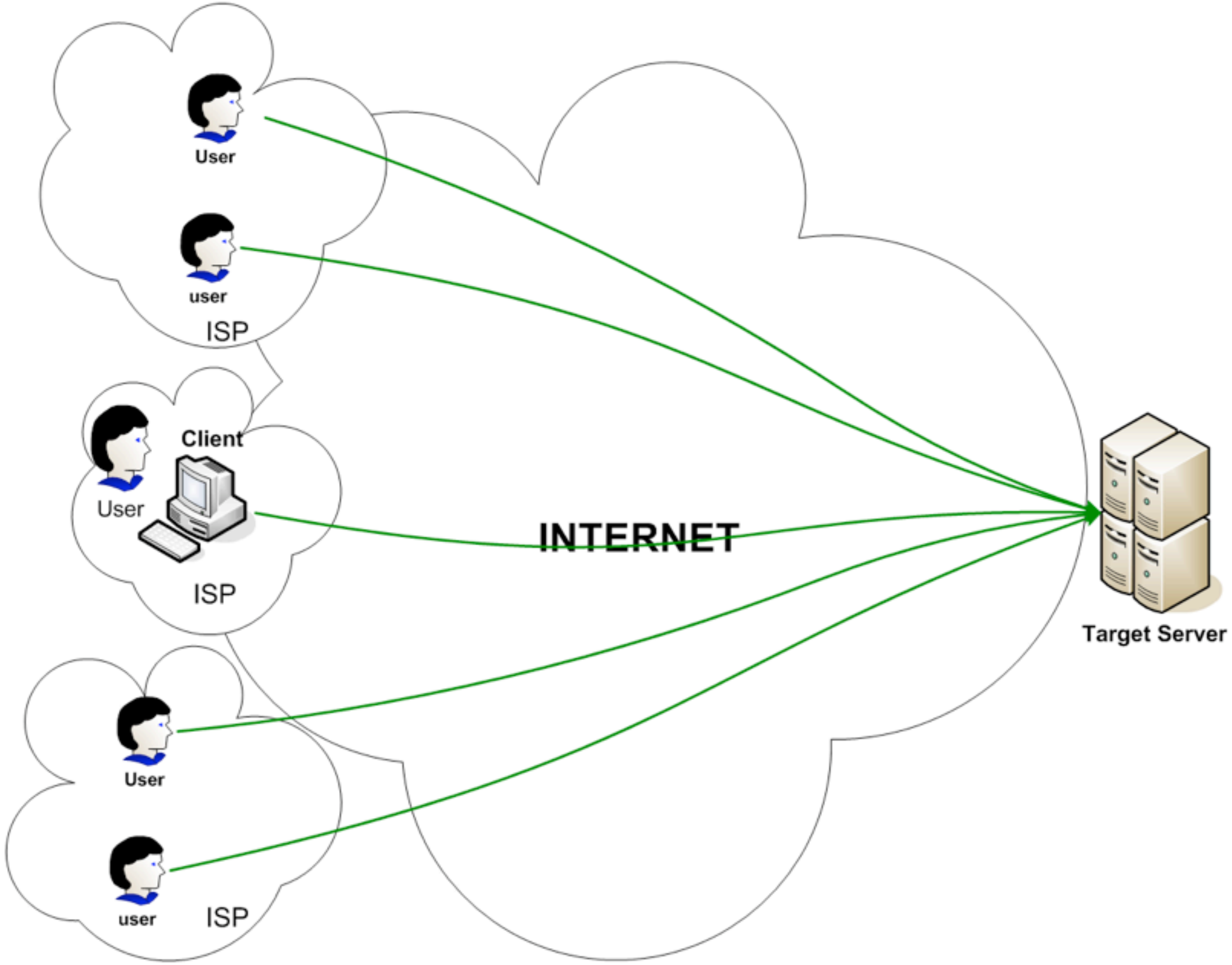
Denial of Service Attacks and Resilient Overlay Networks

Angelos D. Keromytis

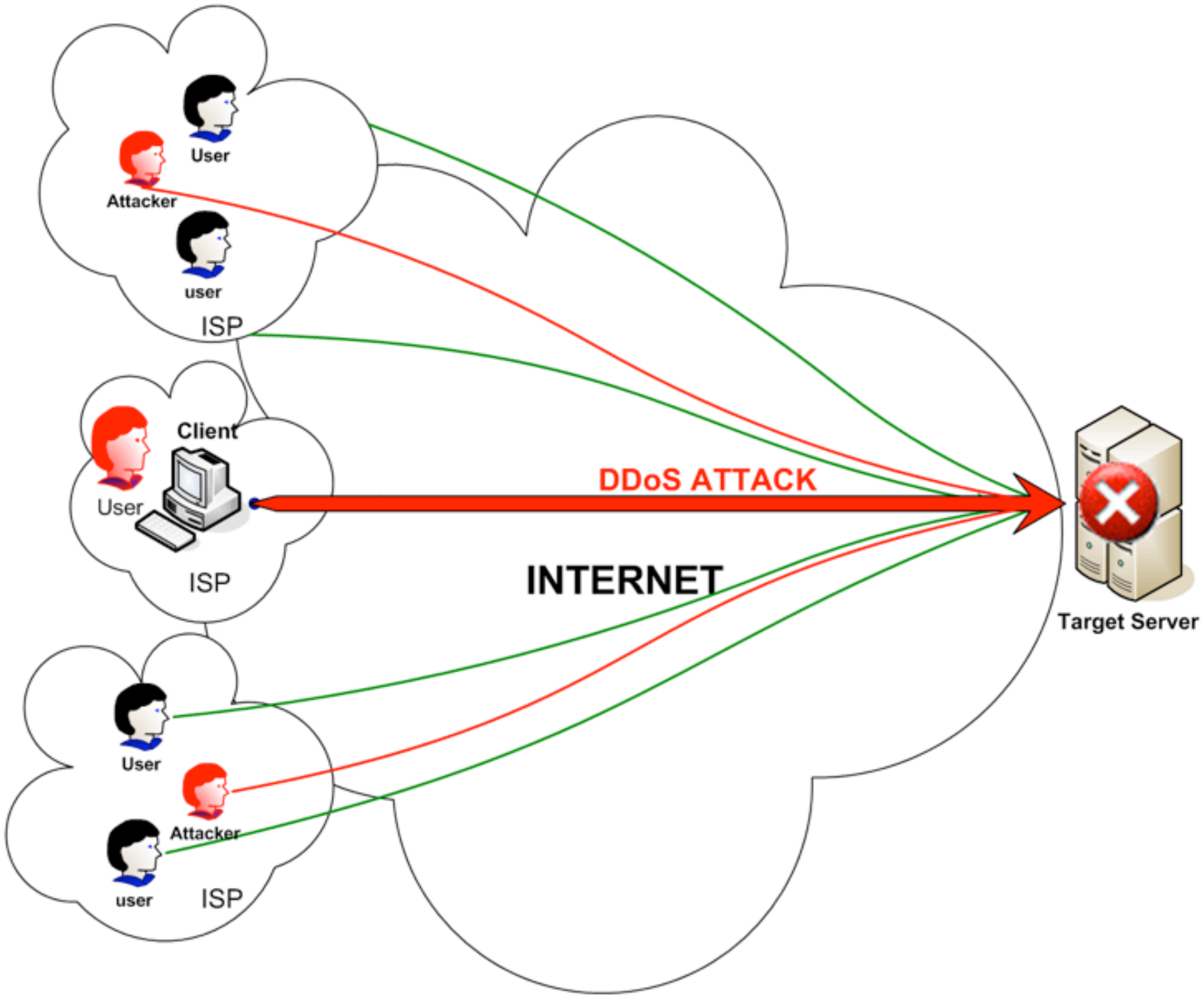
Network Security Lab

Computer Science Department, Columbia University

Motivation: Network Service Availability



Motivation: Network Service Availability



Why Does It Matter?

We are increasingly relying on Internet Services

- Financial services, Voice over IP (VoIP), e- Government, news, “Cloud Computing”, ...

But Internet Services are not dependable...

- Denial of Service attacks can disrupt online service
  - DDoS attack on Estonia (2007)

    2 Weeks, 1M computers, 5,000 clicks per second
  - DDoS attacks against Georgia (2008)
  - Storm Worm: 1.7M infected machines used for DDoS (typically extortion)

- Ease of assembling and controlling botnets means the problem will persist

Defenses

- End-users/sites:
  - Bandwidth over-provisioning
  - Multi-hosting/multi-homing
  - Use of Content Delivery Networks
- ISPs:
  - Blackhole routing
  - Anomaly detection & blocking
    - Centralized vs. distributed

Research Activity

- IP traceback (attribution)
- IP Pushback (reactive blocking)
- Collaborative filtering (reactive blocking)
- Router/receiver capabilities (proactive blocking)
- Improve host-based protection

Impediments to deployment

- Few economic incentives for deployment
  - Most schemes require global adoption & deployment
  - End-users lack the means to react
- DDoS is mostly an externality for ISPs
  - no market opportunity for router manufacturers
- Cross-ISP collaboration not always feasible
  - Competition concerns

Overlay Networks

- A different term of “distributed system”
  - Collection of systems
  - Connected over a wide-area network, such as the Internet
  - Route traffic amongst them without considering physical topology
    - Addressing, “neighborhood”, other properties may differ from those of the actual network fabric
- Good way of introducing new functionality into the network without changing routers/protocols (and, sometimes, end-hosts)

Using Overlay Networks

- Distribute logical function of a firewall across the Internet
  - Allow users to contact any overlay node
  - Any overlay node can validate a legitimate user
  - Once admitted into overlay, user’s traffic is treated preferentially
    - Allowed to reach attacked site
    - All other traffic dropped/rate-limited

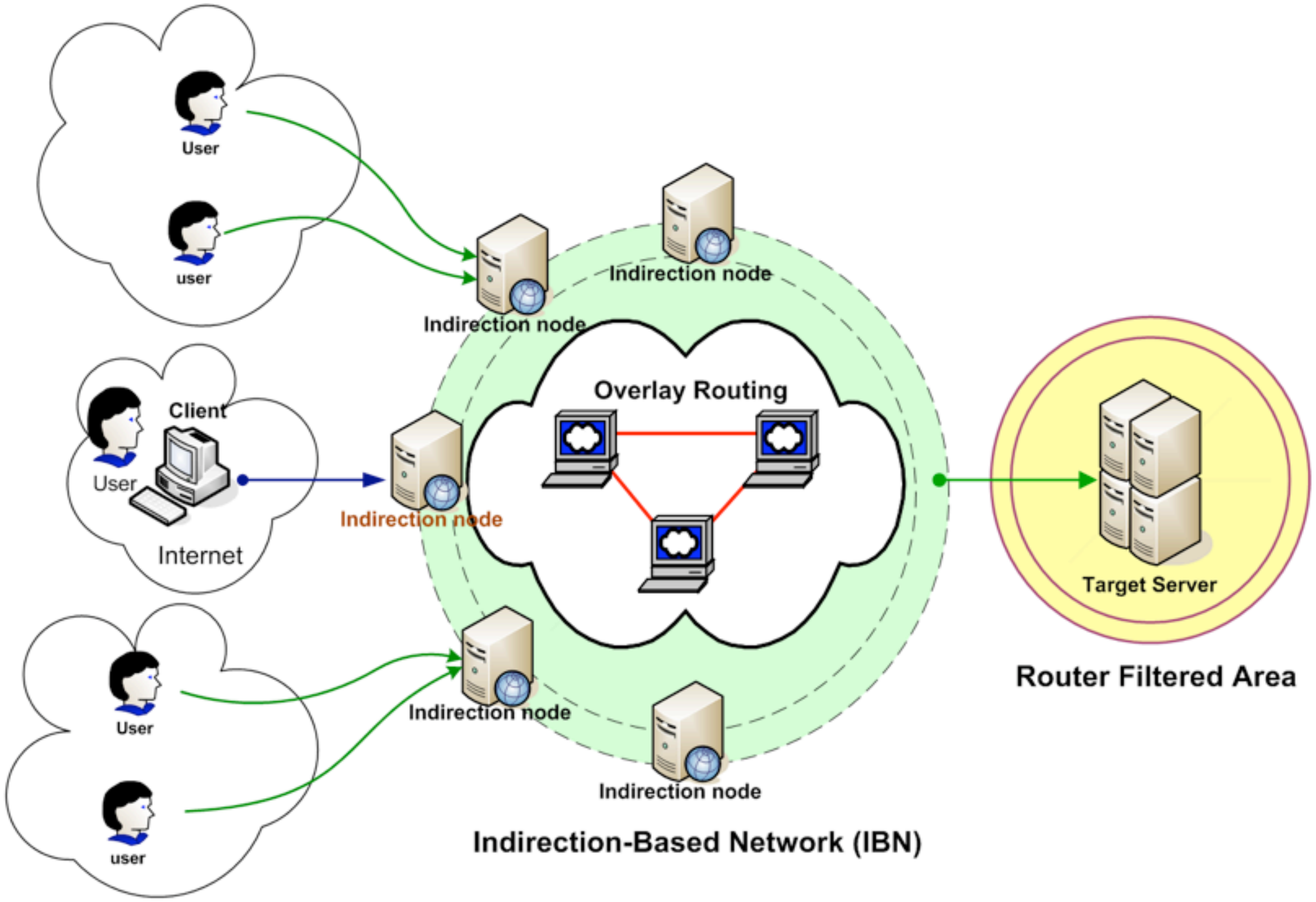
Advantages of Overlay Networks

- Difficult to attack with a DDoS due to distributed nature
  - Assumes “large enough” overlay
- Does not rely on ISP co-operation or goodwill
  - Can take advantage of such, where it exists
- A single overlay can provide protection service to different users
  - Commercialization model similar to CDN
- A large enough distributed organization can create its own overlay

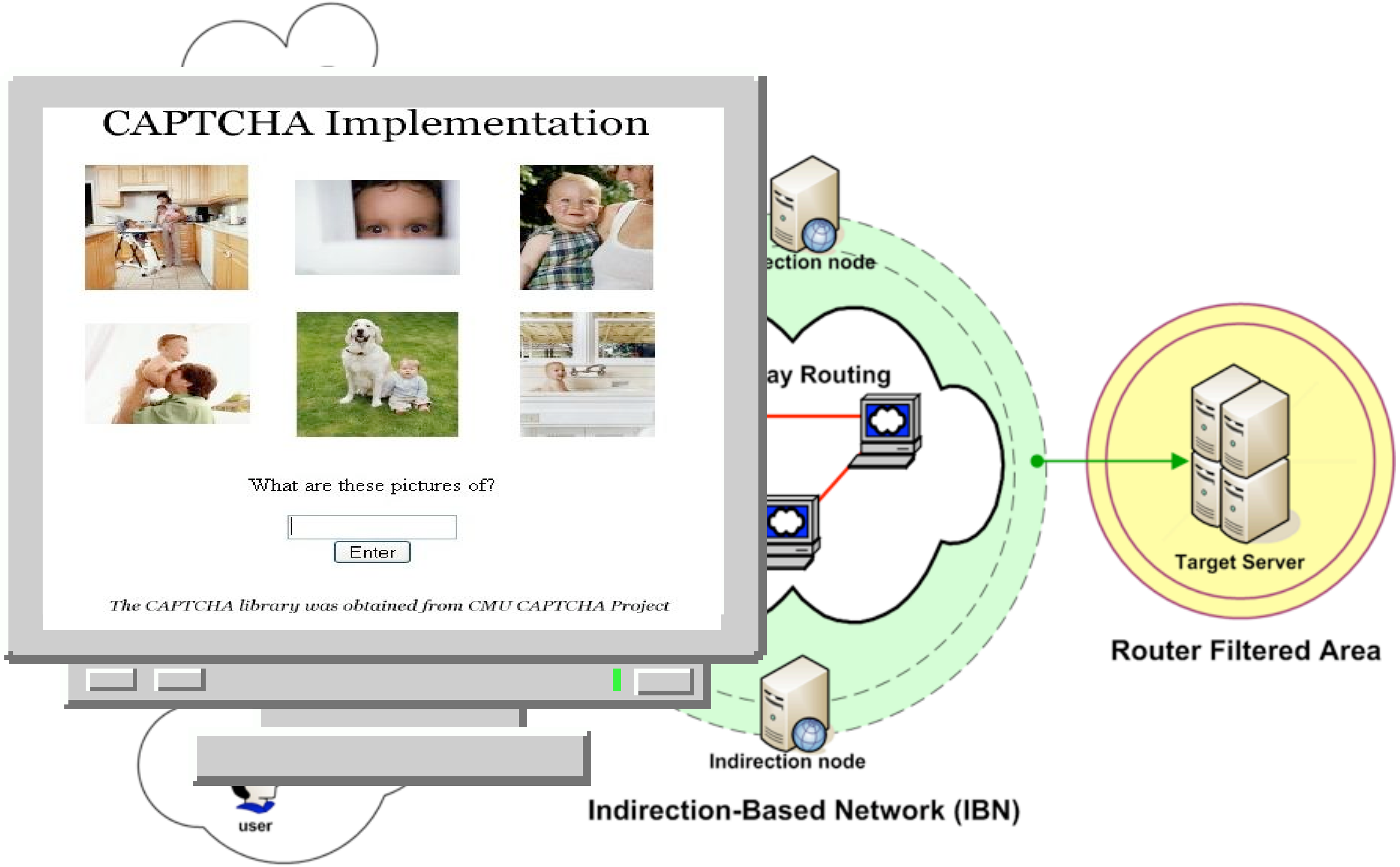
Issues with Overlay Networks

- How do users discover (accessible) overlay nodes?
  - Largely static content, users (software) can access any node
- Overlay network becomes obvious target of attack
  - Dedicated nodes, easier to “harden”
- Performance issues
  - Higher latency, lower throughput due to non-direct routing
- How can we tell who is a legitimate user, vs. a bot?
- How do we effectively discriminate overlay vs. non-overlay traffic?

WebSOS: Protection for Web Services



WebSOS: Protection for Web Services



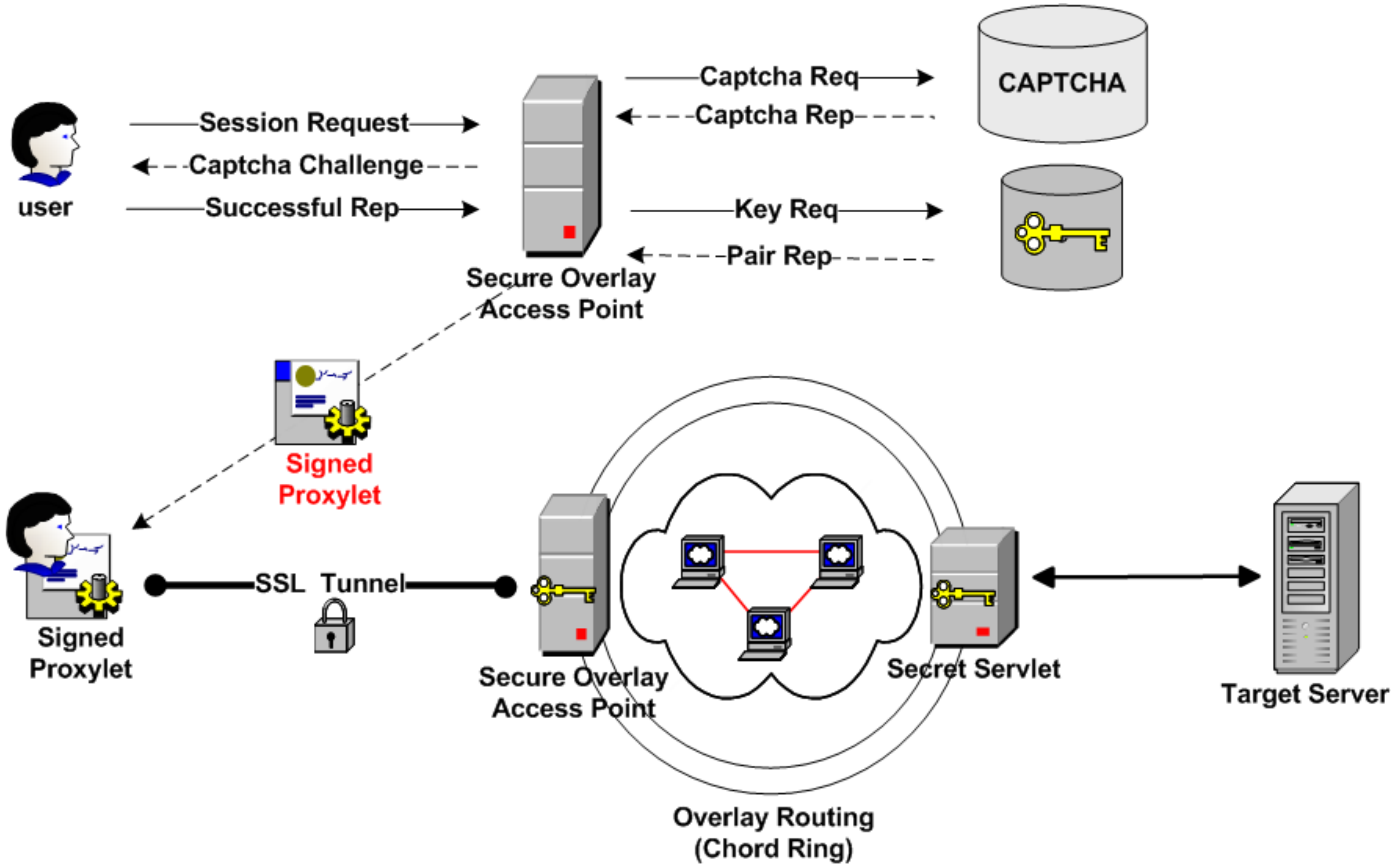
CAPTCHA Implementation

What are these pictures of?

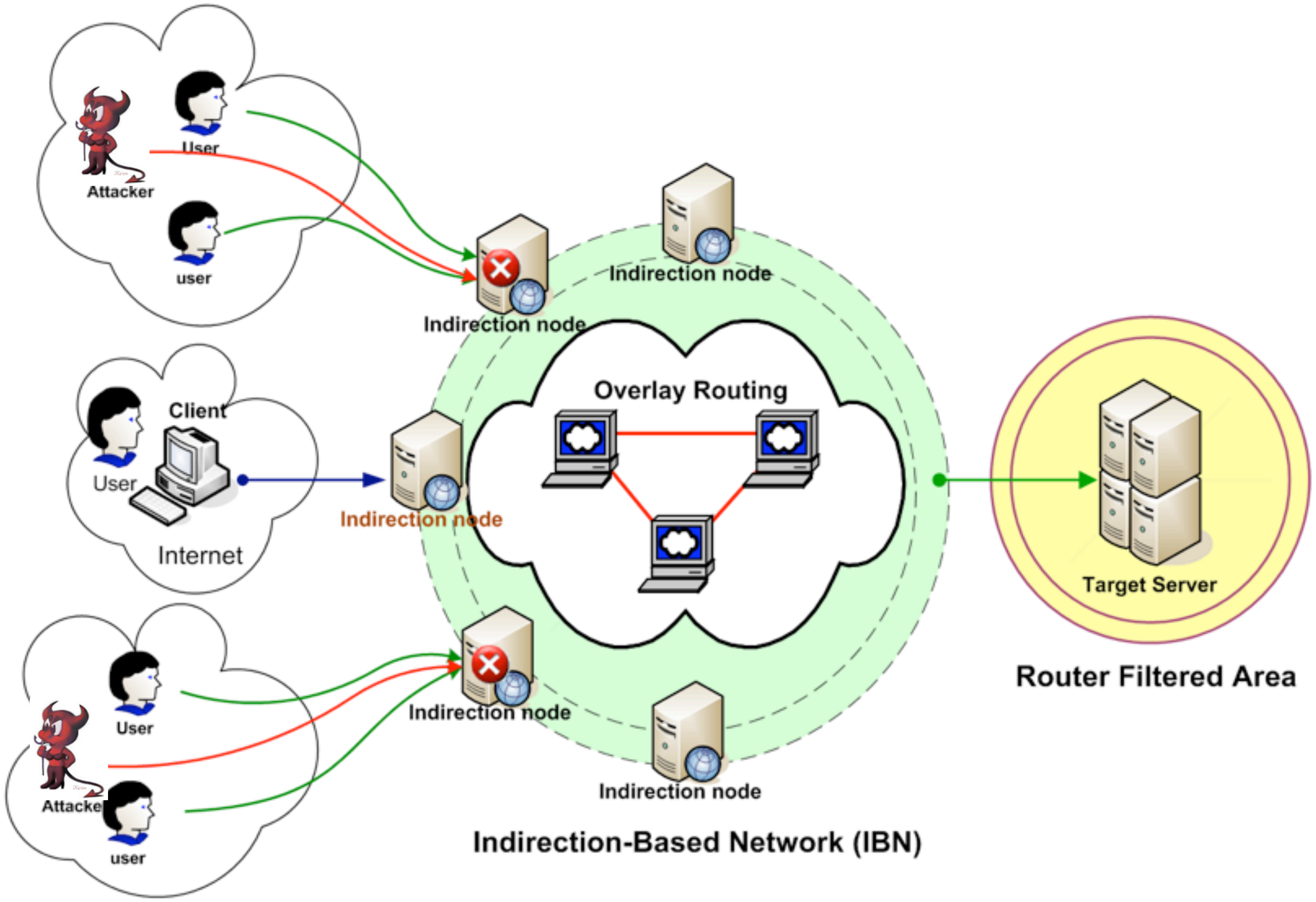
Enter

The CAPTCHA library was obtained from CMU CAPTCHA Project

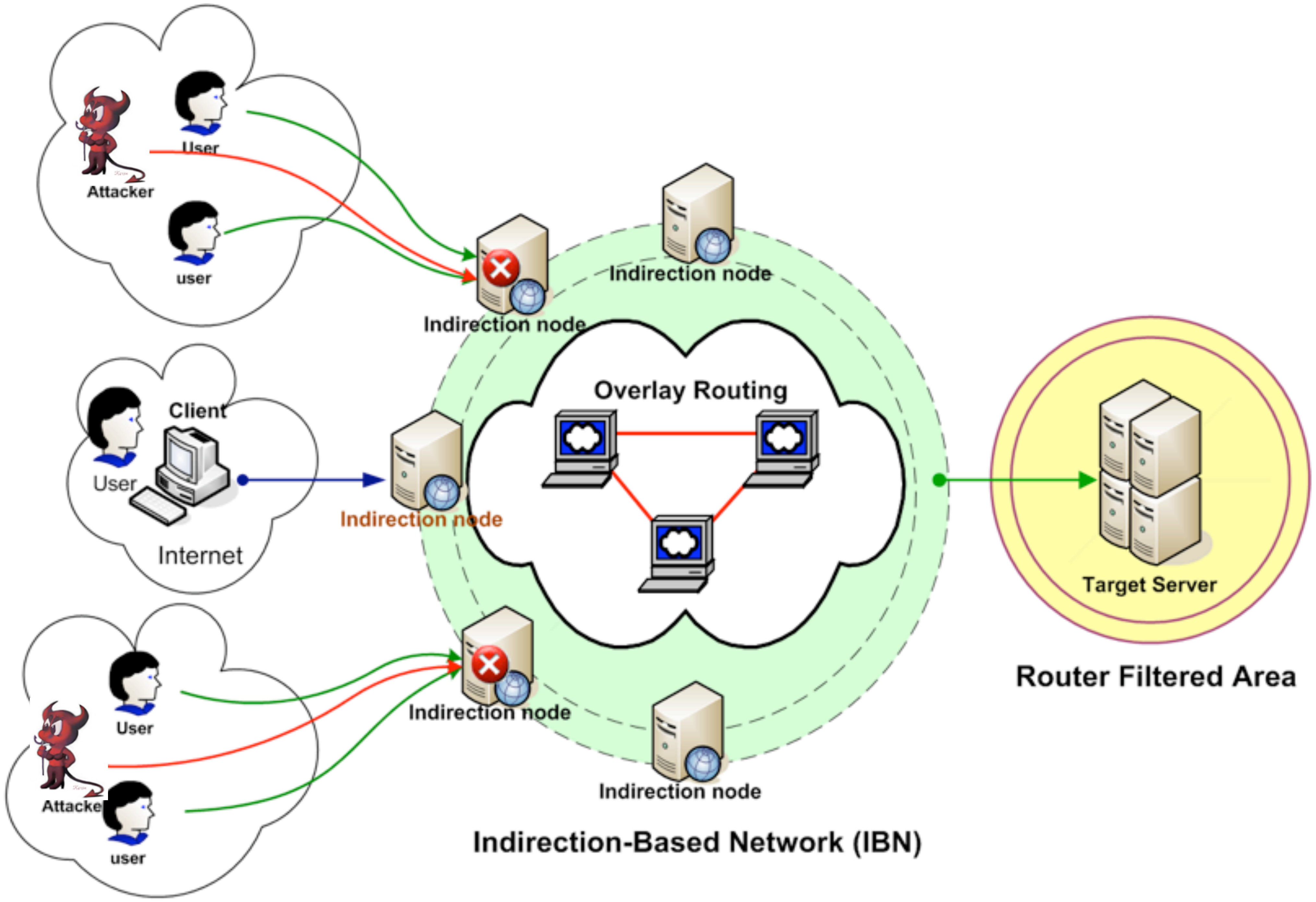
WebSOS: Protection for Web Services



WebSOS: Protection for Web Services

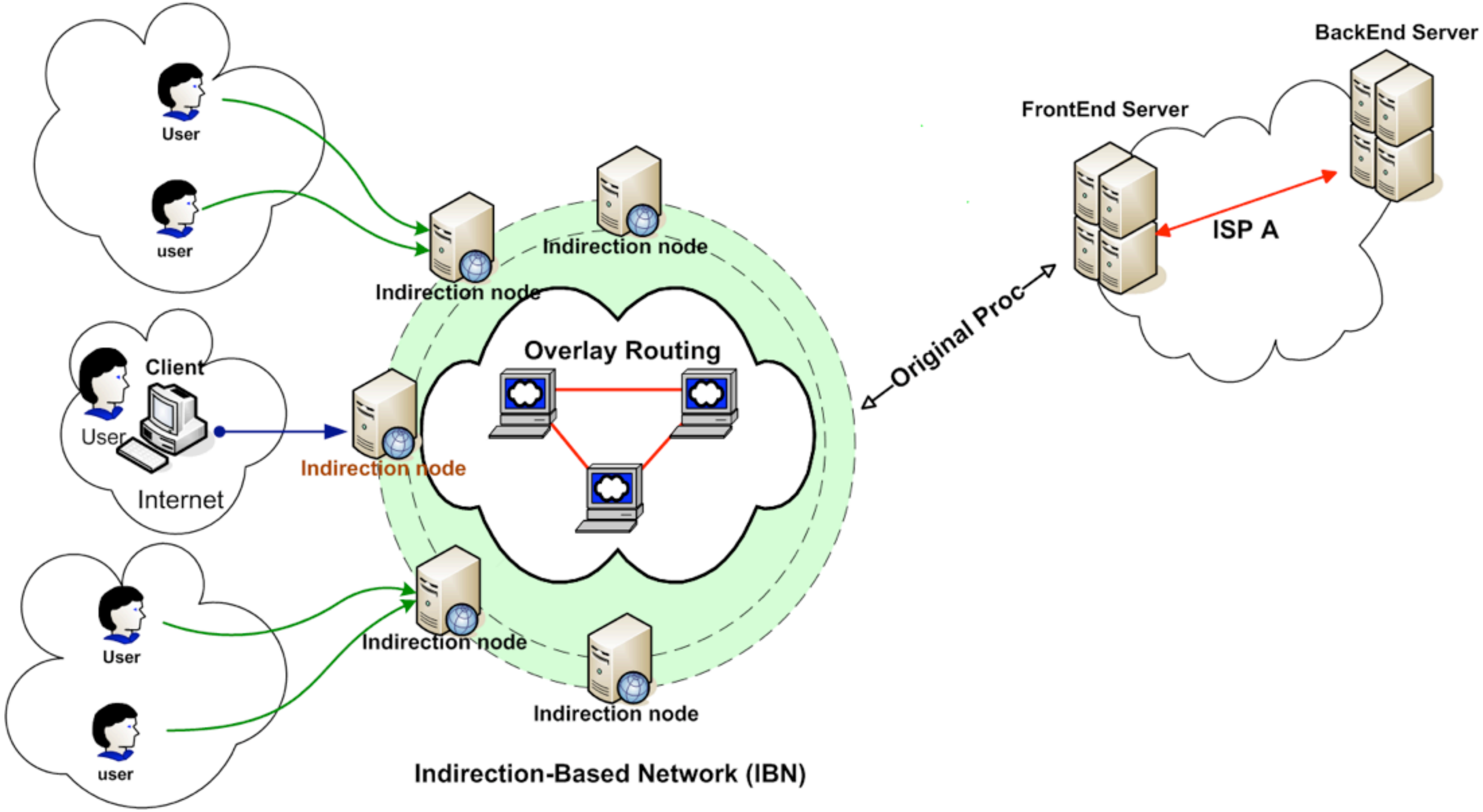


WebSOS: Protection for Web Services

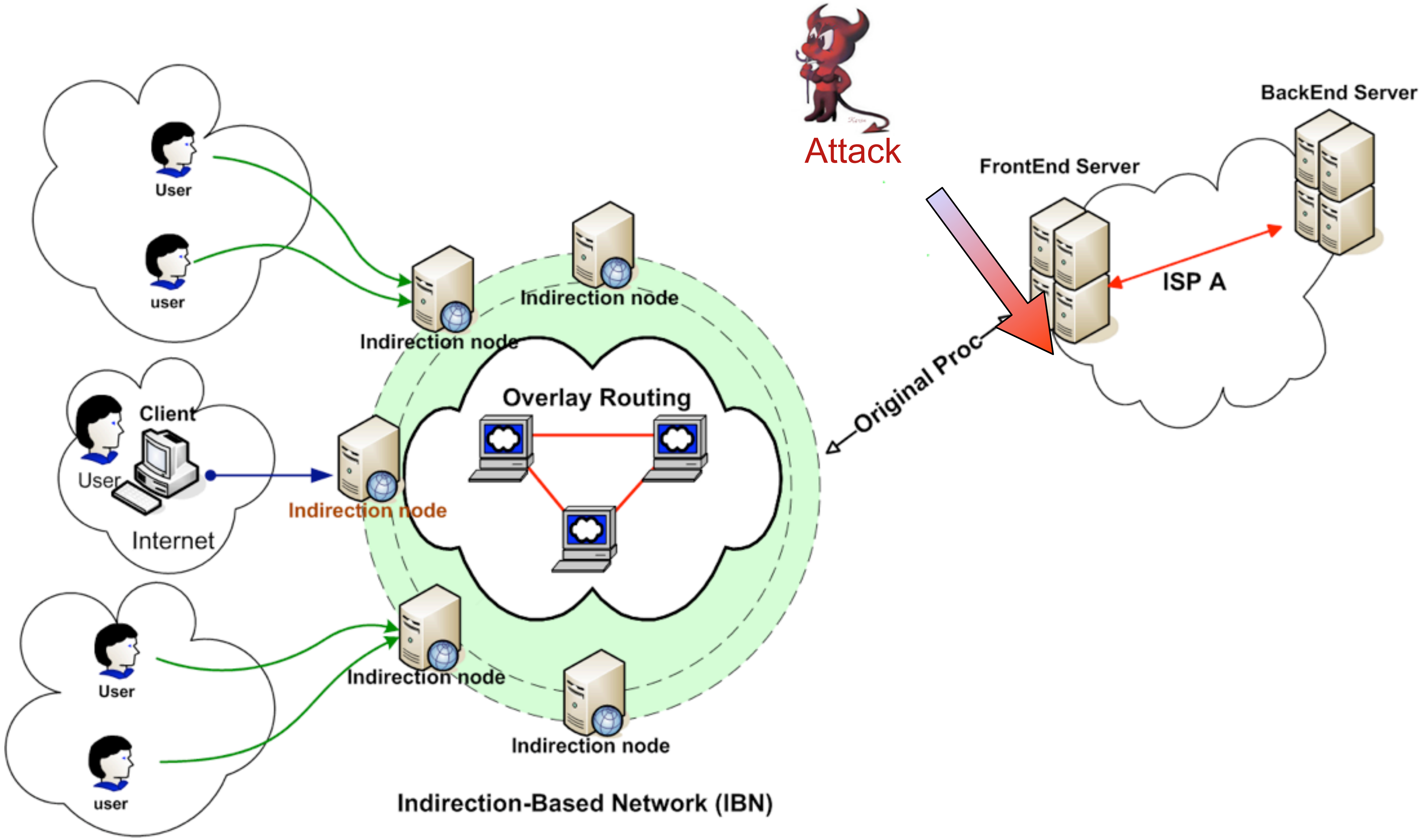


Can we remove Packet Filtering?

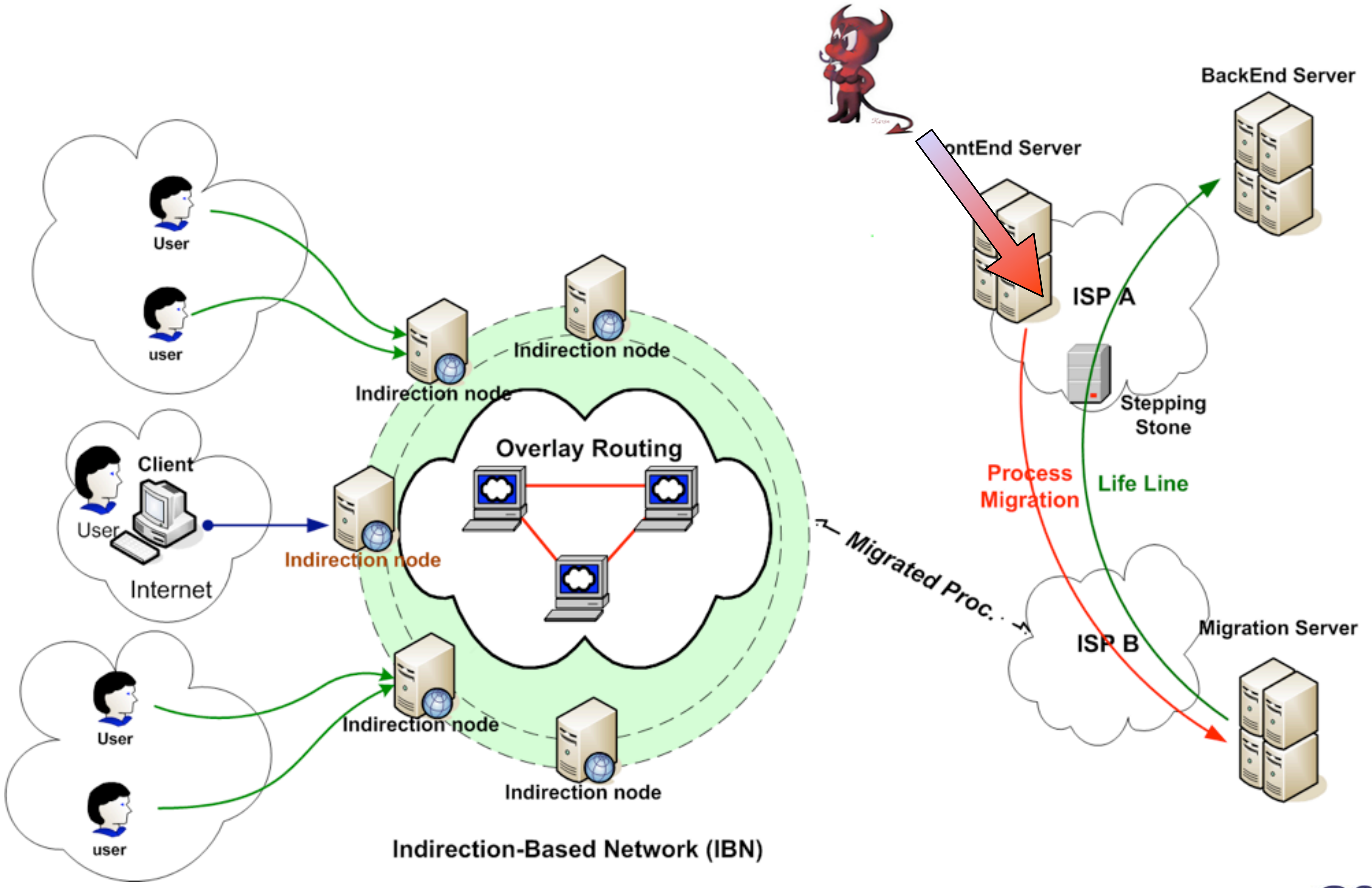
Move: An End-to-End Solution for DDoS



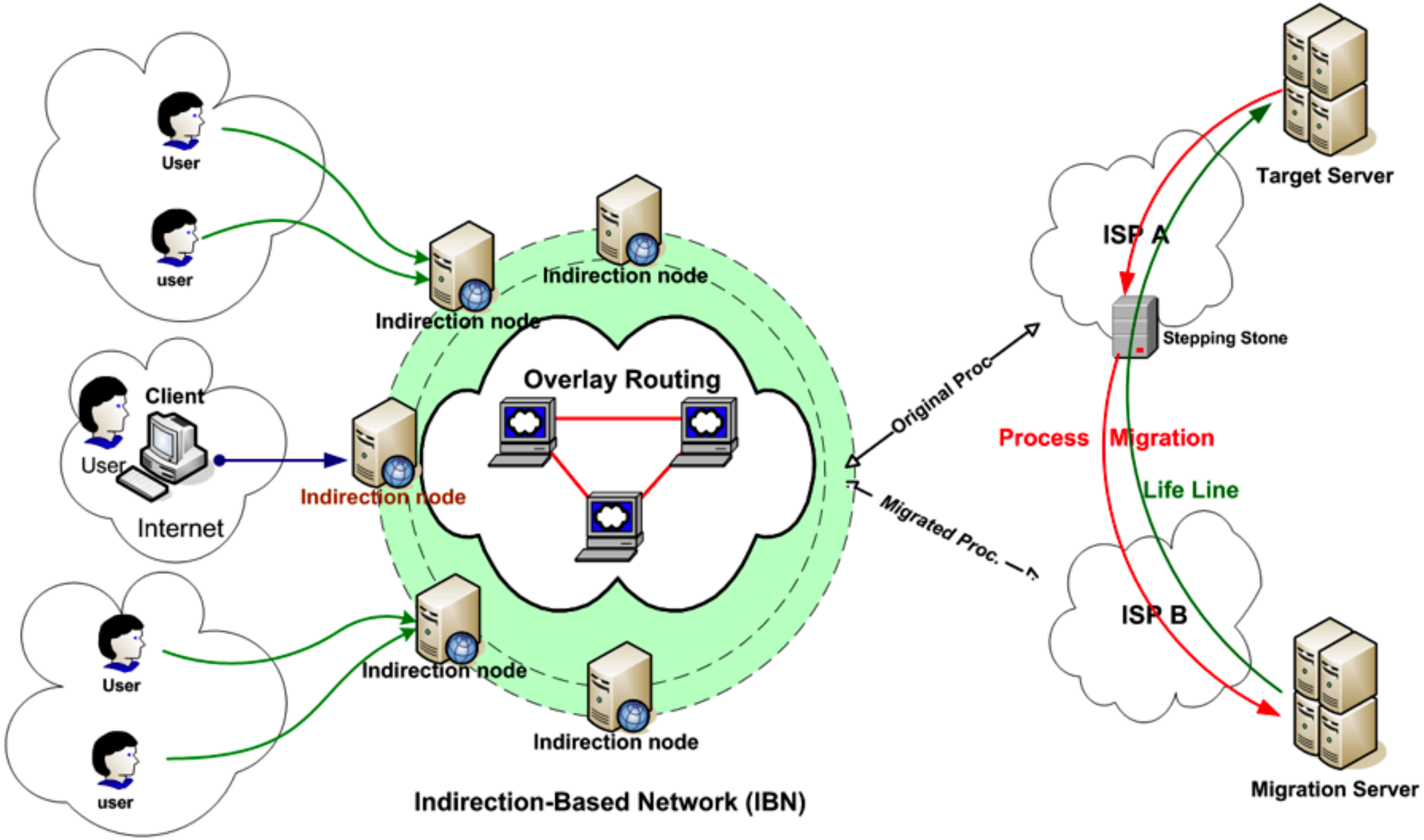
Move: An End-to-End Solution for DDoS



Move: An End-to-End Solution for DDoS



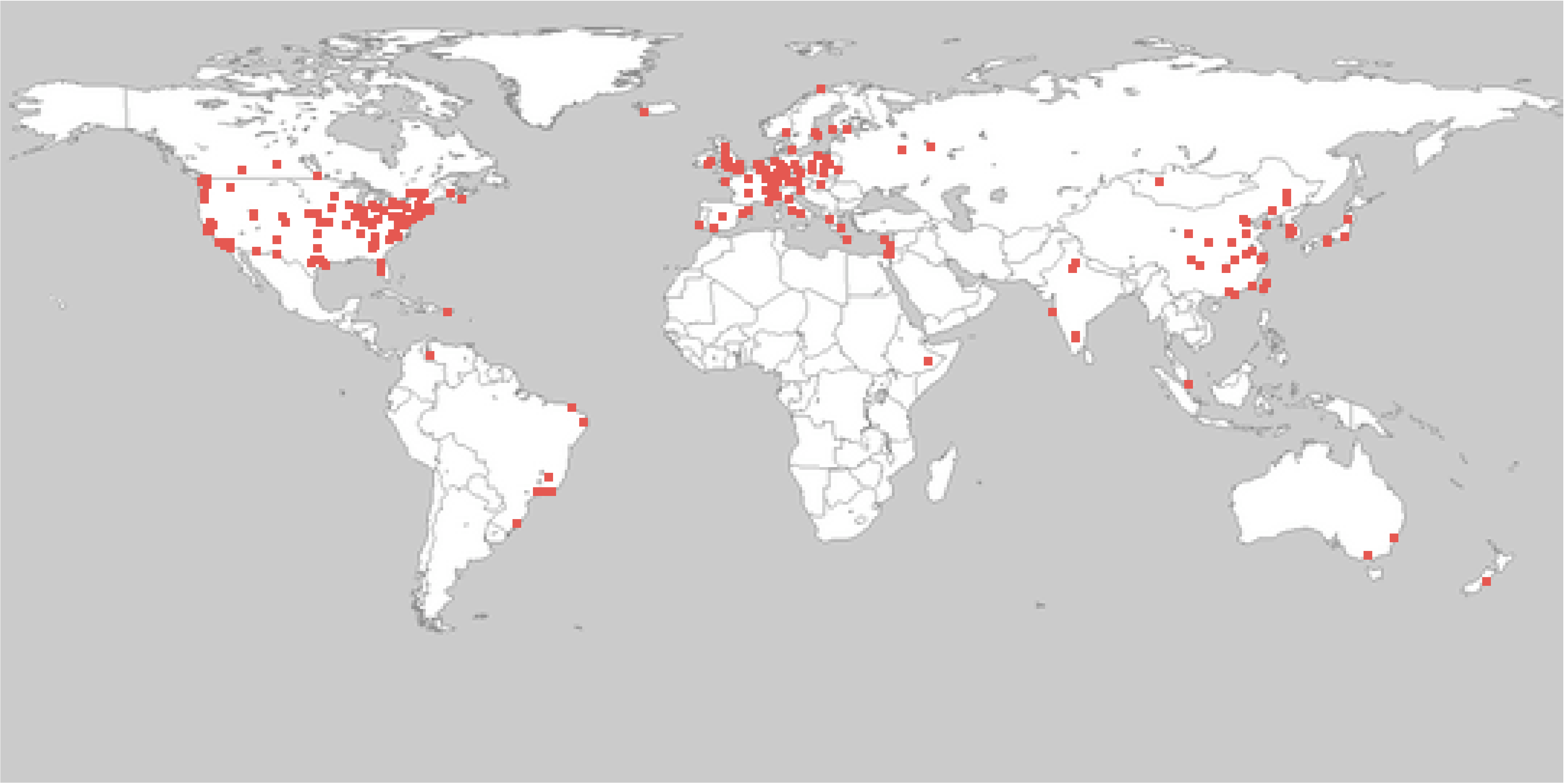
Move: An End-to-End Solution for DDoS



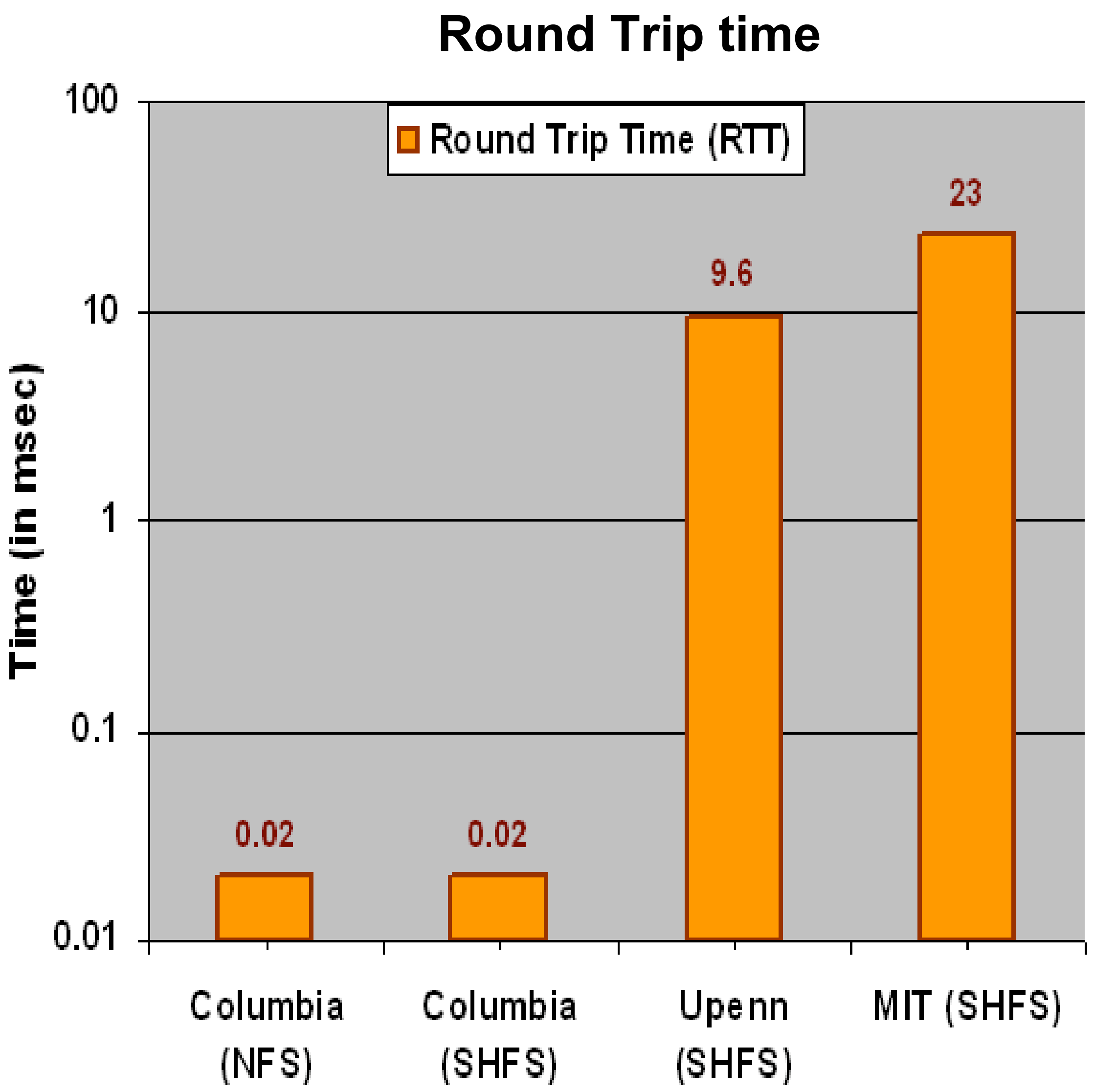
Prototype in Planet-Lab

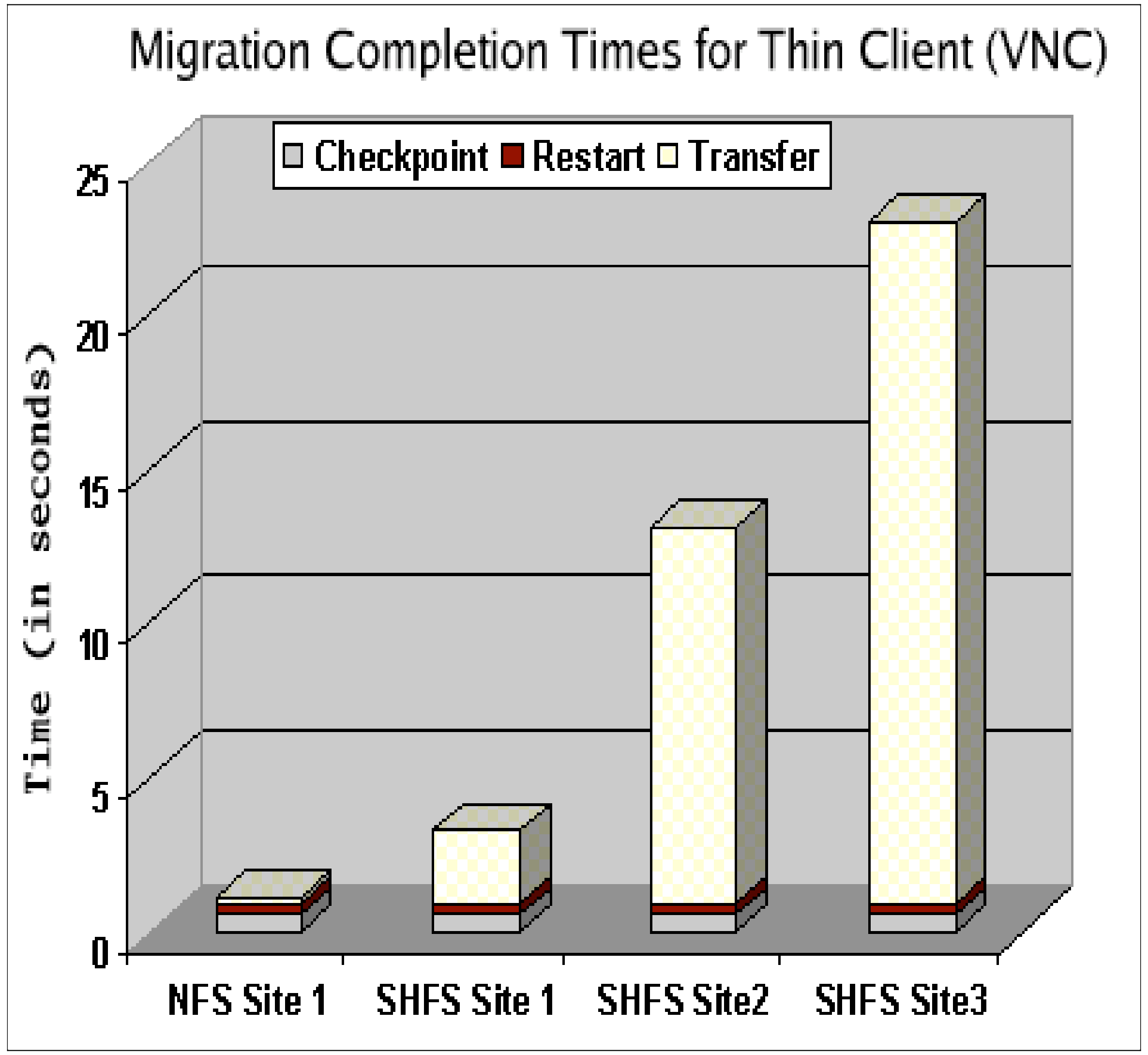
PLANETLAB

An open platform for developing, deploying, and accessing planetary-scale services

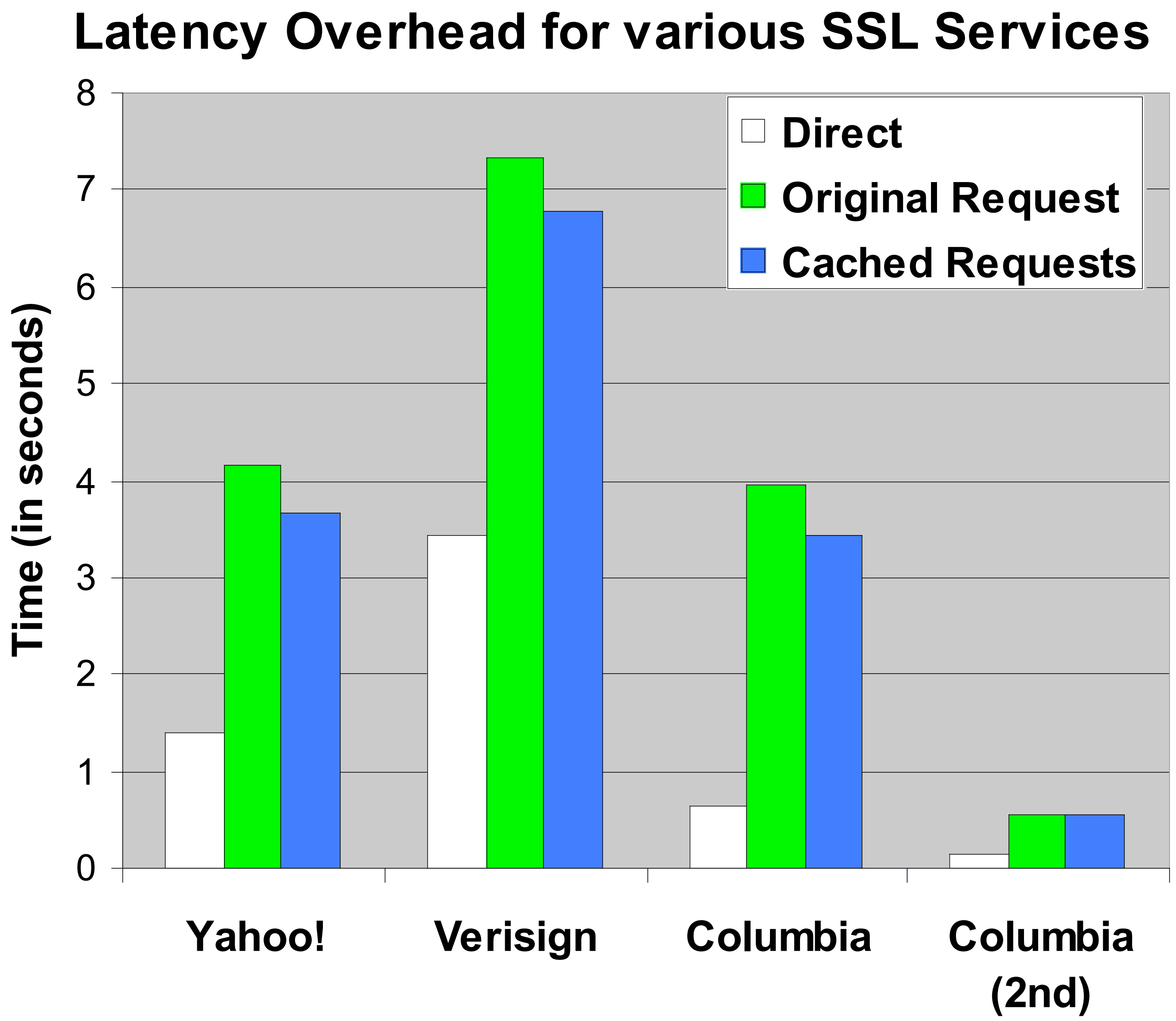


Migration Performance



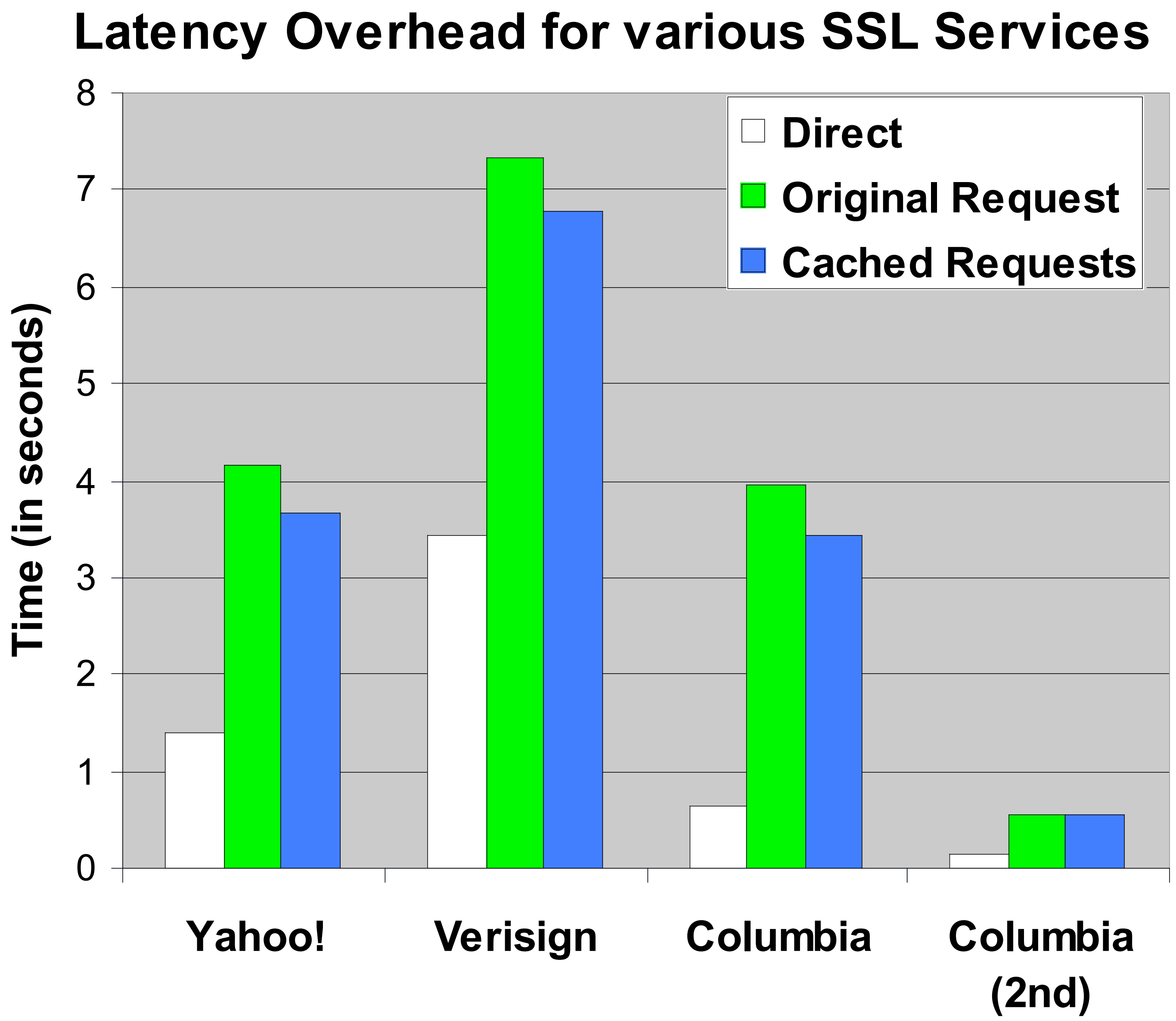


Limitations of WebSOS & MOVE



Latency increase by a factor of 2 when using indirection

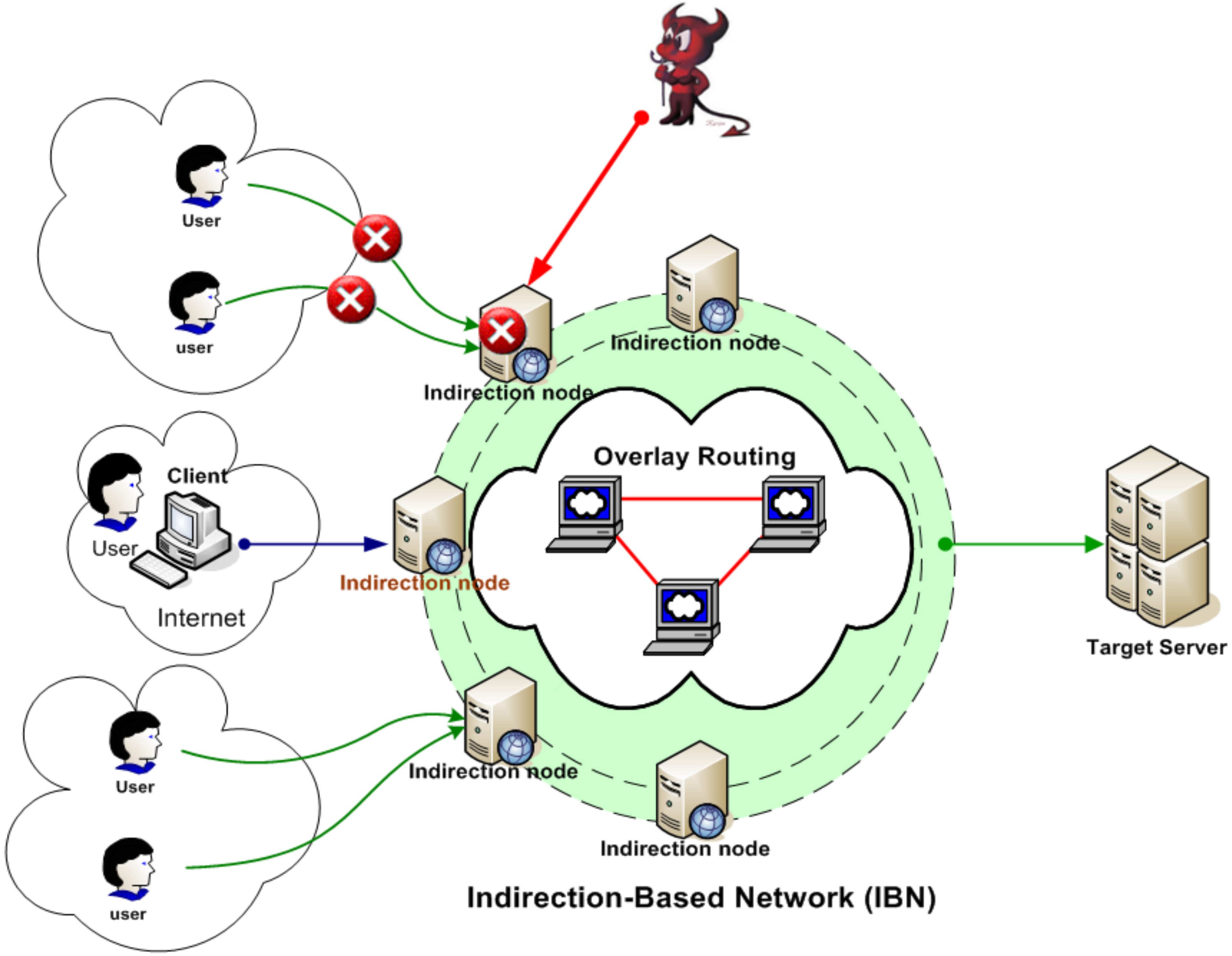
Limitations of WebSOS & MOVE



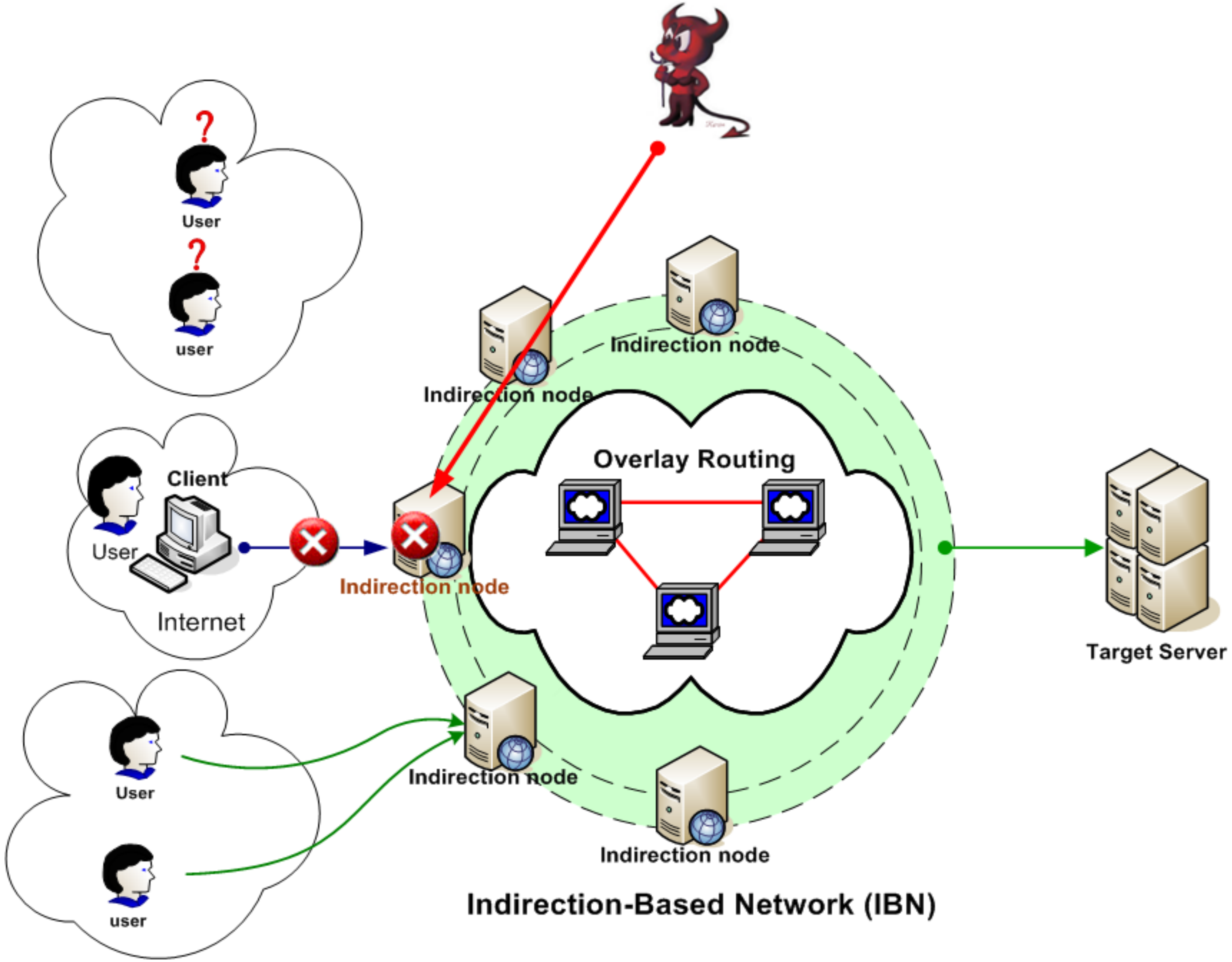
Latency increase by a factor of 2 when using indirection

Also vulnerable to some more intelligent attacks ...

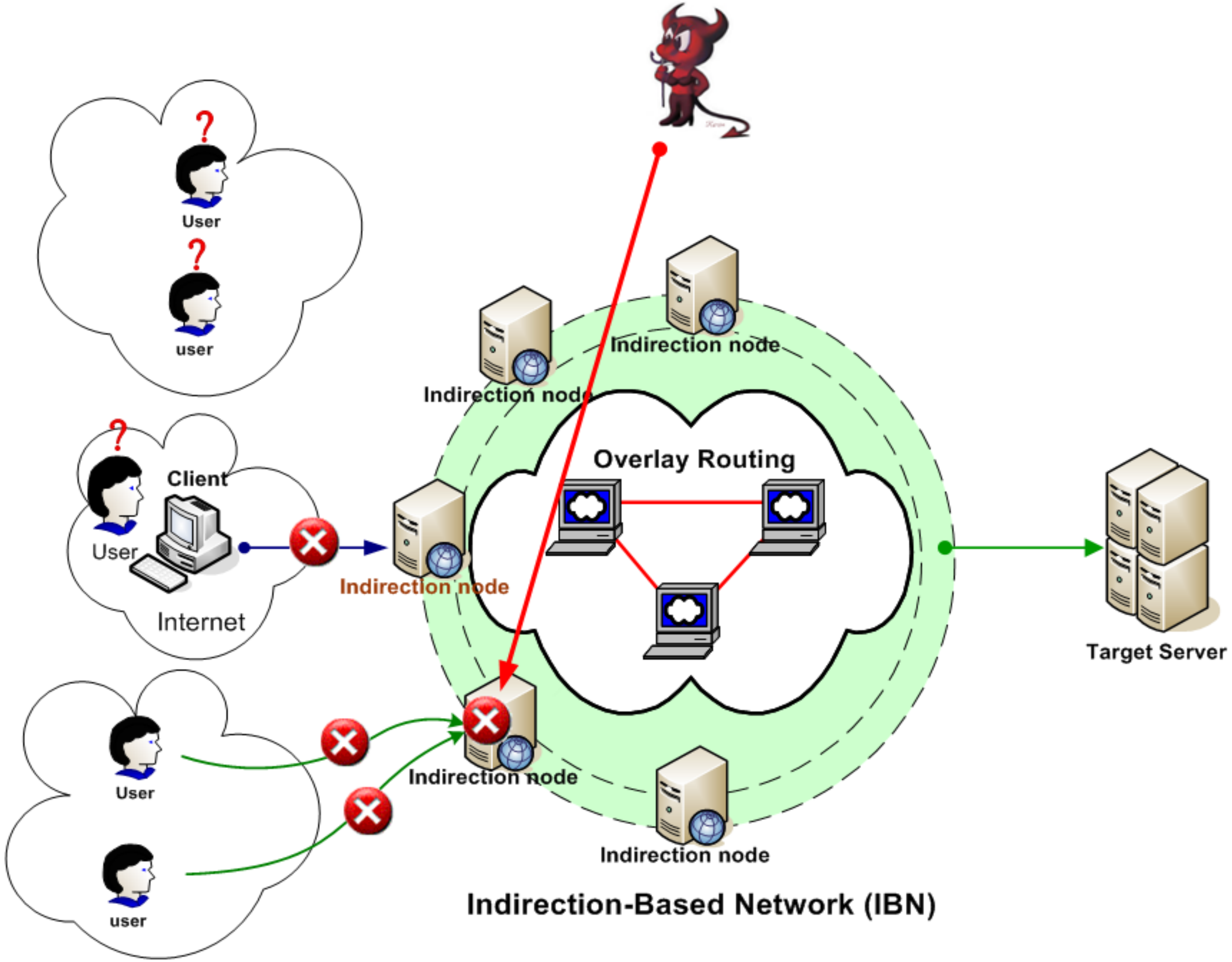
New Attack: Sweeping Attack



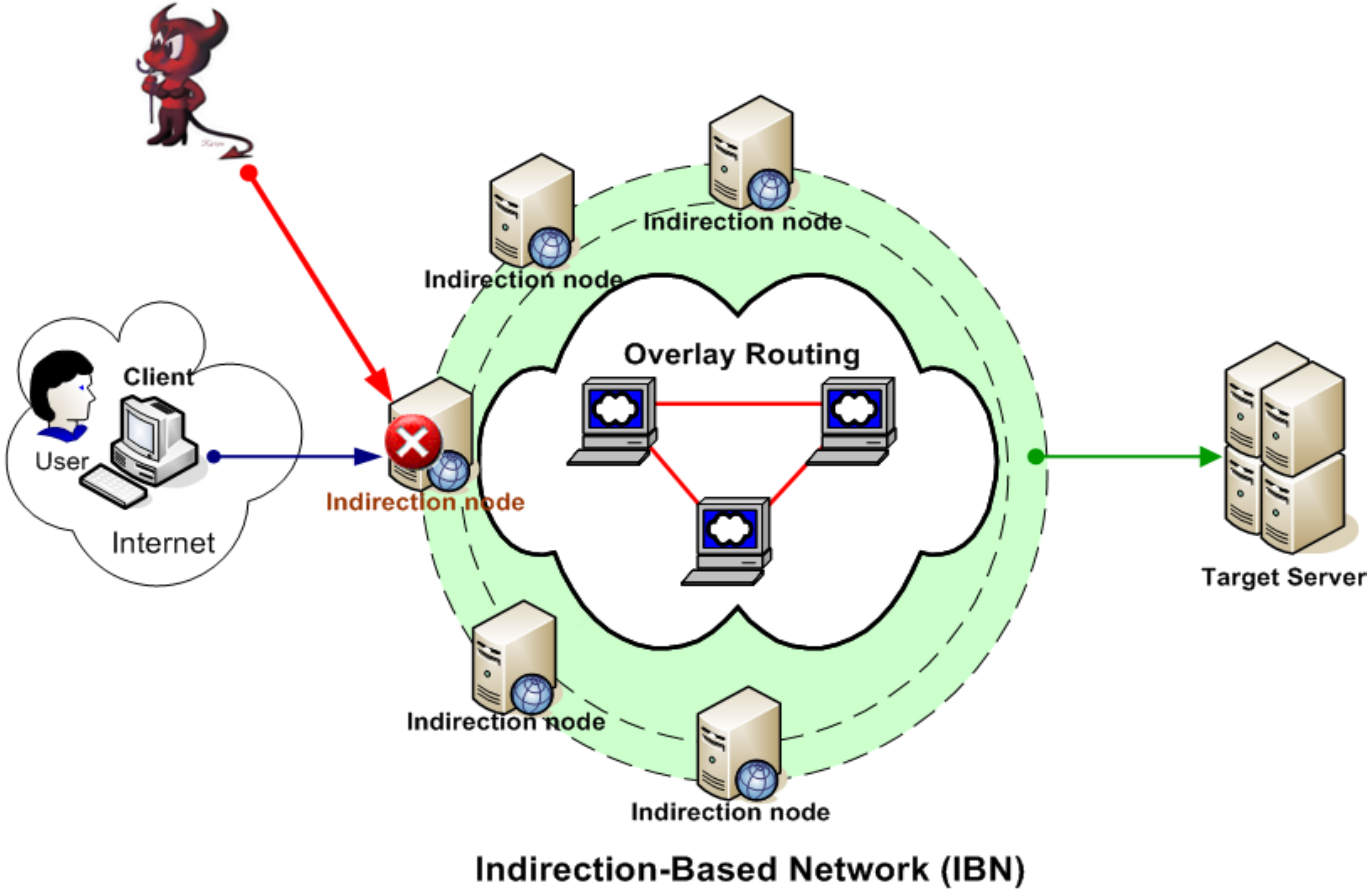
New Attack: Sweeping Attack



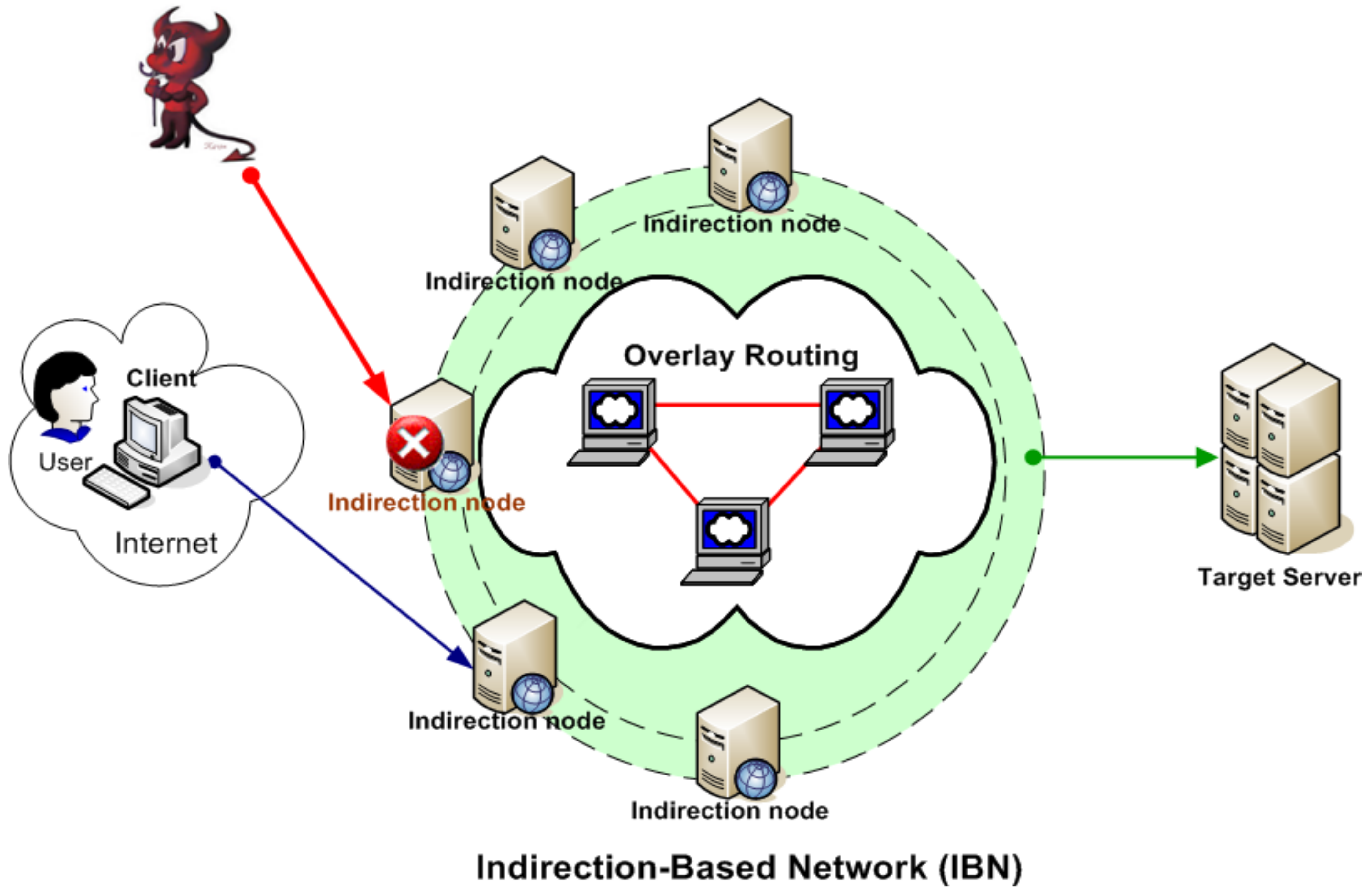
New Attack: Sweeping Attack



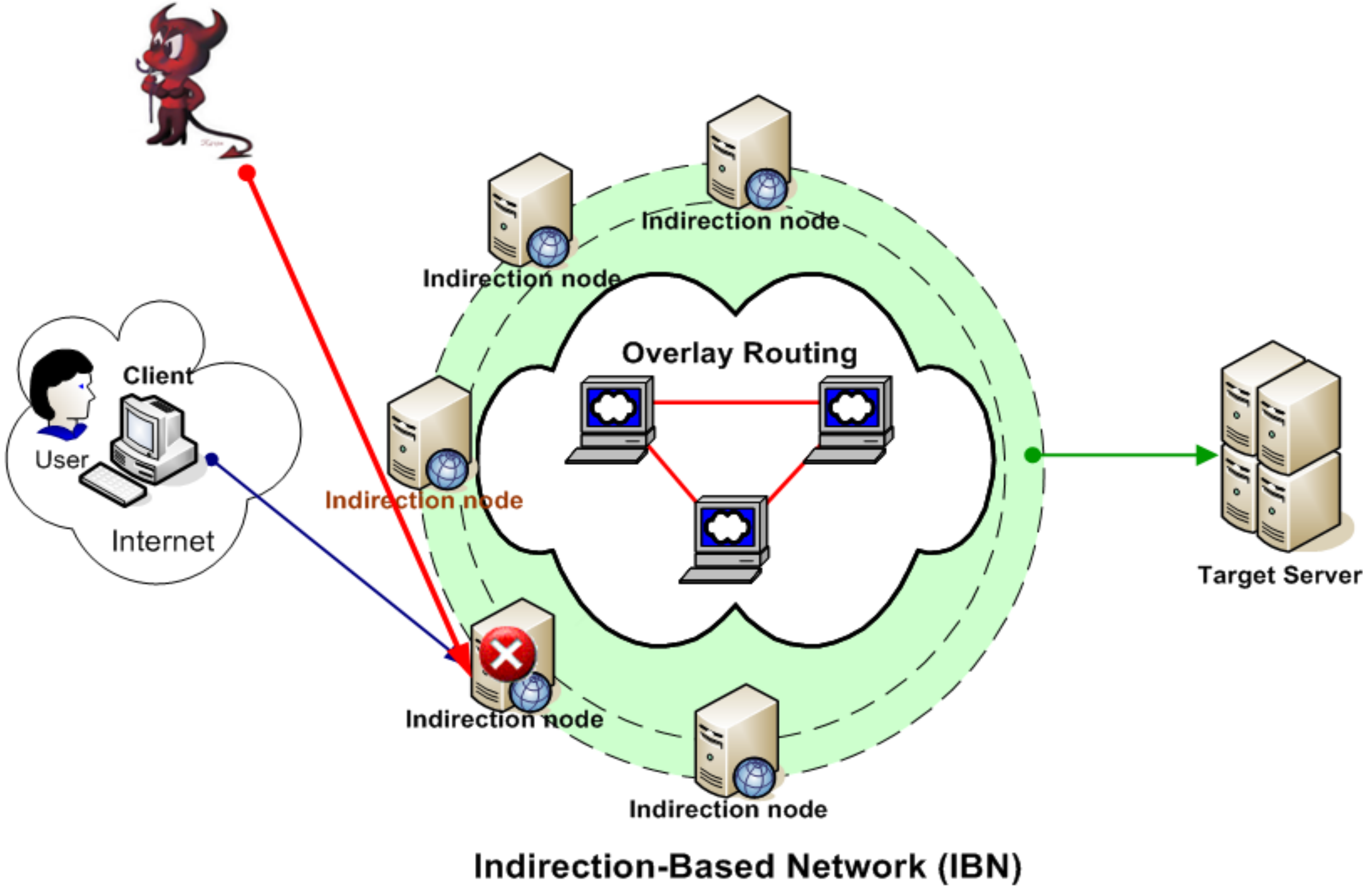
New Attack: “Stalker” Attack



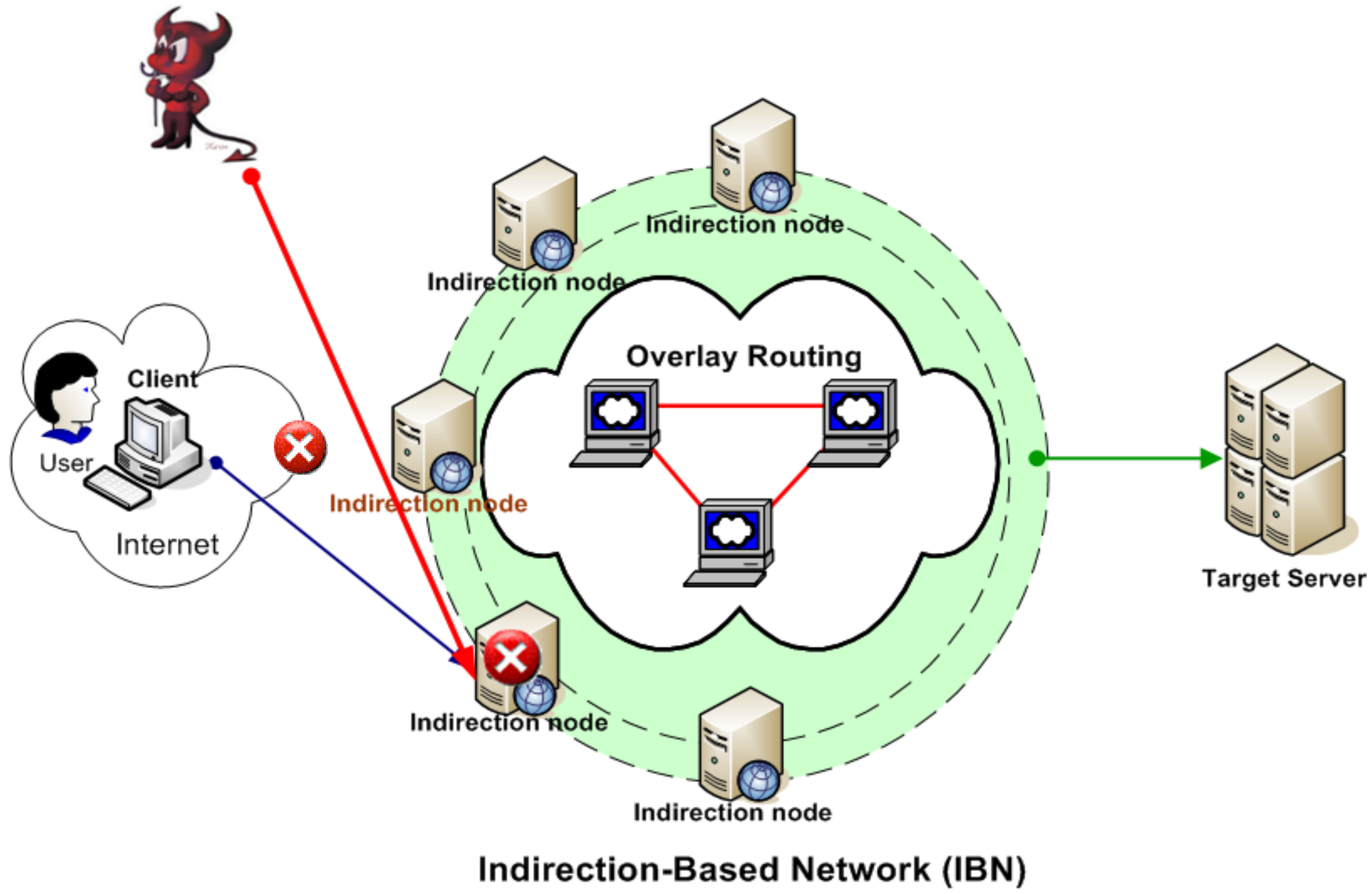
New Attack: “Stalker” Attack



New Attack: "Stalker" Attack

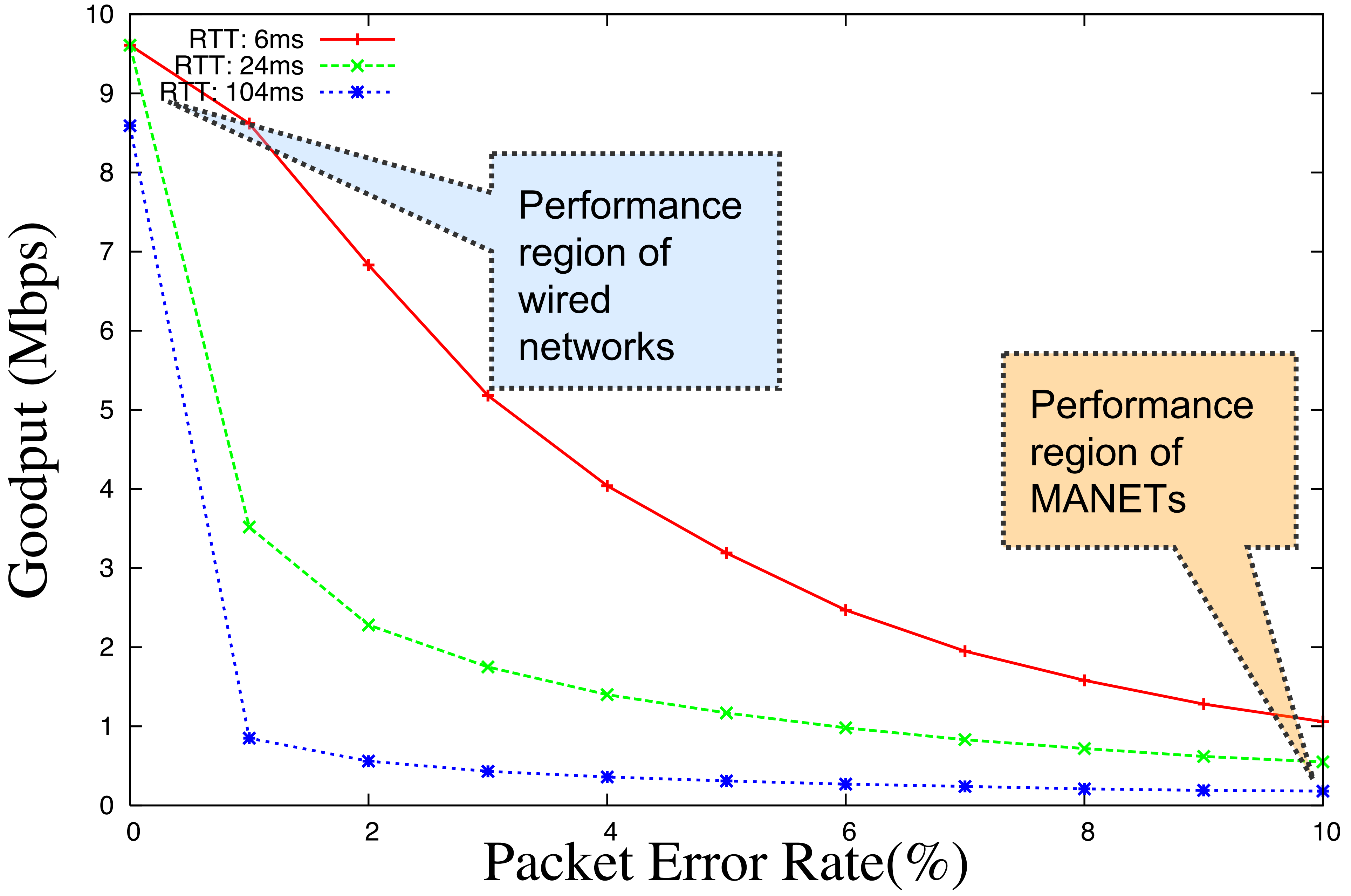


New Attack: “Stalker” Attack



Resilience Results: Throughput

Throughput vs Error Rate in regular TCP

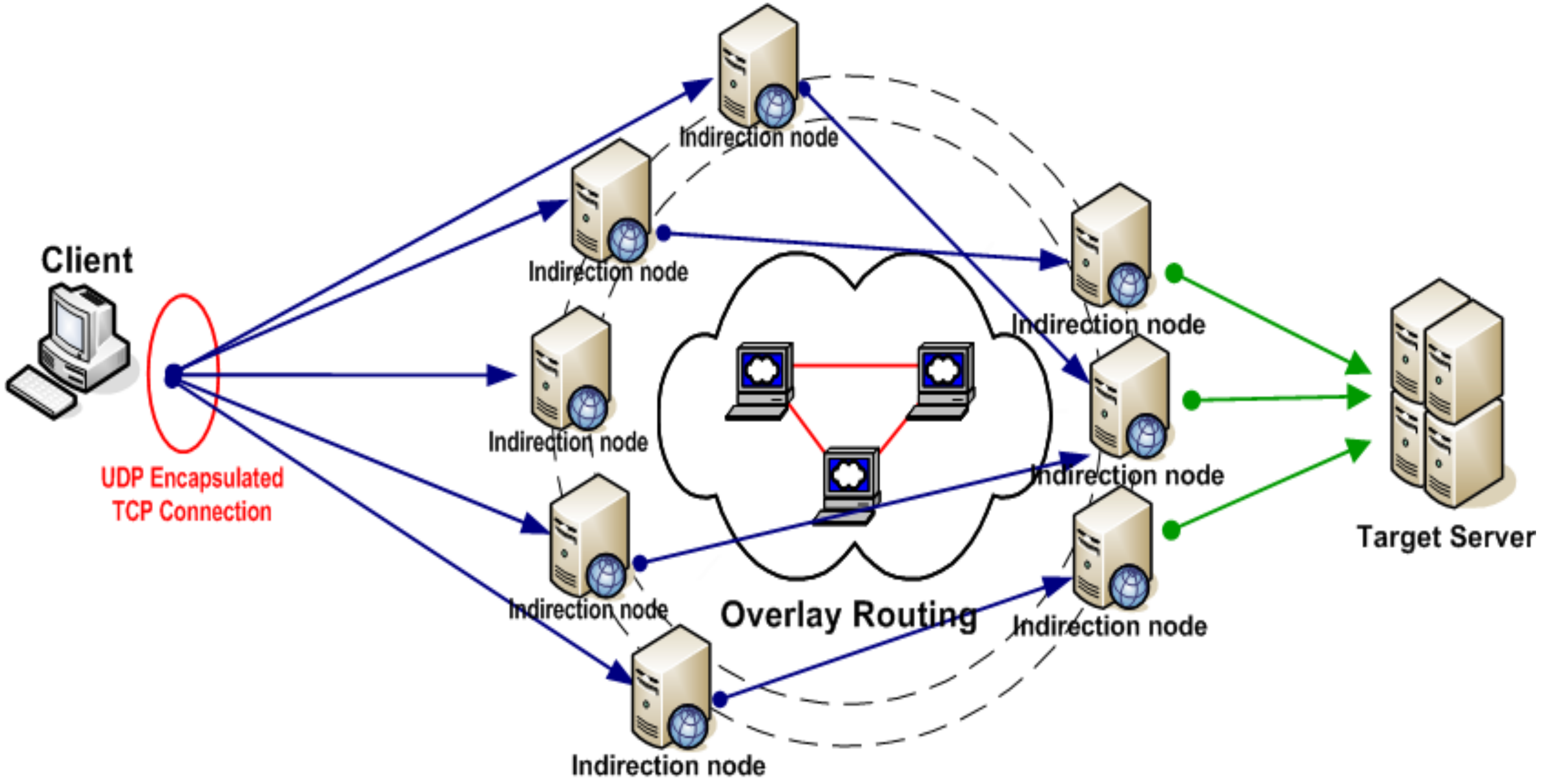


Performance region of wired networks

Performance region of MANETs

Source: Robust TCP for Large-Bandwidth Delay, Packet Erasure and Multi-Path Environments.
Shivkumar Kalyanaraman (RPI), K.K. Ramakrishnan (AT&T Labs Research)

Fix attempt: use many entry points



Indirection-Based Network (IBN)

But this solution increases the state stored!!!

Ticket-based mechanism to the rescue

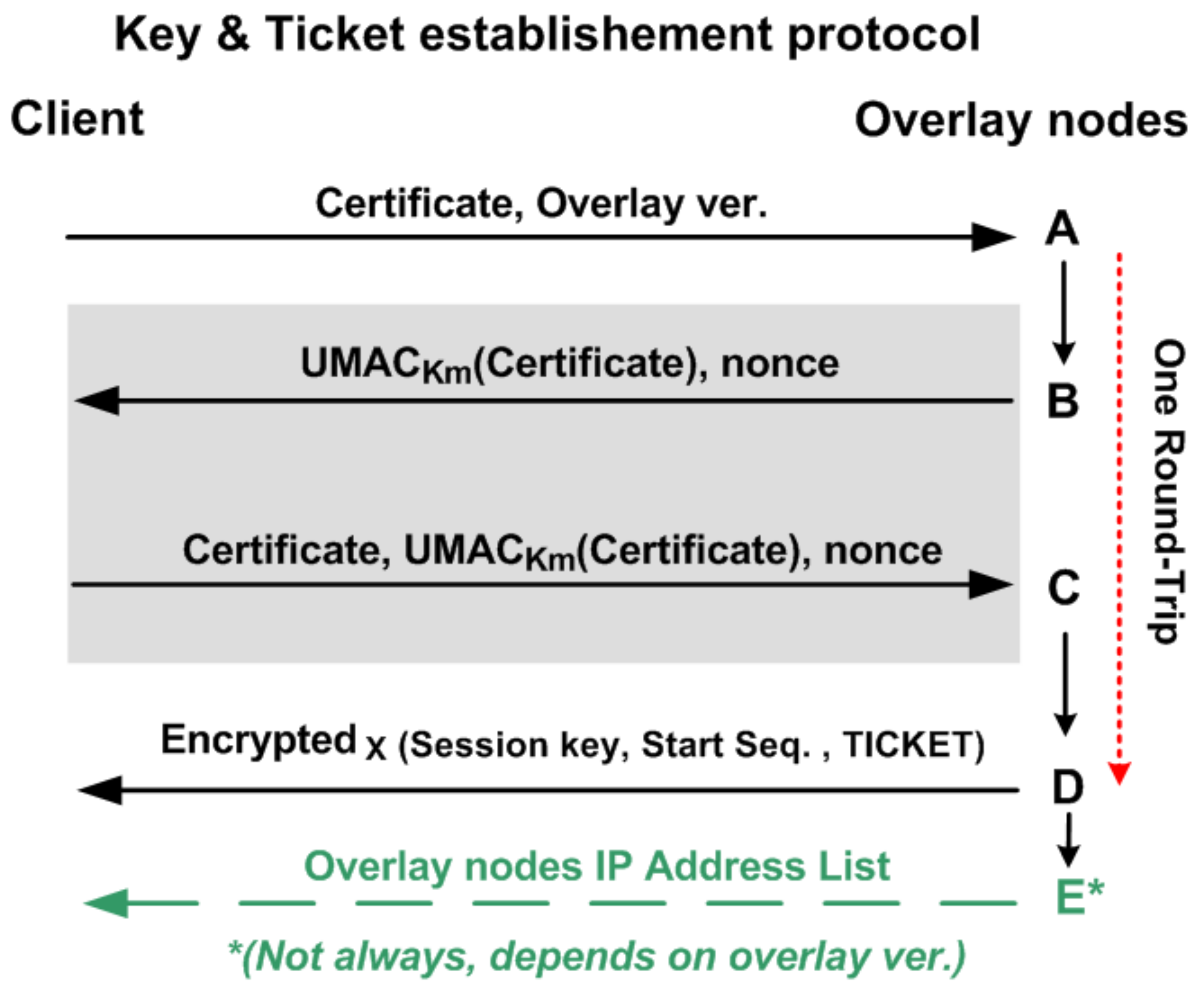
- Move state to the ticket

- Ticket is issued by the Overlay using a shared key

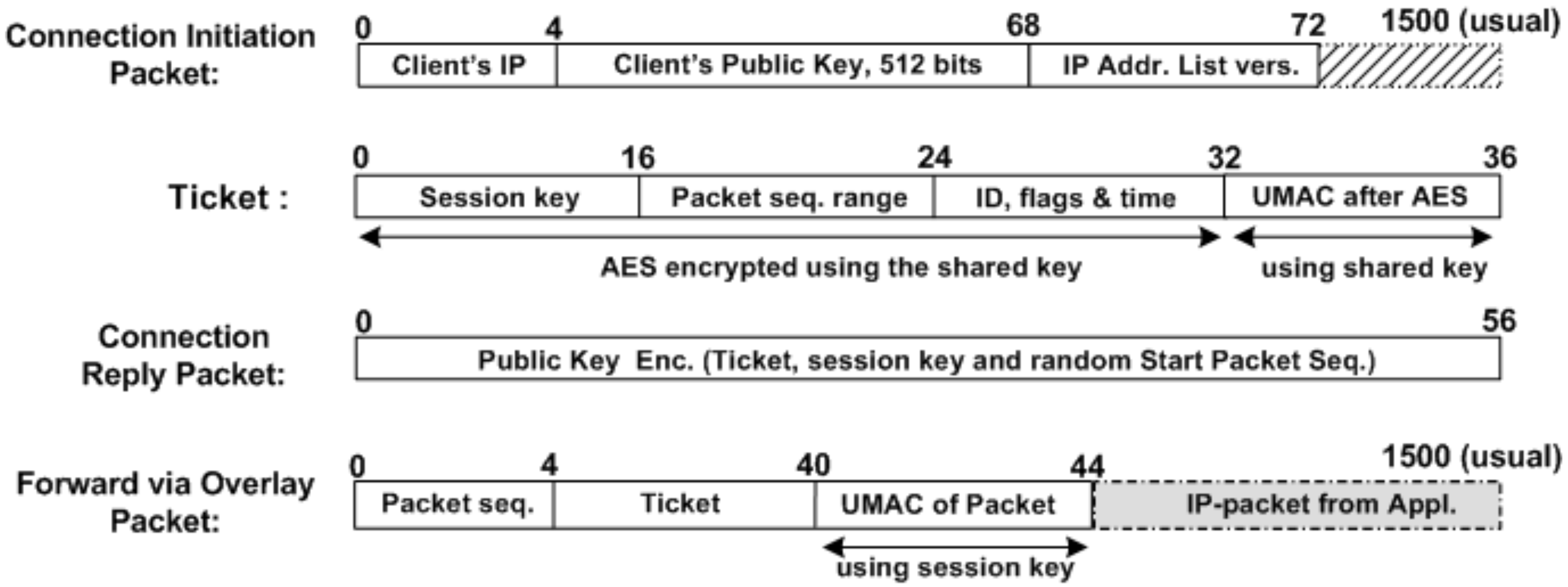
- Ticket becomes a contract between the user and the overlay

- Use of a shared key guarantees honor of the agreement

Key & Ticket Establishment protocol

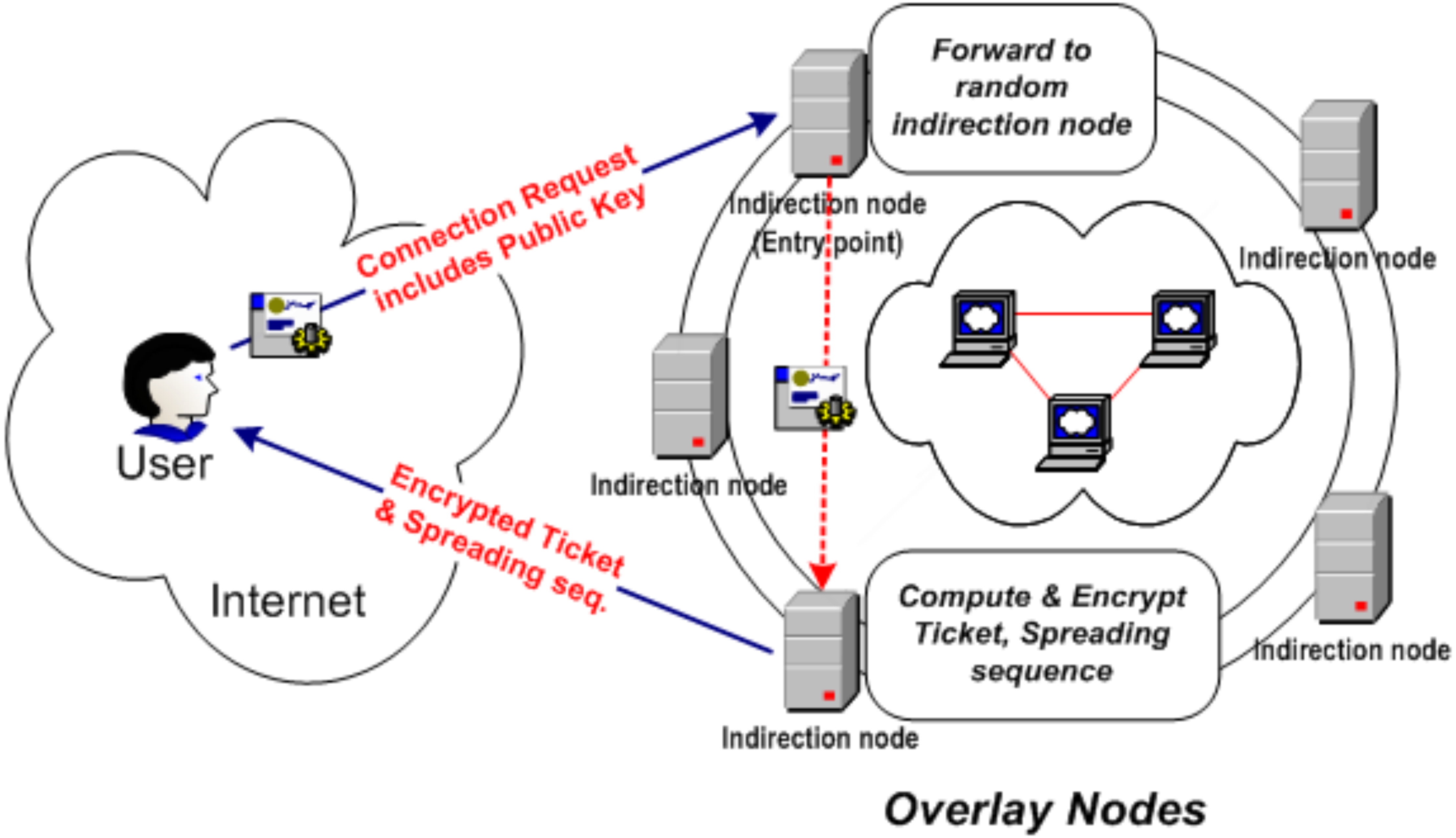

Key & Ticket establishement protocol
Client
Overlay nodes
Certificate, Overlay ver.
A
UMAC$_{Km}$(Certificate), nonce
B
Certificate, UMAC$_{Km}$(Certificate), nonce
C
One Round-Trip
Encrypted$_{X}$ (Session key, Start Seq. , TICKET)
D
Overlay nodes IP Address List
E*
*(Not always, depends on overlay ver.)

Ticket Design

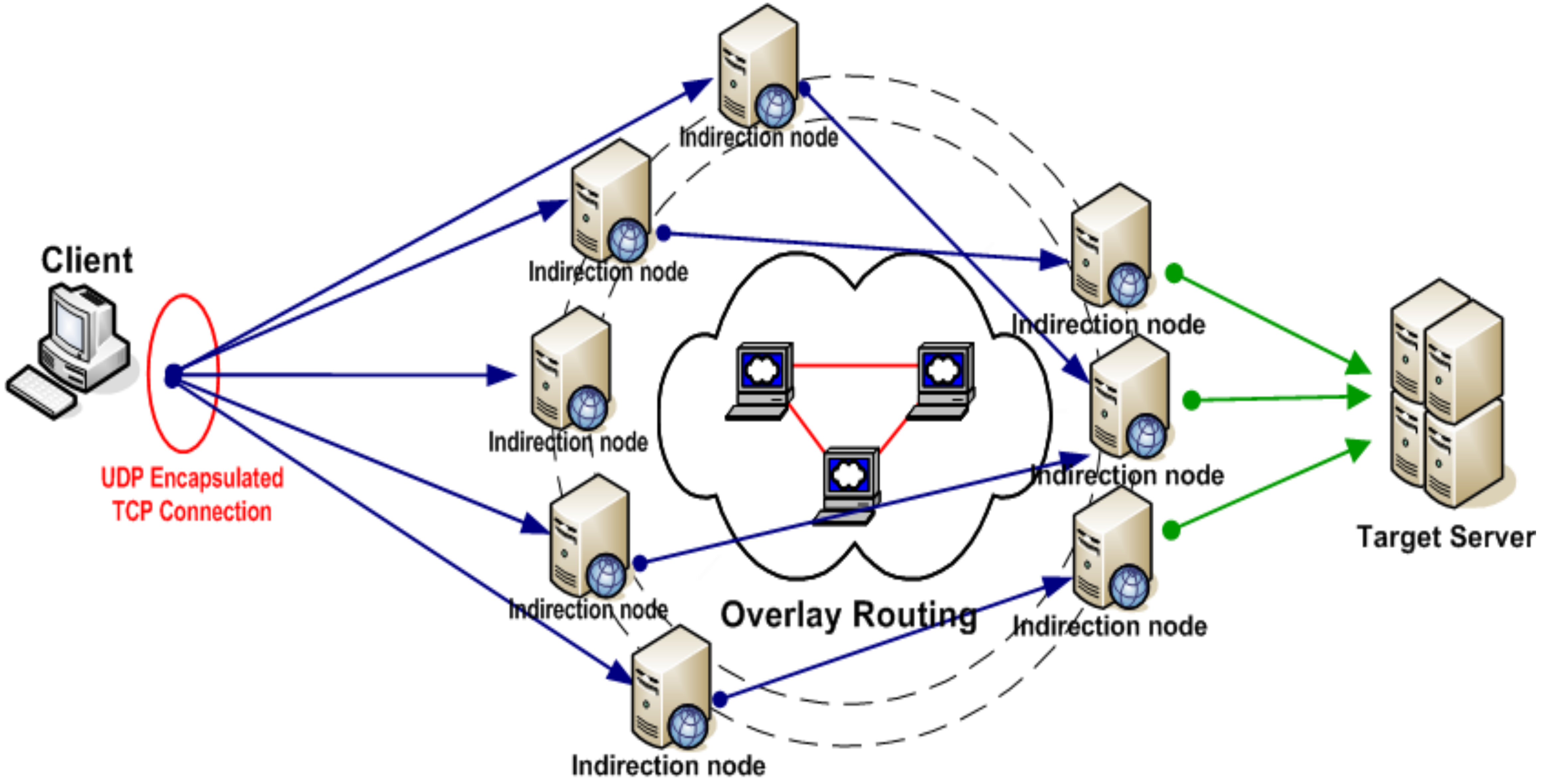


- Random spreading sequence protects against "stalker" attacks
- Packet sequence range guarantees traffic control
- Ticket design and issue protocol prevent replay, spoofing and computational attacks

Client Connection Initiation



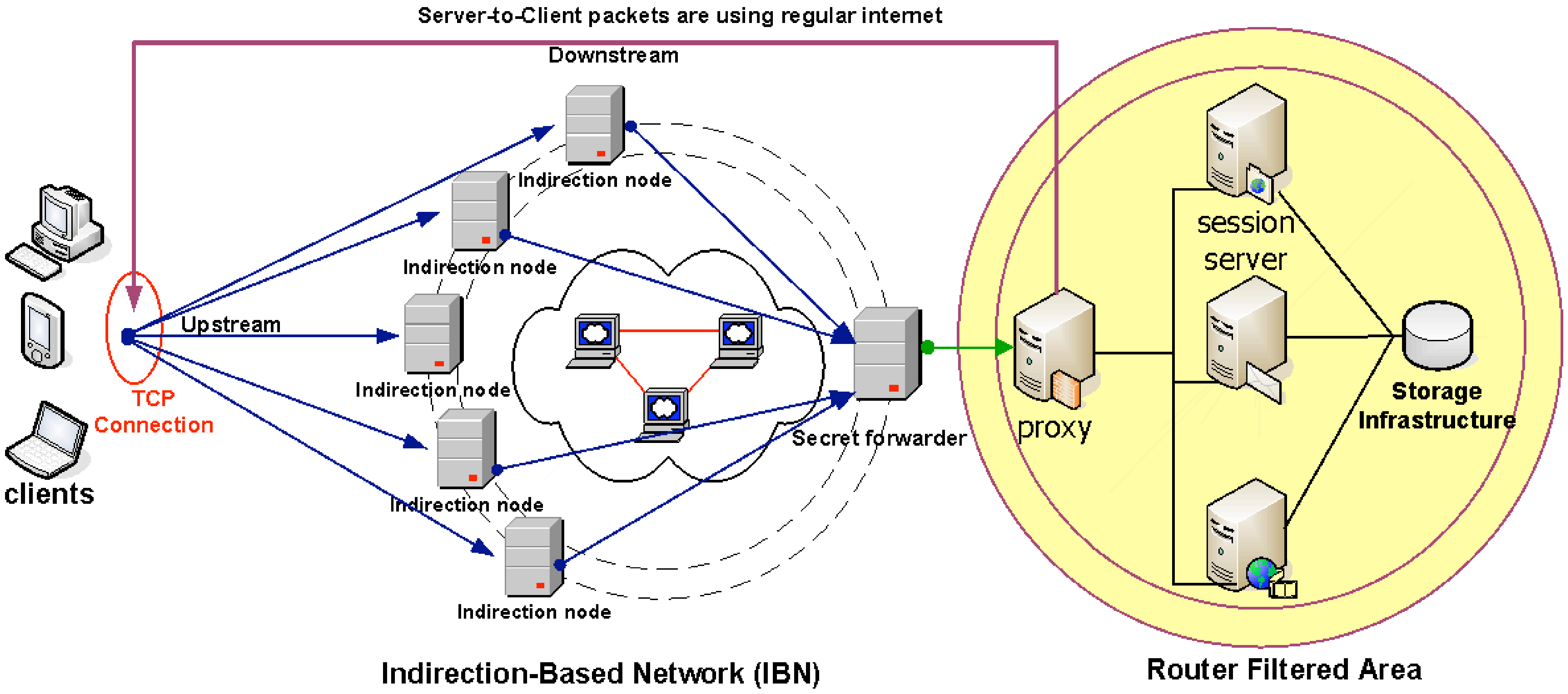
Spread Spectrum Architecture - Replication



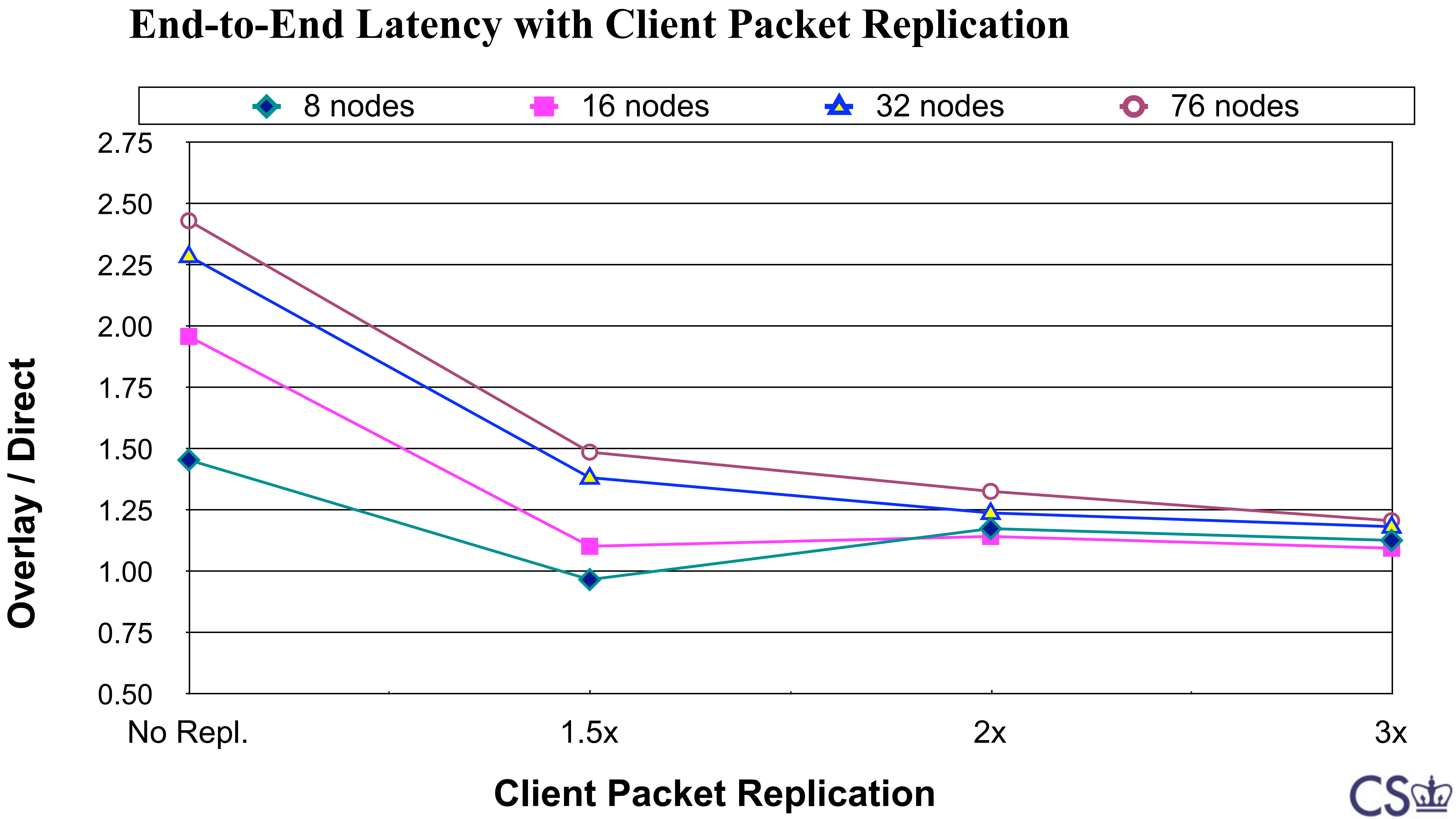
Indirection-Based Network (IBN)

Multi-Path + Spreading + Ticket allows Packet Replication

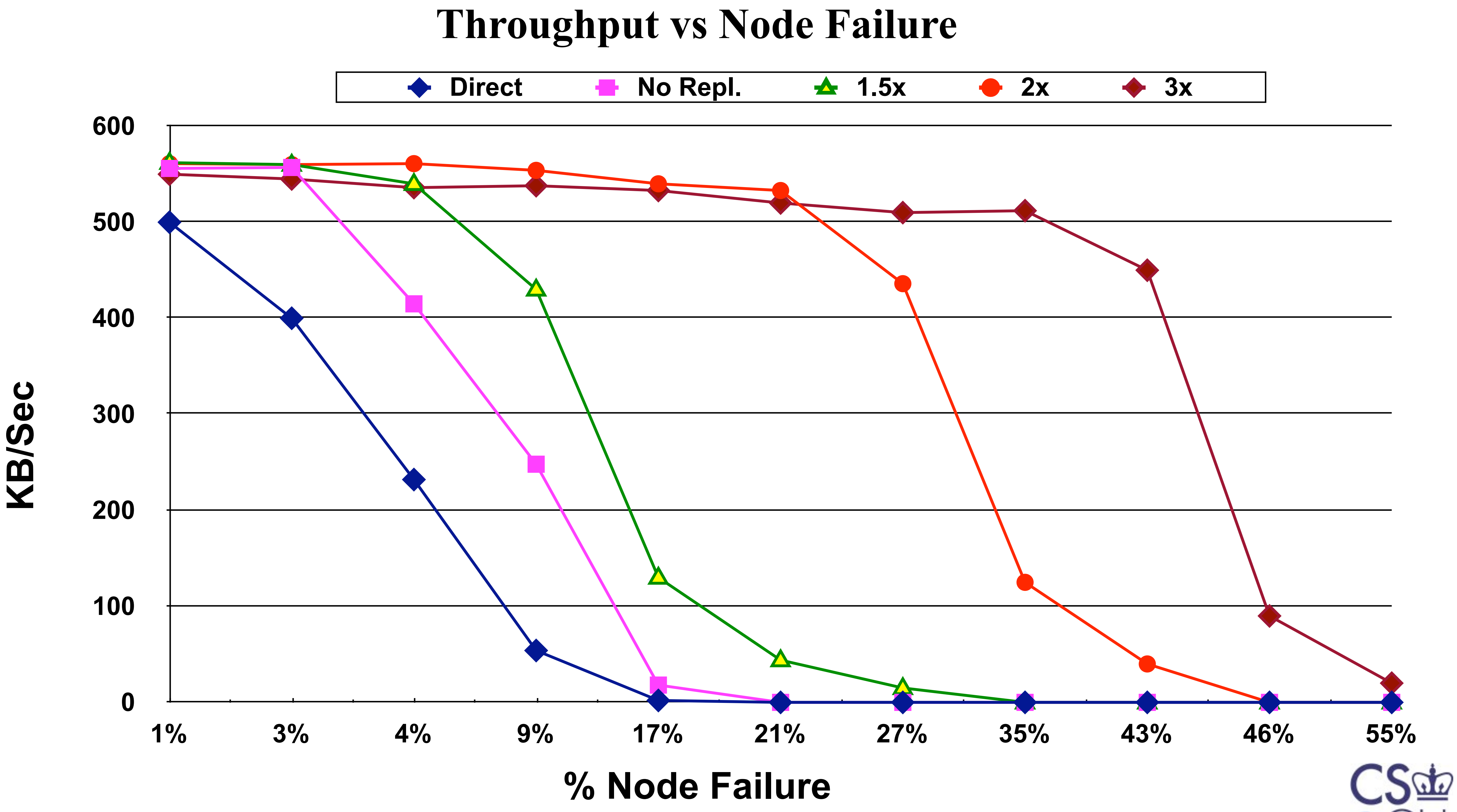
A2M: Access Assured Mobile Desktop Computing



Performance Results: Latency

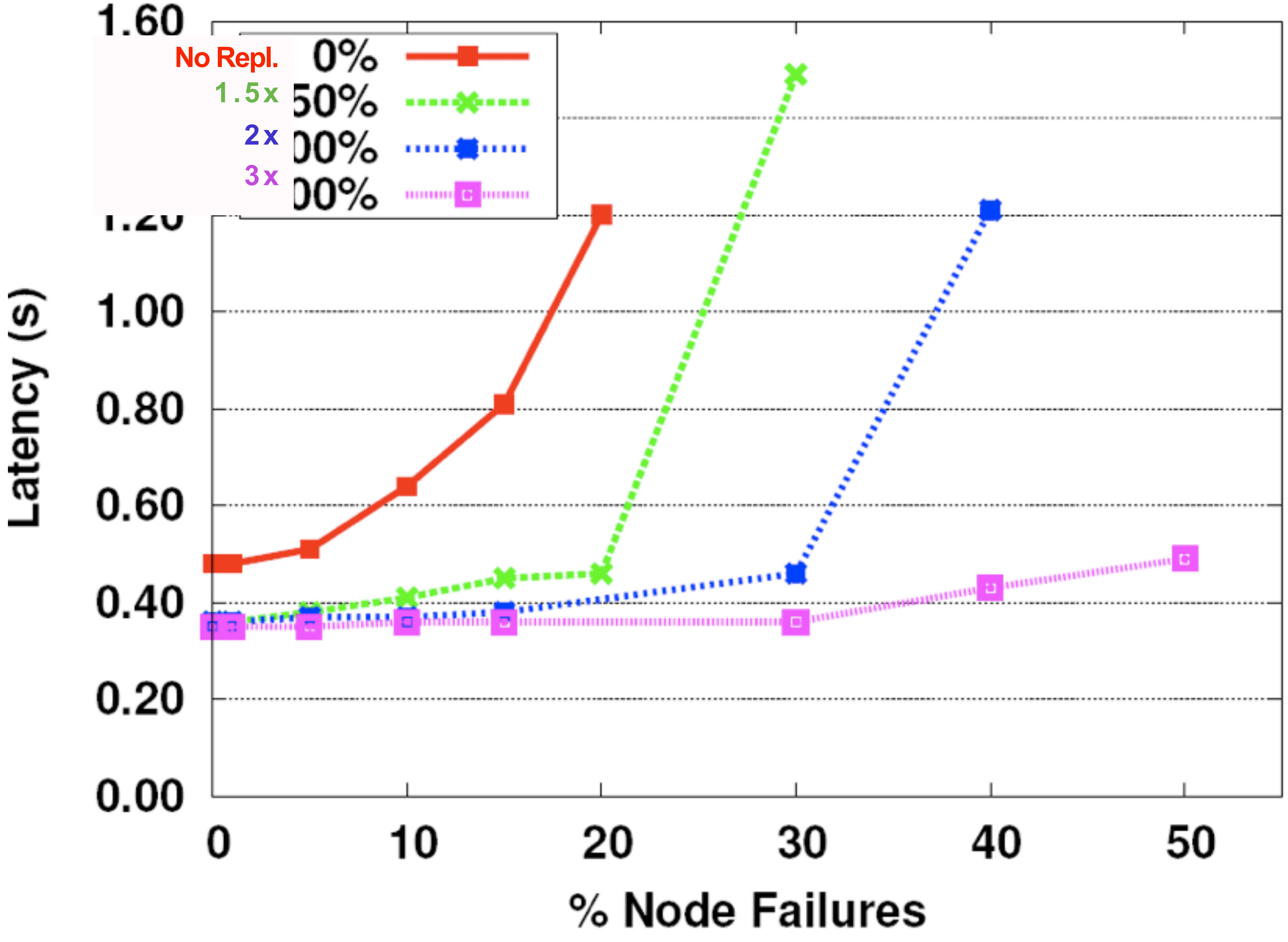


Resilience Results: Throughput



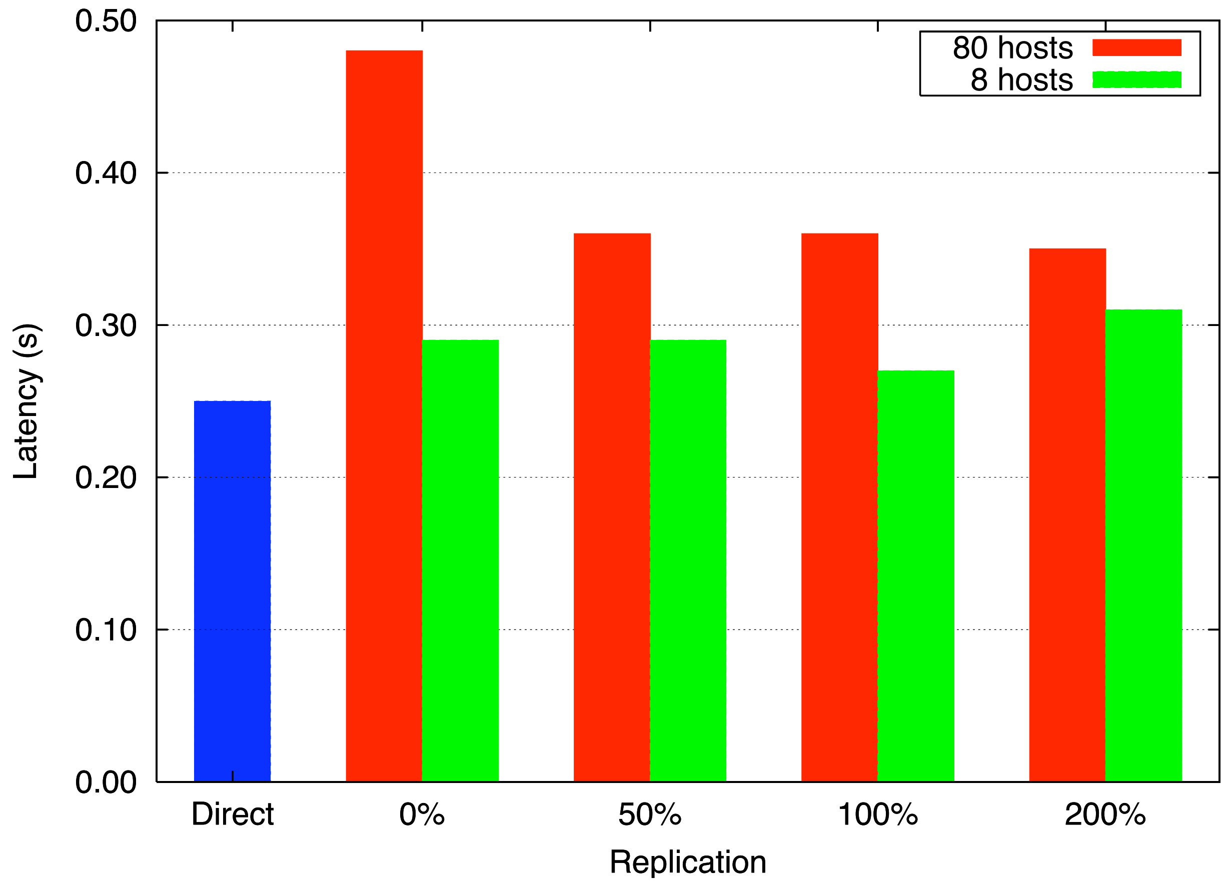
Resilience Results: Latency (Web)

End-to-End Latency vs Node Failure (Web)

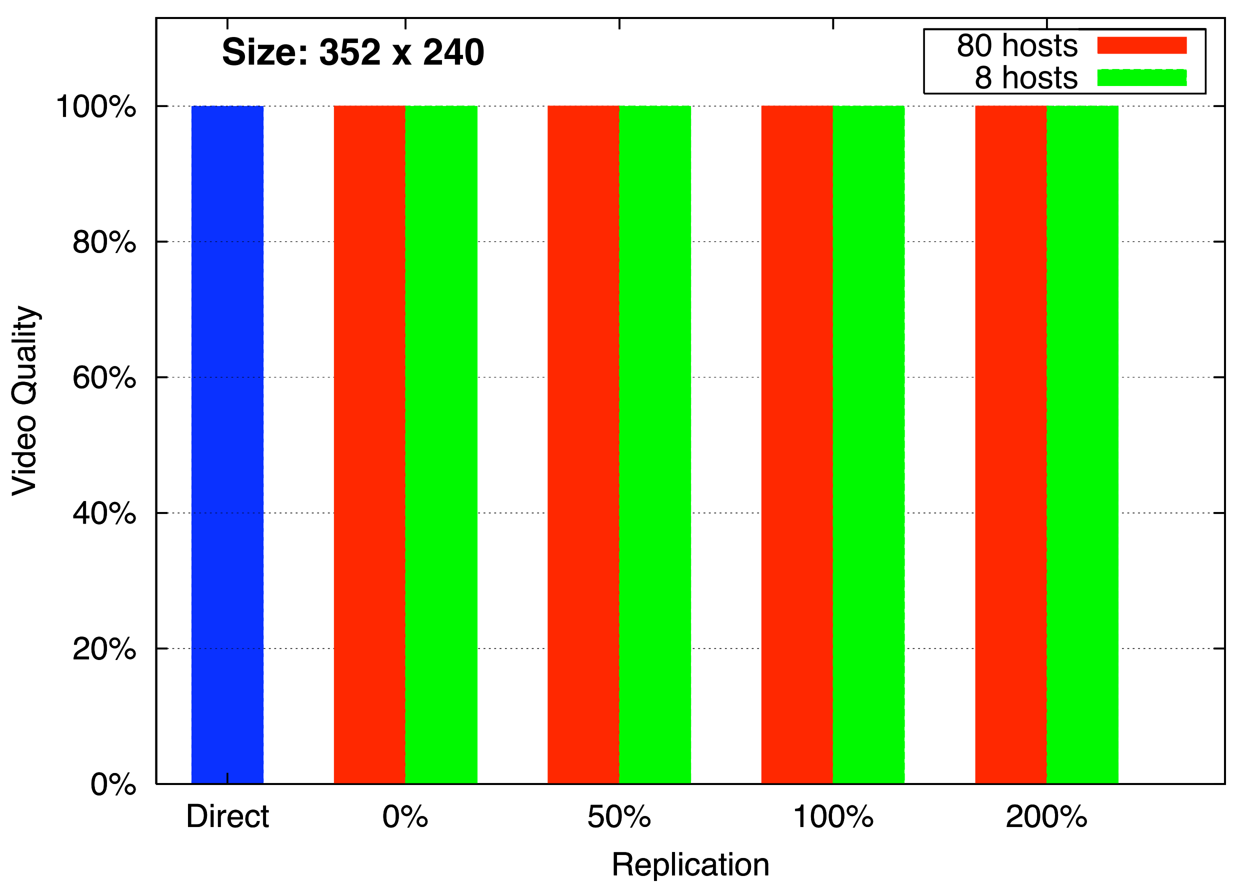


CS@CU

Performance Results: Latency (Web)

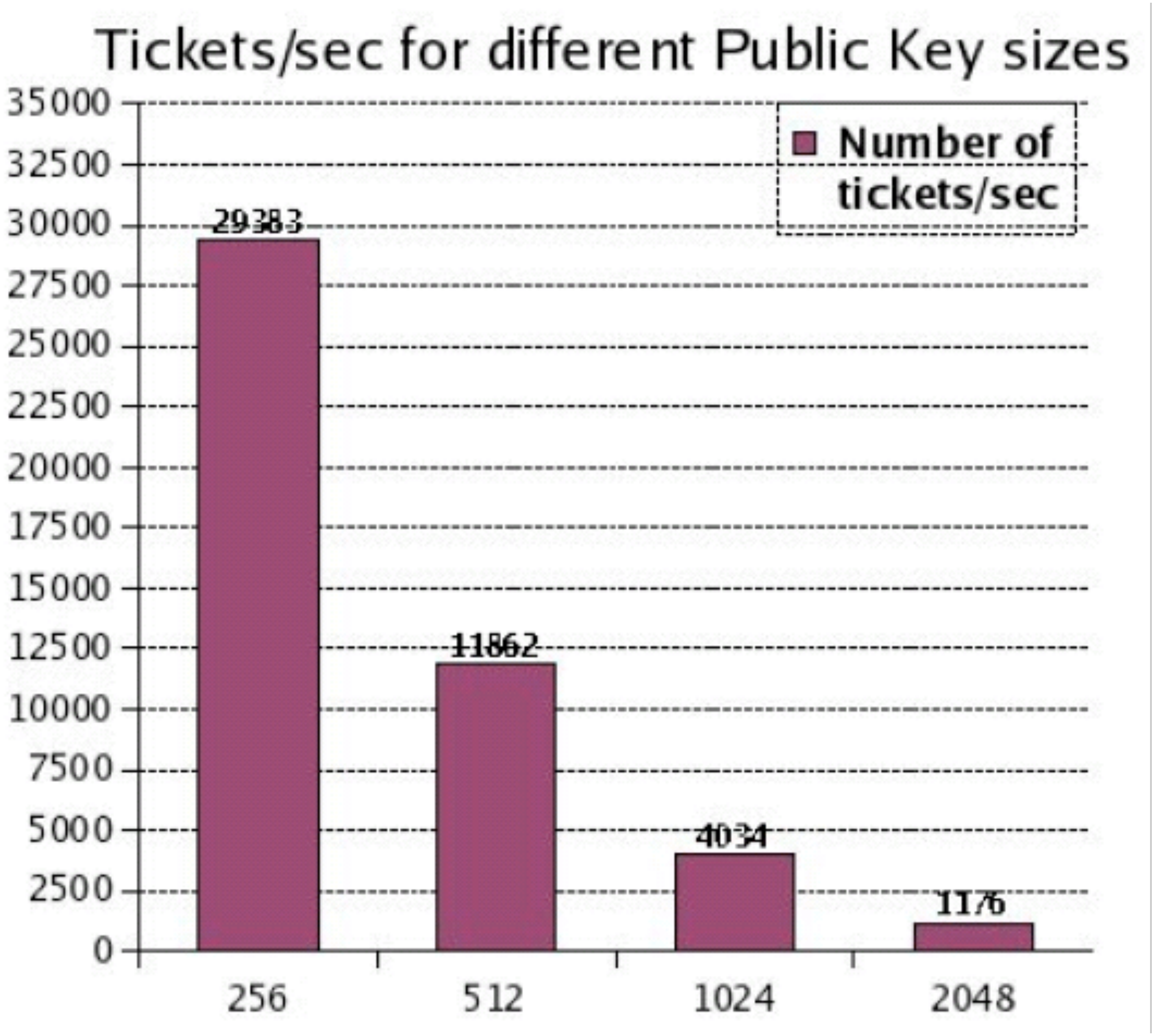


Web Latency vs Packet Replication

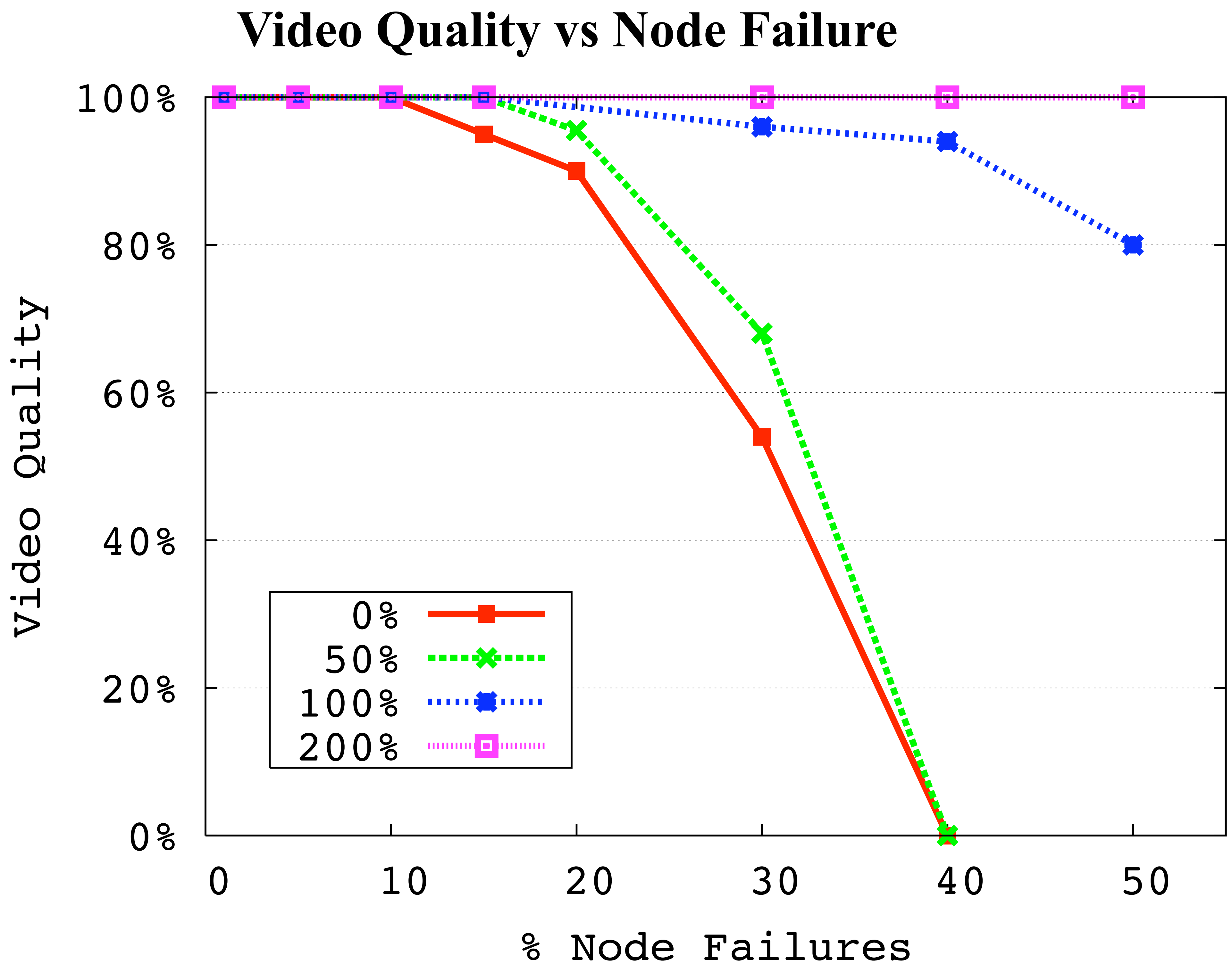


Video Quality vs Packet Replication

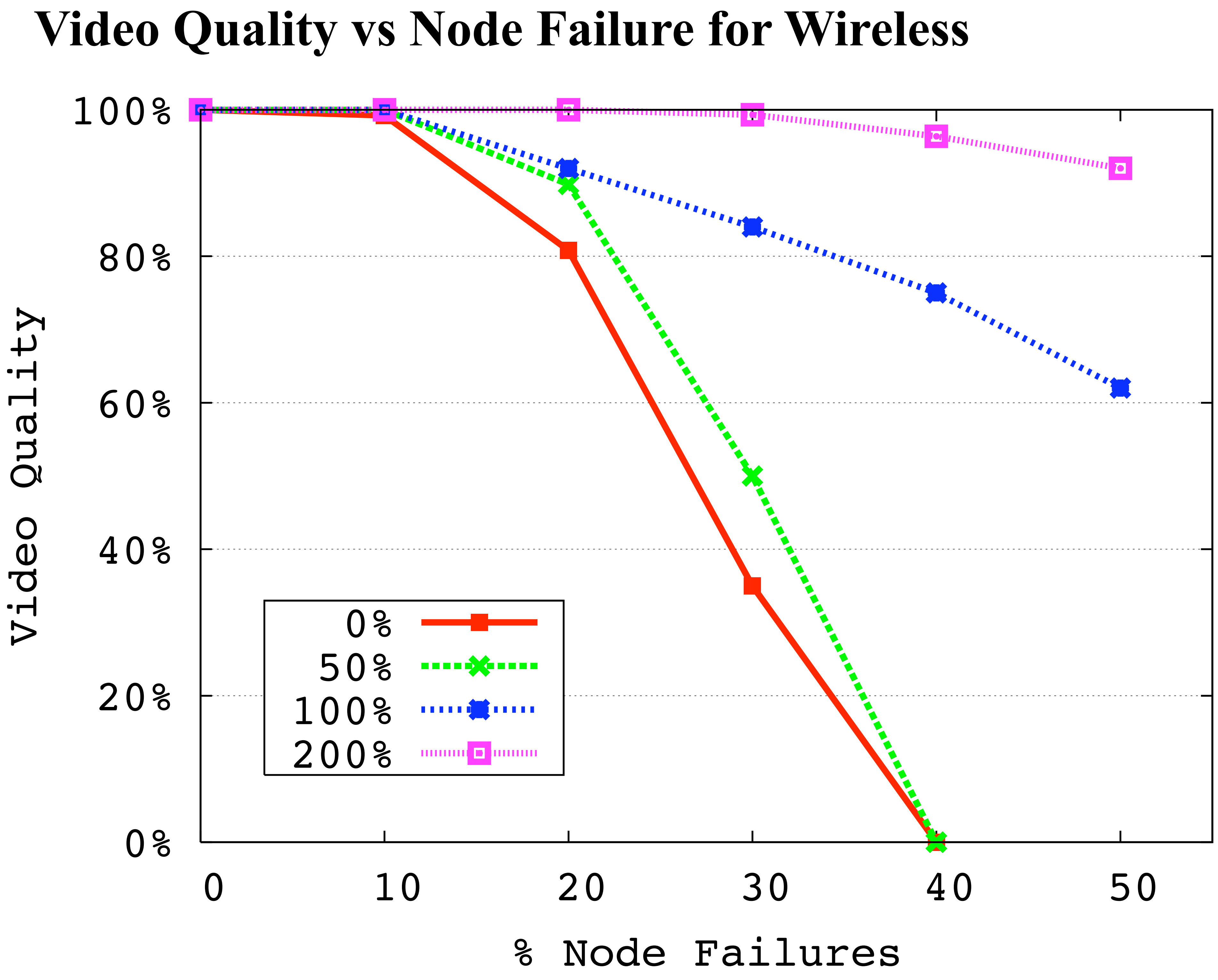
Ticket Generation Benchmark



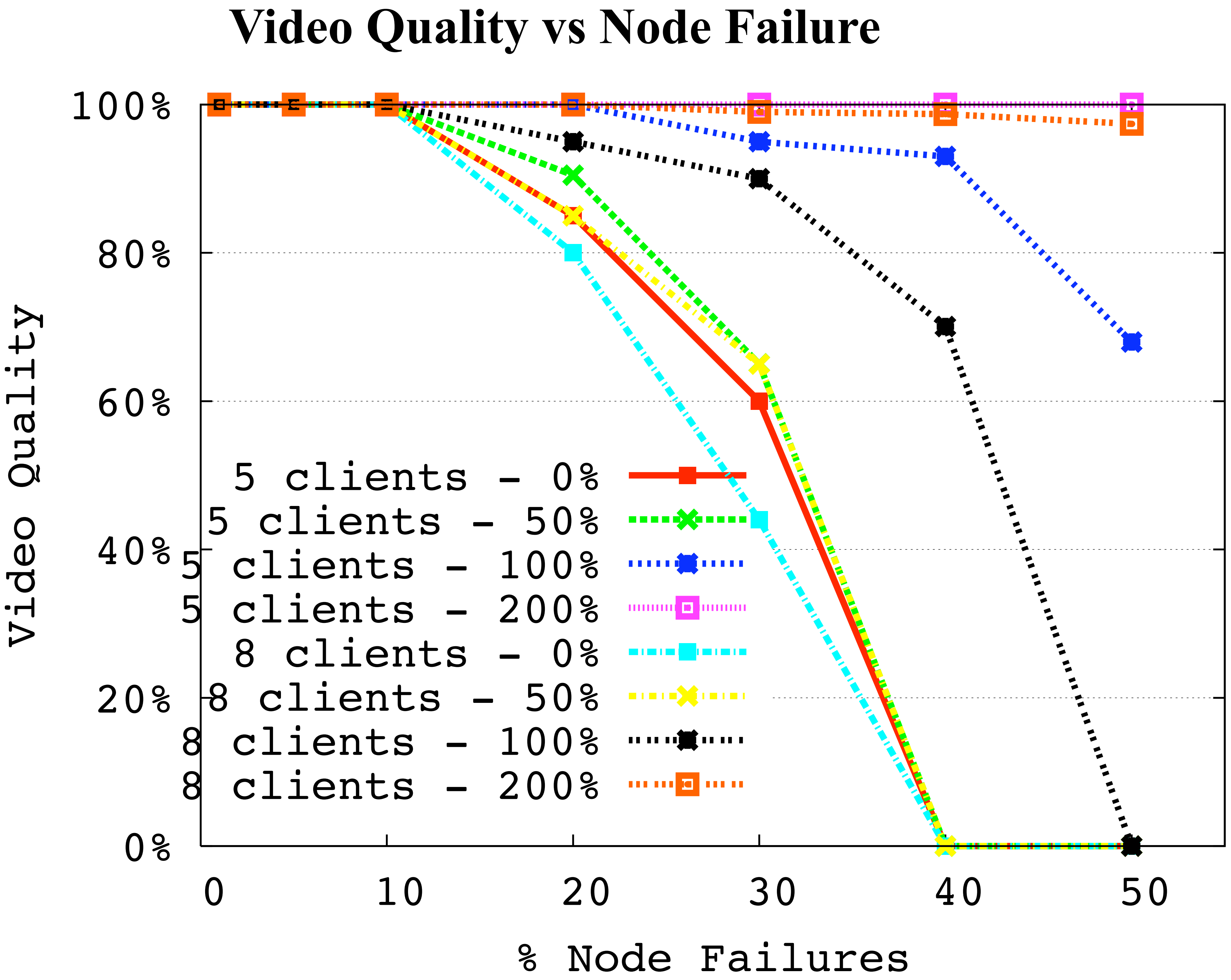
Resilience Results: Video Streaming



Resilience Results: Video Streaming



Resilience Results: Video Streaming



TCP Friendliness of Approach

- Initial implementation non-TCP friendly provided the worst case scenario (use of non-responsive channels)
- Current implementation encodes path in the TCP options field for acknowledgments generating a different TCP-window for each path
- Works for regular TCP, UDP, and UDP-encapsulated TCP
- Existence of multiple paths makes attacks against TCP more difficult

Conclusion

- Recent events have demonstrated the continued and real threat of DDoS as an effectve instrument of both cyber-warfare and cyber-crime

- Overlay-based mechanisms can mitigate the impact of large DDoS attacks
  - Topology- and provider-independent deployment at relatively low cost
  - Performance impact low (< 10%), only incurred during attack periods
  - A pan-European DDoS Protection Network?
    - Leverage PlanetLab/GRID sites as "seeds"

What is the underlying problem?

How clients connect to the overlay:

- Connection to a single indirection node (entry point)
- Client’s state is stored to this entry point
- End-to-End connection depends on a small but static set of overlay nodes

What is the underlying problem (II)?

How the overlay sees the client:

- User can establish multiple connections to an overlay node
- An authenticated client can inject any amount of traffic to the overlay network
- Even if there is access control in the entry point the user can reset that by attacking the entry point