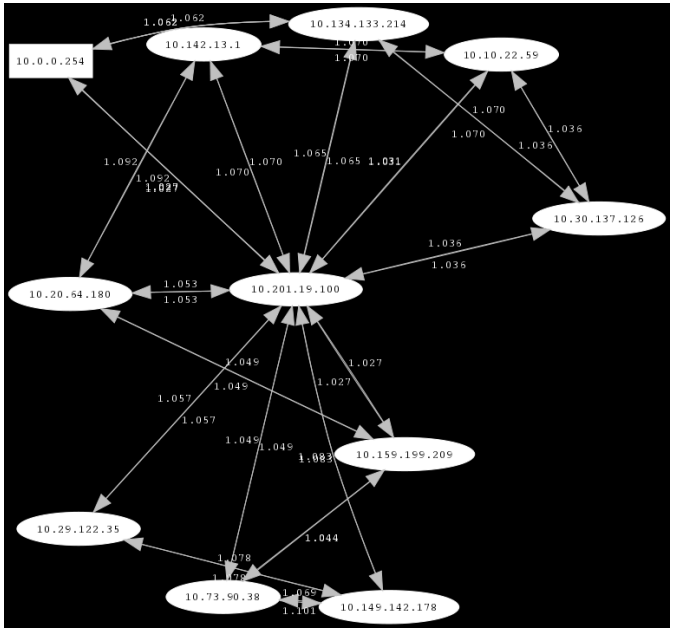


Implementation

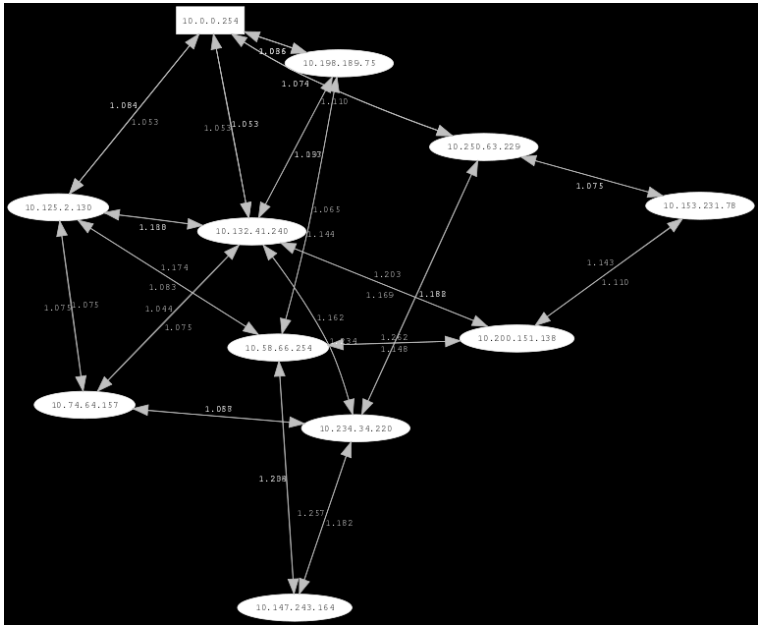
- FairVPN is a python script that:
  - Runs the FairVPN algorithm
  - Configures a (patched) TincVPN
    - Selects neighbours to "ConnectTo"
  - Configures the **OLSR** routing protocol
  - Starts tincd and olsrd
- Implementation available
  - http://minerva.netgroup.uniroma2.it/fairvpn
  - Presented at FOSDEM 2011
  - Tested on emulated network with Netkit
    - Just ~20 nodes to test implementation

Validation with Netkit

- We used netkit for testing, a UML emulator
  - http://wiki.netkit.org
- Short overlay VS Fair overlay:

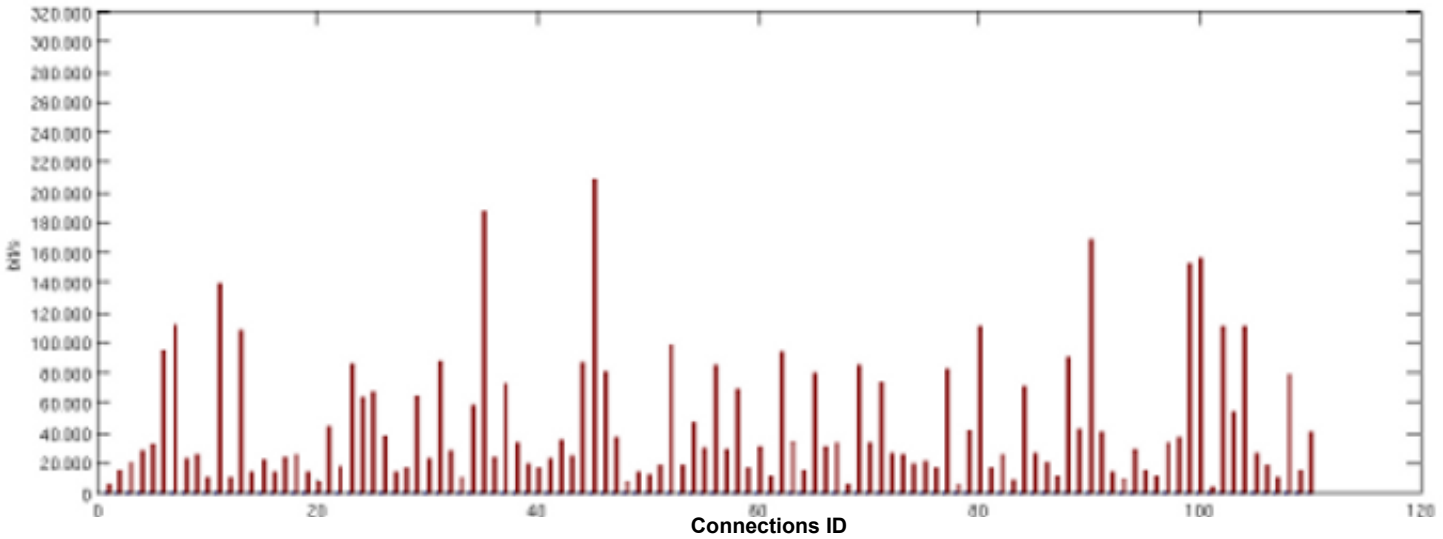


Topologia Short-overlay



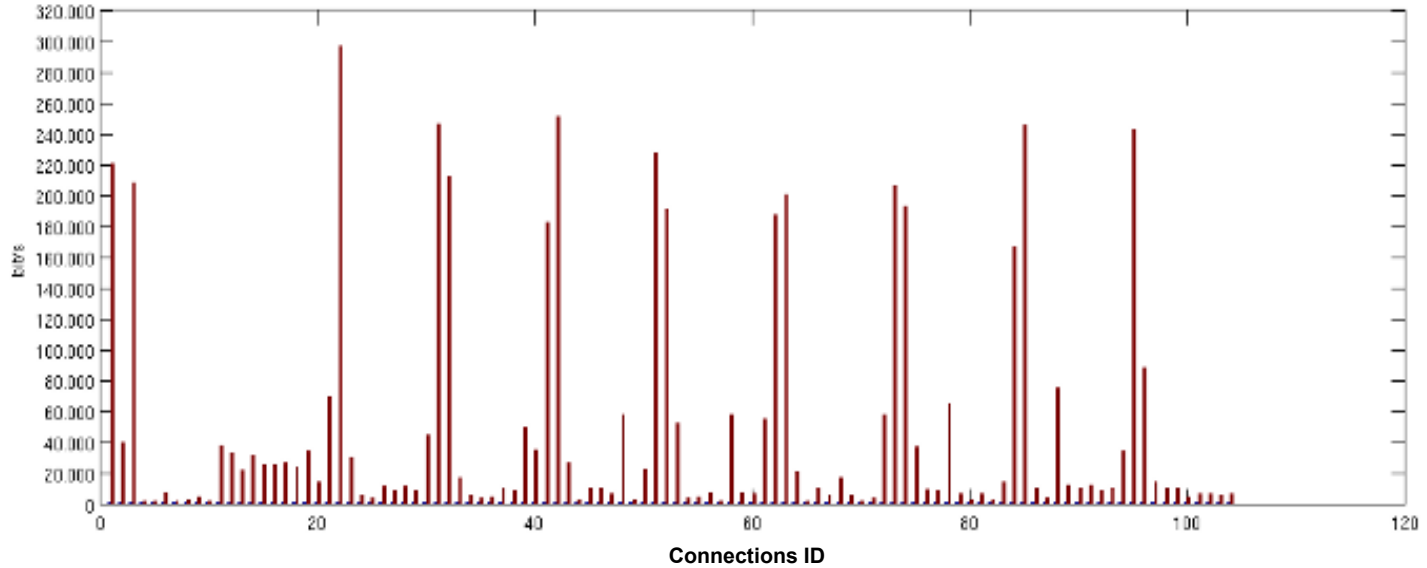
Topologia Fair-VPN

Results



FAIR TOPOLOGY

X=TCP connection ID
Y=Throughput

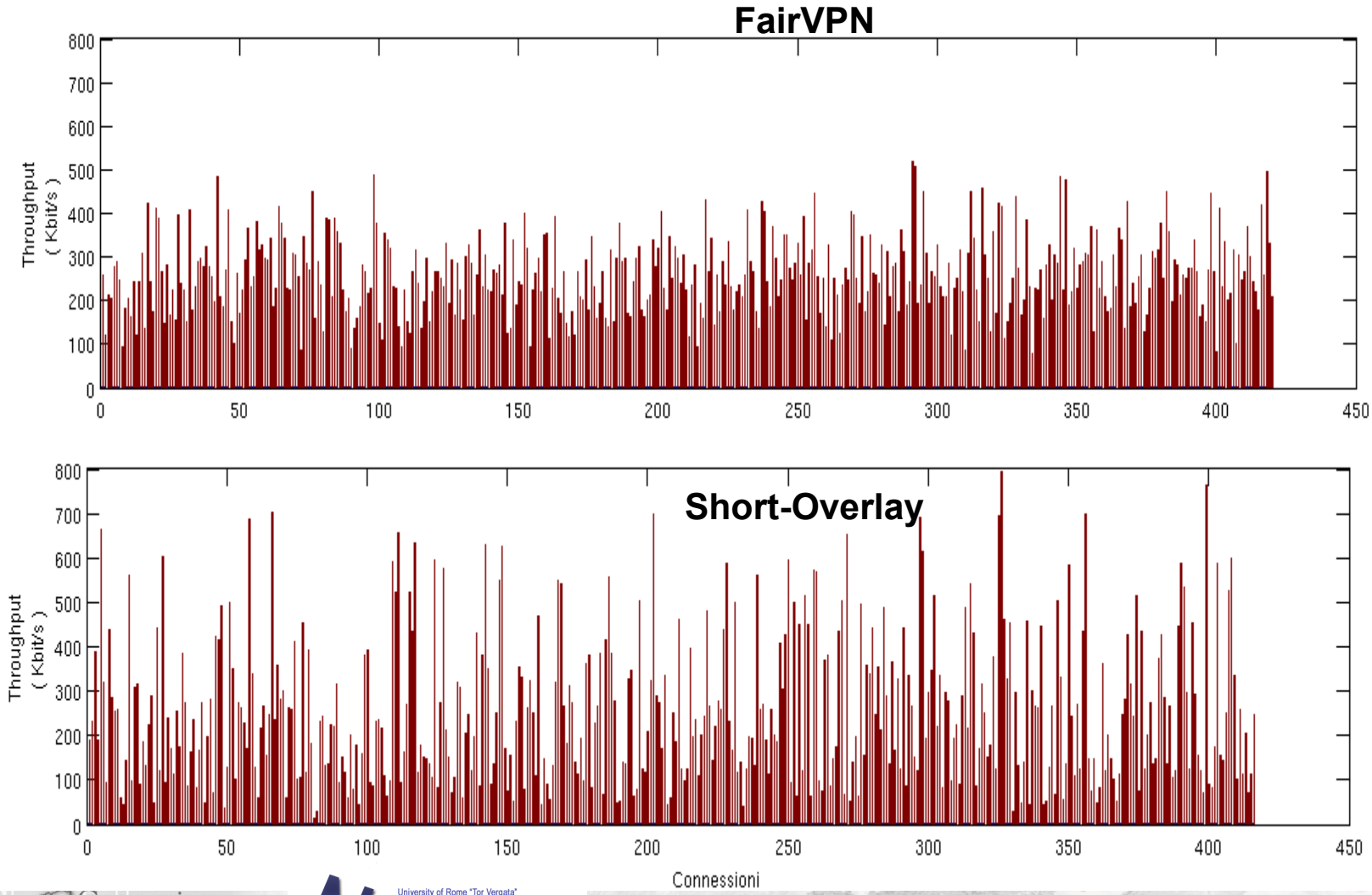


SHORT TOPOLOGY

X=TCP connection ID
Y=Throughput

Results

Same results with 21 nodes (420 connections)



Planet Lab / VINI

- PlanetLab is a group of computers available as a testbed for computer networking and distributed systems research.

- It was not possible to deploy FairVPN on Planet Lab or VINI
  - Linux Vserver Container Based virtualization limits access to Kernel routing tables and traffic control

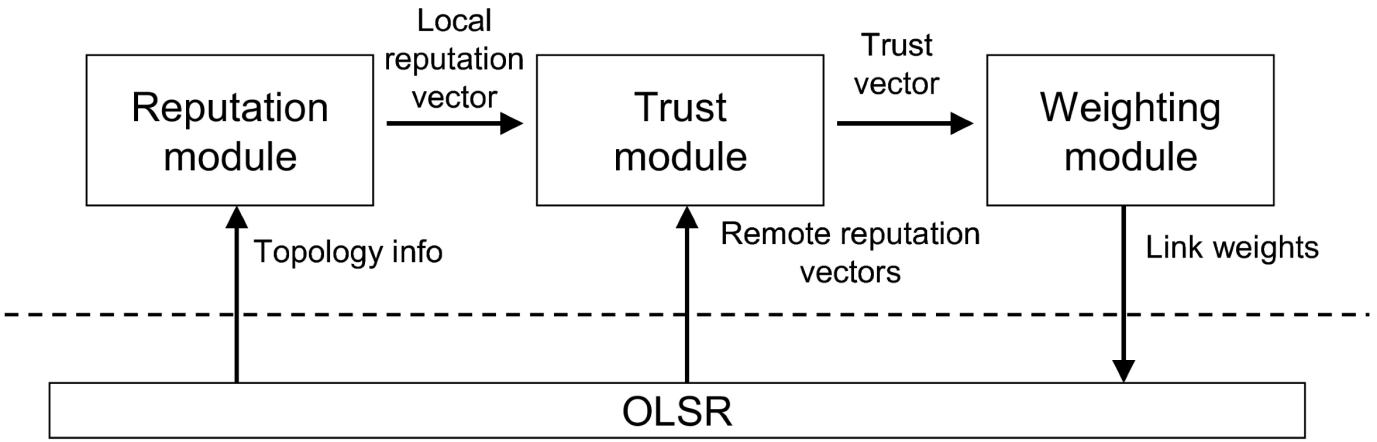
Trust Based Routing Framework

F. S. Proto, A. Detti, C. Pisa, G. Bianchi;
"A Framework for Packet-Droppers Mitigation
in OLSR Wireless Community Networks"
Articolo accettato ed in fase di pubblicazione su rivista ICC 2011

Trust Based Routing Framework

- Distributed networks
  - Every node is self-managed
  - Security policy cannot be enforced globally
- Scenarios
  - Overlay Networks applications
  - **Wireless Communities**
  - Spontaneous networks (smart devices)
- Wireless Communities
  - OLSR routing protocol
  - Decentralized management
    - Common faulty configuration of routers/firewalls leads to packet dropping attacks on the data plane
    - Attackers should be isolated by the routing plane

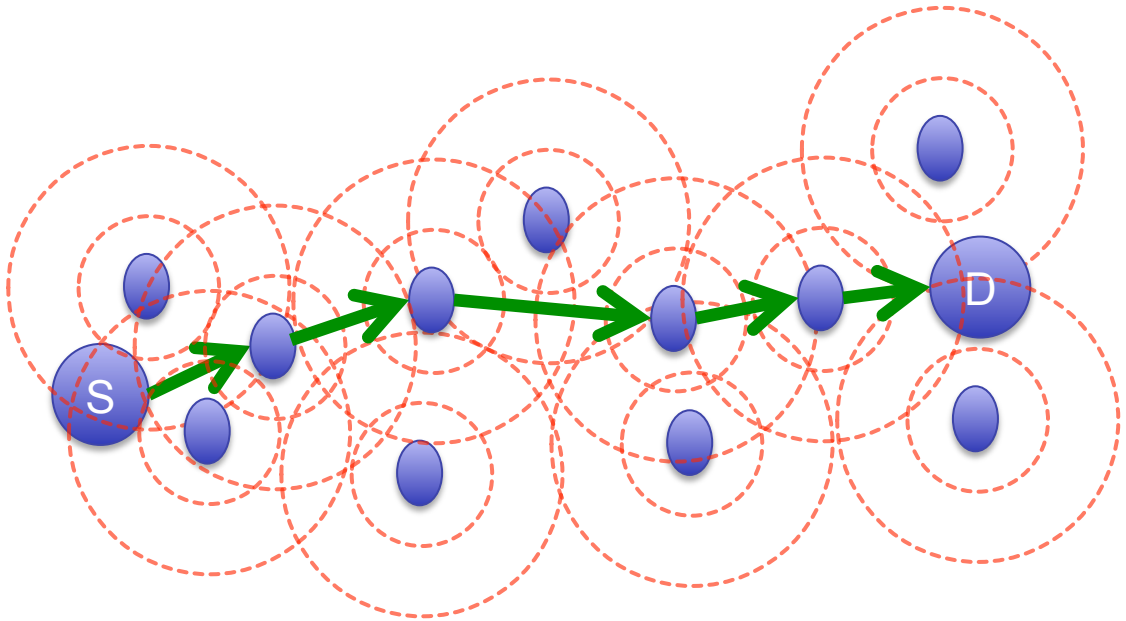
Trust Based Routing Framework



- Security in the routing plane
  - Gather **reputation** information on other nodes in the distributed network
  - Compute trustworthiness of nodes, to a shared Trust value
  - Mix trustworthiness with routing metric to avoid attackers in the path

Reputation module: overview

- Attacker model: Packet Dropper
  - Firewall misconfiguration
    - Not detected by routing planet but fatal on data plane
  - Targeted attack exploiting total or selective packet dropping



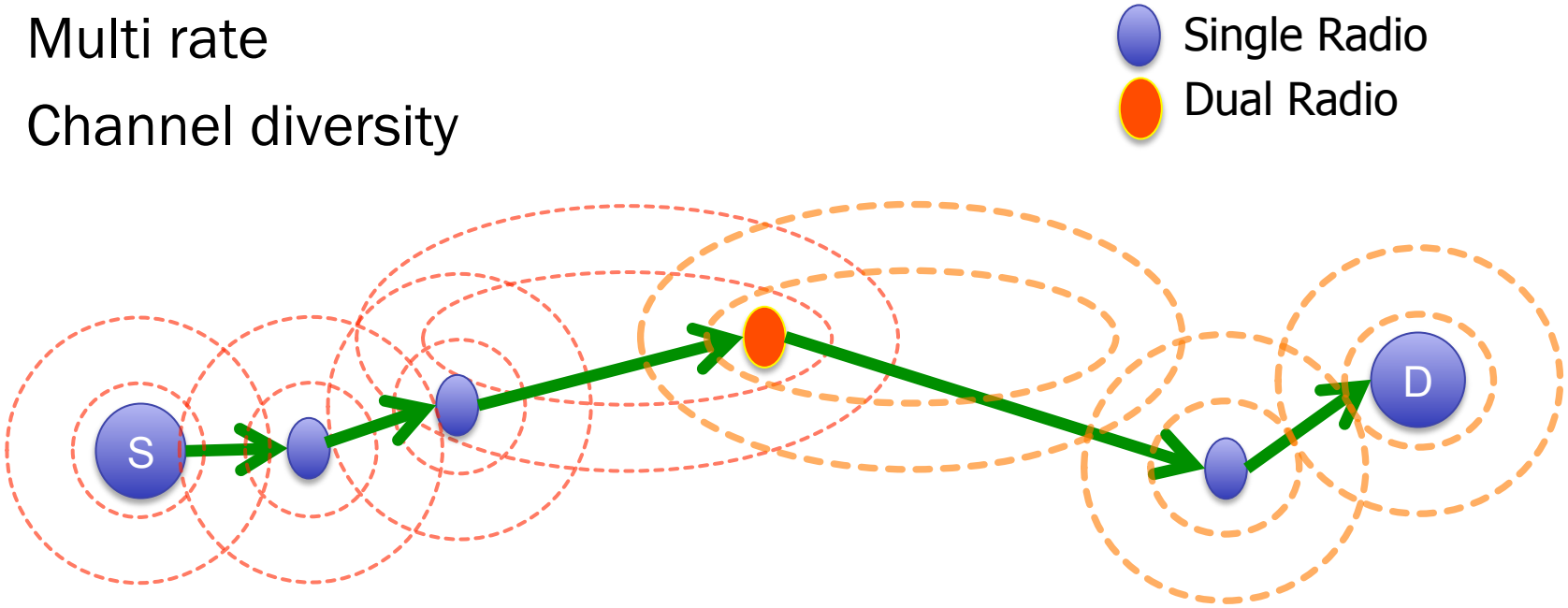
Reputation module: overview

- Path-wide and probe-based reputation module
  - UDP traffic carries **implicit** probes
  - All nodes on path are evaluated
  - Reusable for wired wireless and virtual networks
    - Note that most existing work in literature focus only on wireless networks, exploiting overhearing (not always feasible in real systems)

- Steganographic technique to hide implicit probes
  - Source and Destination share a secret Ksd
  - Packet P is a probe if HMAC(Ksd+P) < threshold

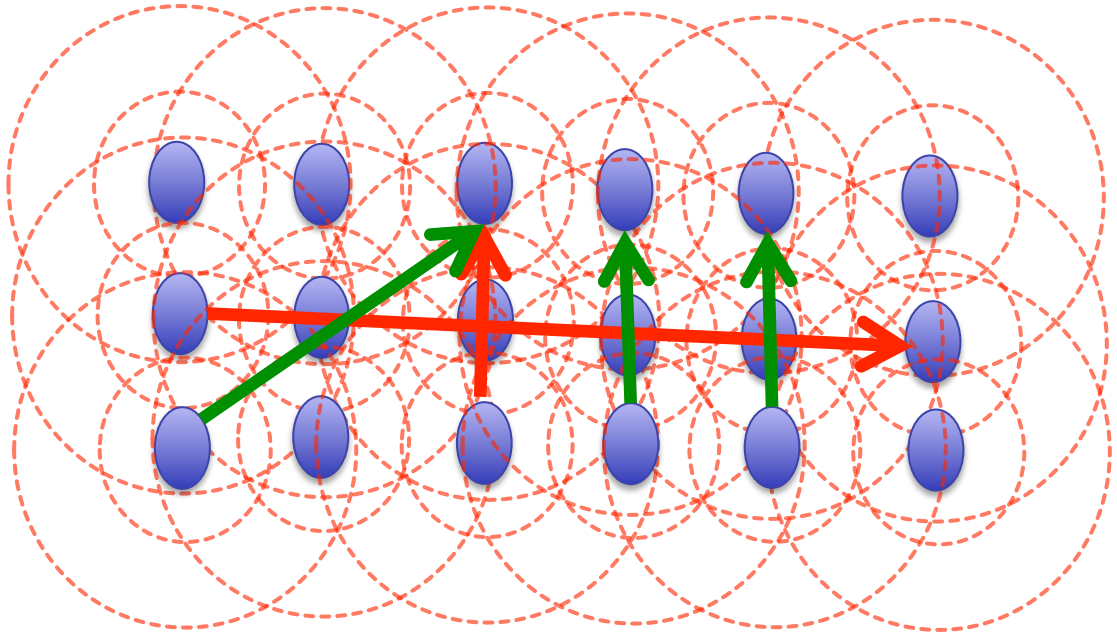
Reputation module: implicit probes

- State of the art based on overhearing
- Overhearing could be not feasible in real networks
  - Directional antennas
  - Multi rate
  - Channel diversity



Reputation module: overview

- Nodes are tested on different traffic flows
  - All nodes in a path are evaluated
  - Information from different UDP flows is correlated



Trust module

- Reputation to Trust
  - Reputation info collected by all nodes is shared
  - Info is processed to converge a global shared trust value

- Eigen Trust
  - State of the art algorithm
  - Based on transitive trust

- ITRM
  - Stronger against bad mouthing
  - No transitive

Weighting

- GOAL: Shortest path routing selects always the most trusted path
  - Unstrusted nodes are skipped when shortest path is calculated with dijkstra

$$\begin{cases} ML \cdot w_{high} < w_{medium} \\ ML \cdot w_{medium} < w_{low} \end{cases}$$

  - ML: Maximum Path Len

- ML = 10 hops
  - W low = 100
  - W medium = 1
  - W high = 0.01

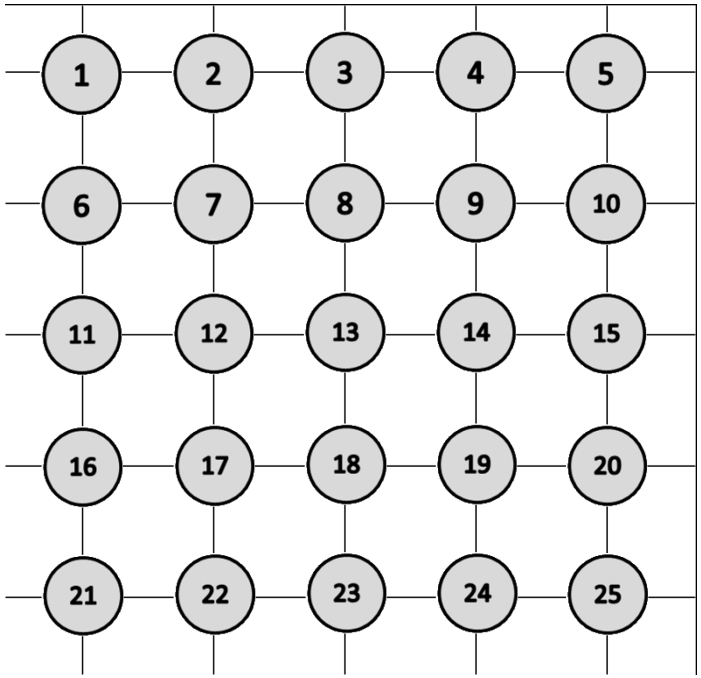
Results with ns2 simulator

- Ns2 extended with OLSR, and our framework

- Each node starts a CBR UDP session at 220Kbps with 1492 packet size. Threshold 1/32. We have in average 6 probes in 10 seconds

- Reset of local reputation value after 60 seconds of probing inactivity

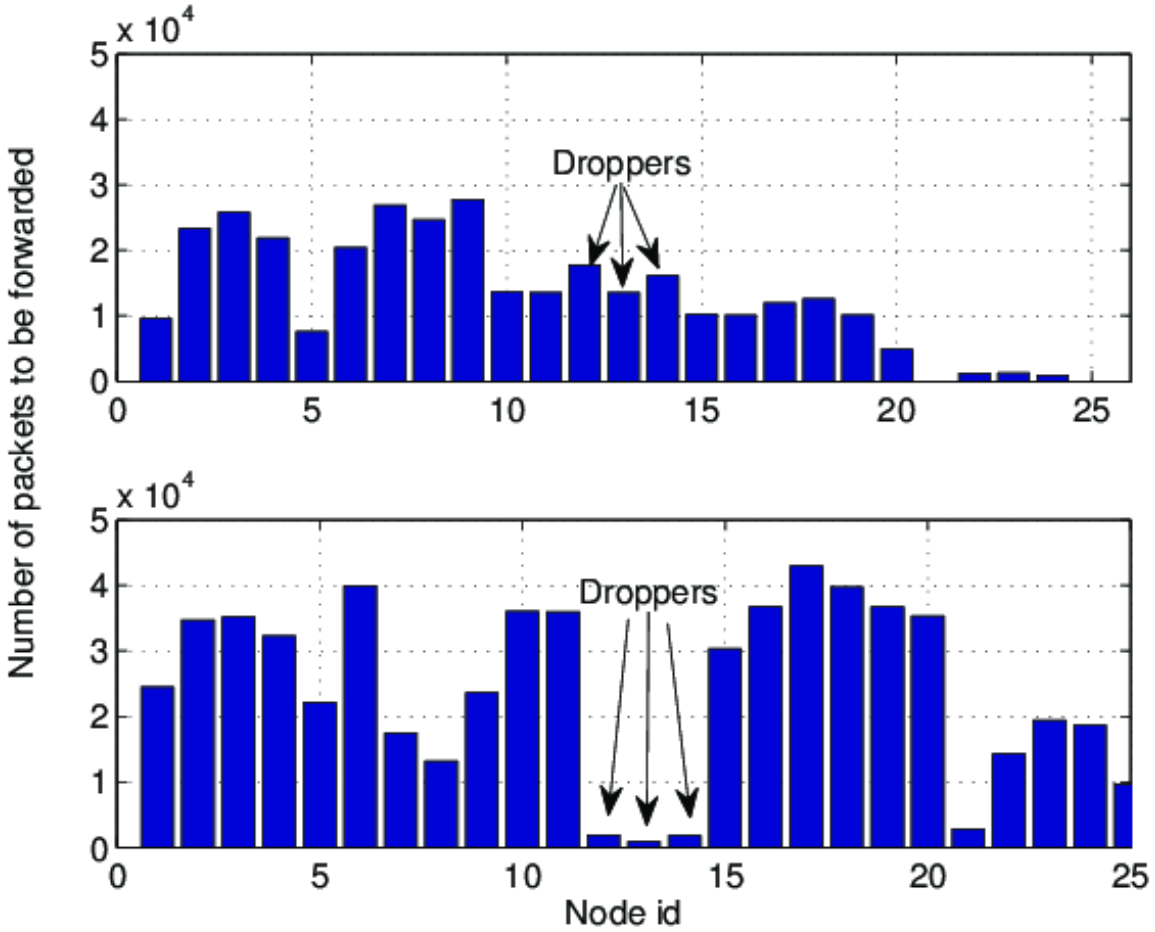
- Attackers drop 100% of packets



Results with ns2 simulator

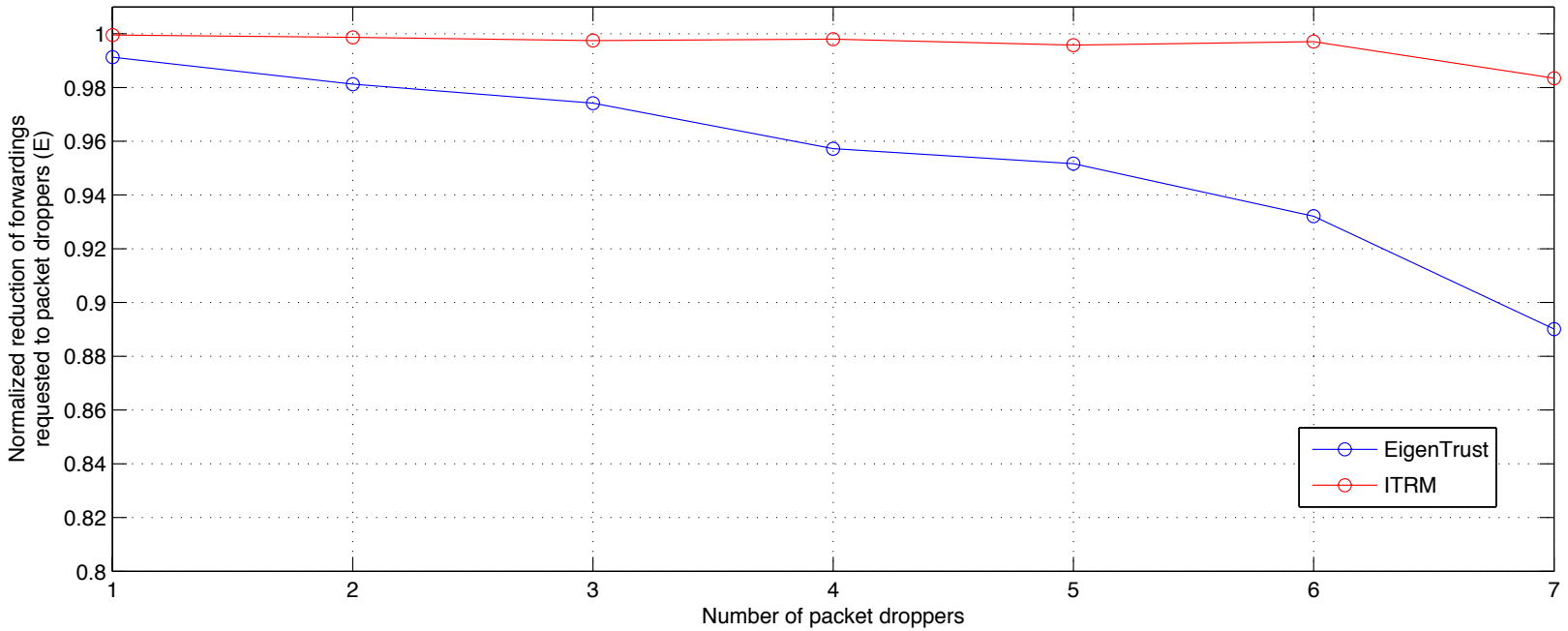
- Ns2 extended with OLSR, and our framework

- Enable the trust routing framework attackers are detected and isolated
- Traffic is no more relayed to attackers for forwarding
- Throughput of the all network increases



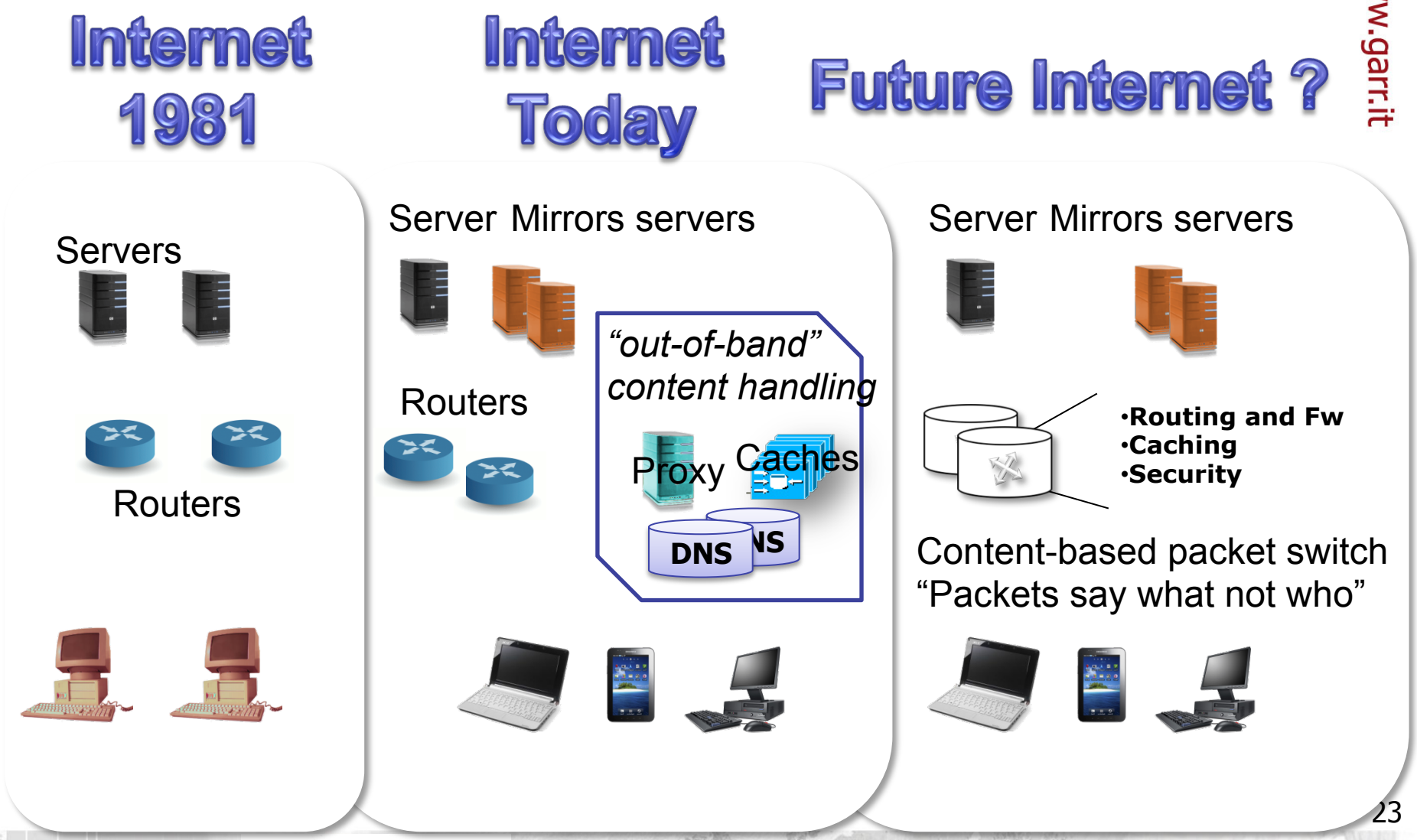
Results with ns2 simulator

- Normalized reduction of packets to be forwarded by attackers
  - 1 = routing completely skipped the attackers when computing the shortest paths
  - ITRM (red) is way better than EigenTrust (blue)



Future Work
Trust and Security
In
Content Centric Networks

Future work


Internet 1981
Internet Today
Future Internet ?
Servers
Routers
Server Mirrors servers
Routers
"out-of-band" content handling
Proxy
Caches
DNS
Server Mirrors servers
•Routing and Fw
•Caching
•Security
Content-based packet switch
"Packets say what not who"

Future work

- IP Internet Protocol
  - Host to Host communications
  - Security and identity of data is inherited from security of connections and identity of hosts
- Content Centric Network
  - User requests a content, not a connection with a server
  - Network routes user request toward the best source (anycast)
  - Network nodes could “cache&reply” traversing contents
- Trust issue
  - User and nodes has to trust content
    - Content is split in chunks introducing research challenges for security and trust

Questions ?

Questions ?