

Countering DoS Attacks With Stateless Multipath Overlays

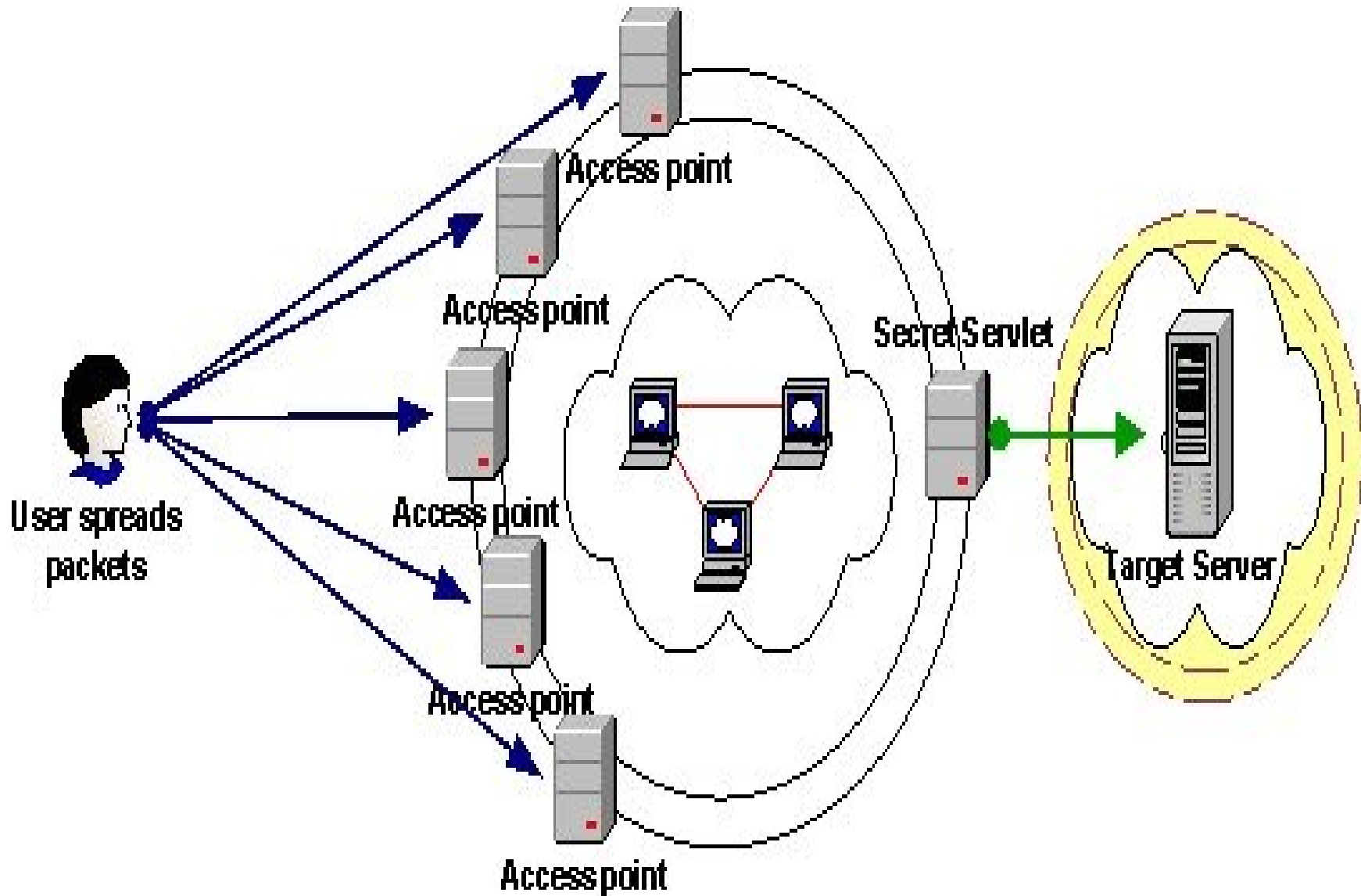
paper authors:
Angelos Stavrou
Angelos D. Keromytis

overview and comments by:
Miika Komu <miika@iki.fi>
18.10.2006

The Idea in a Nutshell

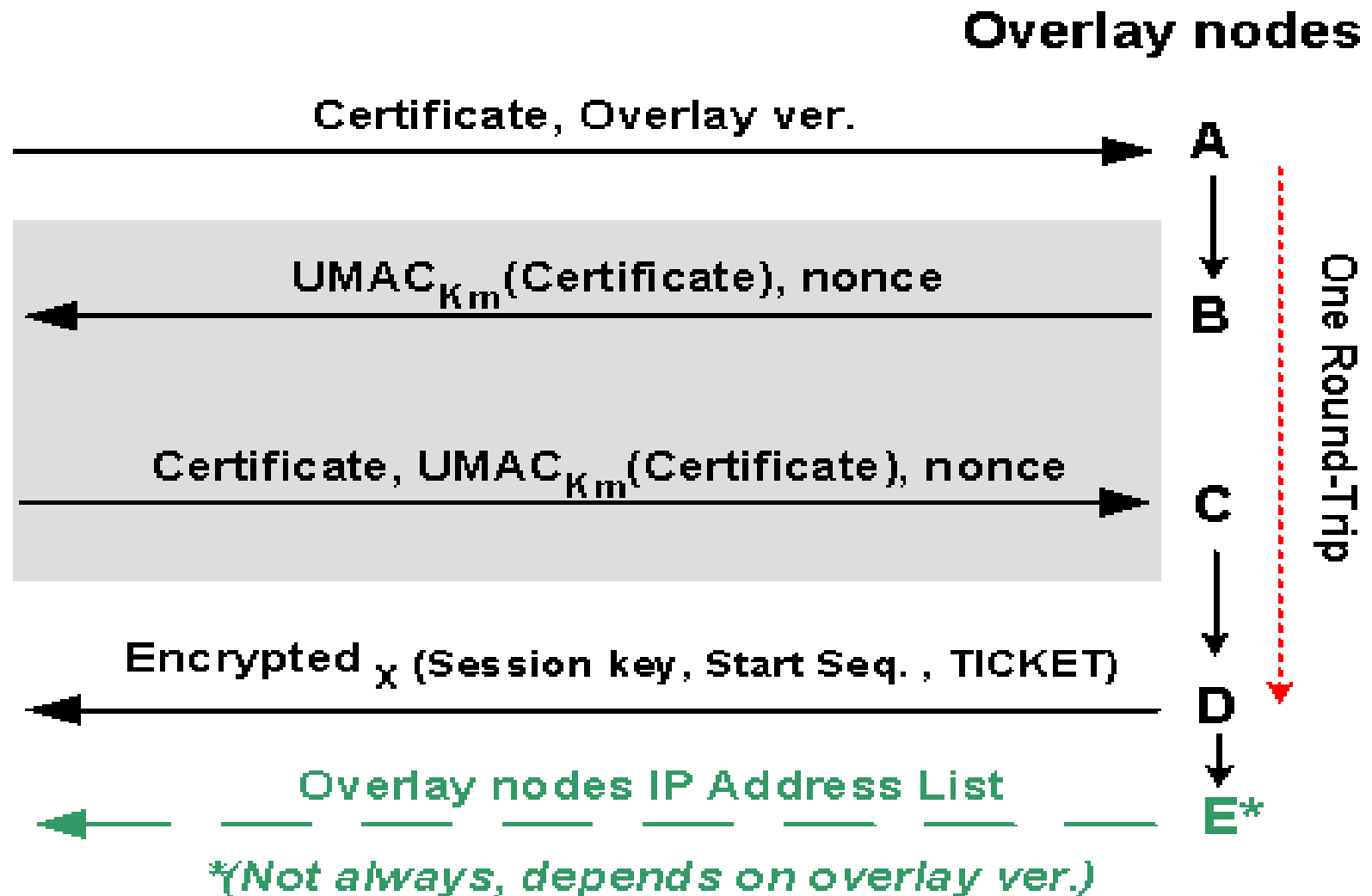
- Protects overlay clients from DDoS attacks
 - DDoS attacks = distributed attacks against the overlay proxies the client is connected to
- Basic mechanism: duplicate and spread traffic through several overlay proxies
 - Includes mechanisms to prevent the abuse the spreading mechanism by attackers

Traffic Spreading / Duplication

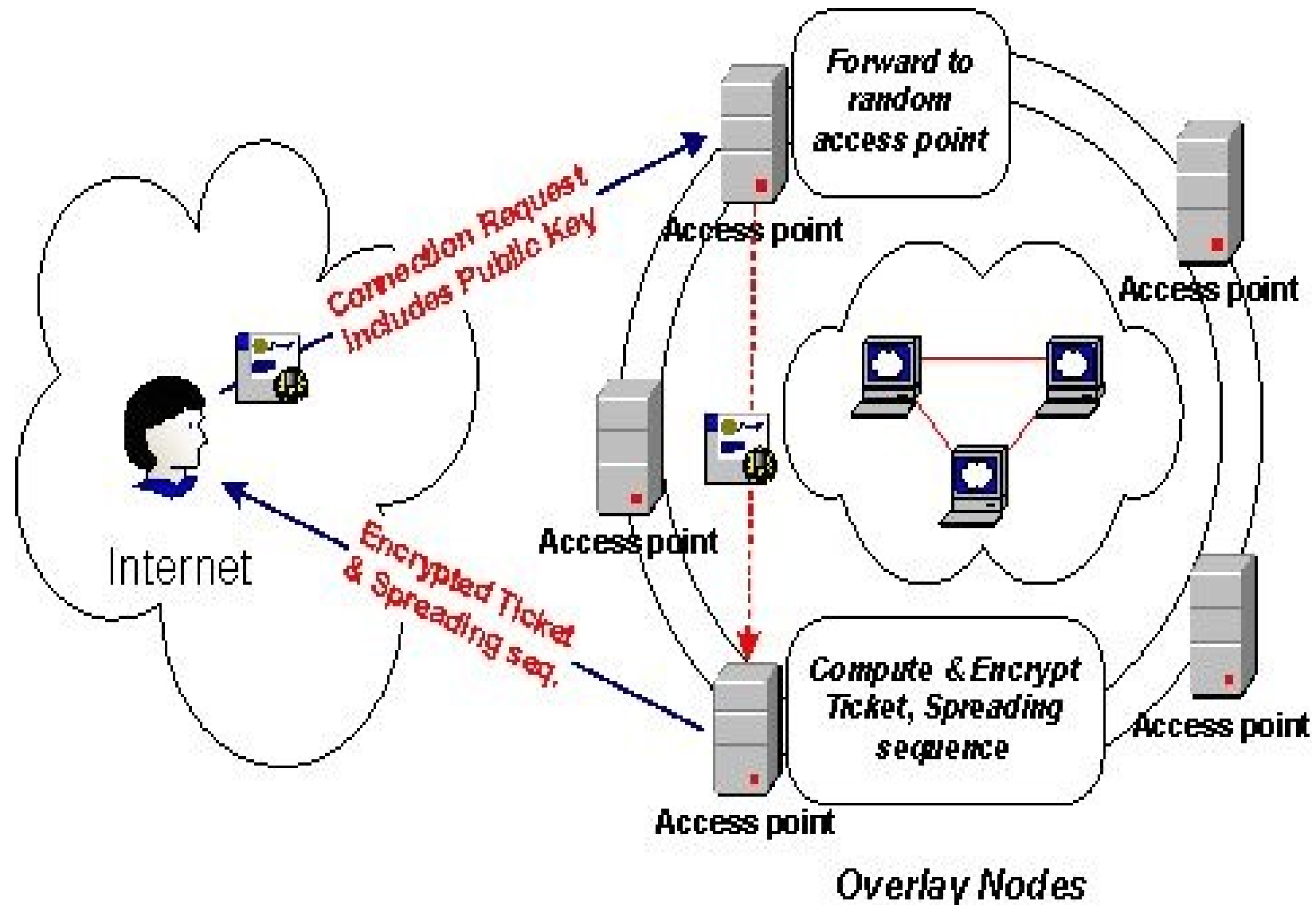


Packet Sequences

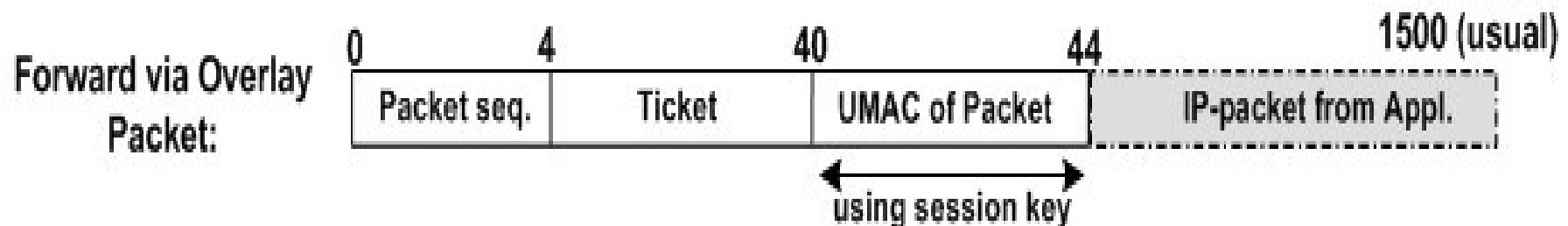
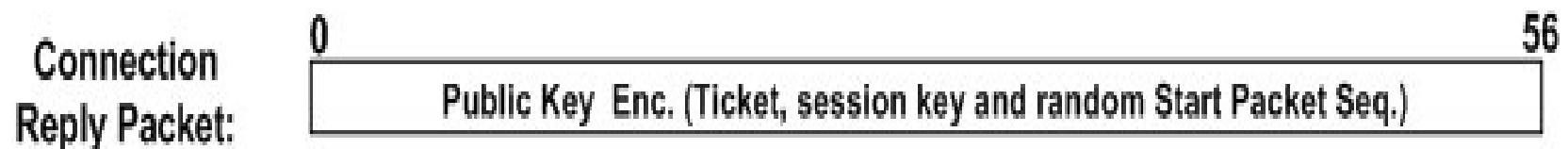
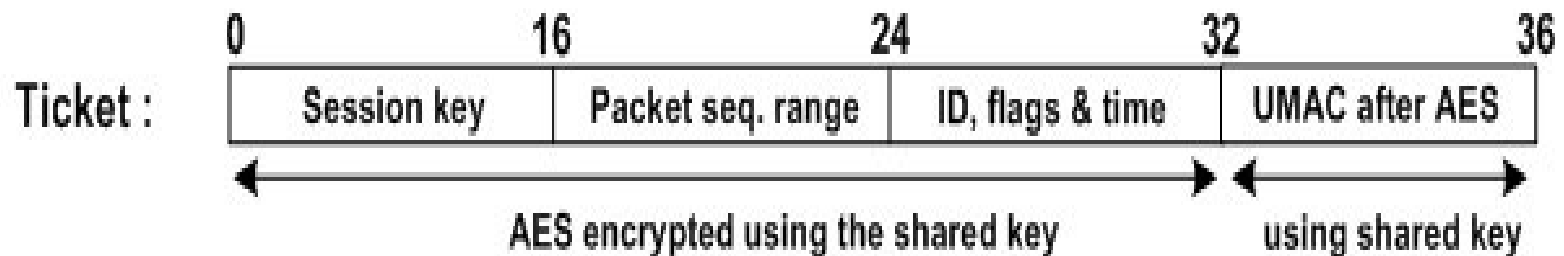
Key & Ticket establishment protocol



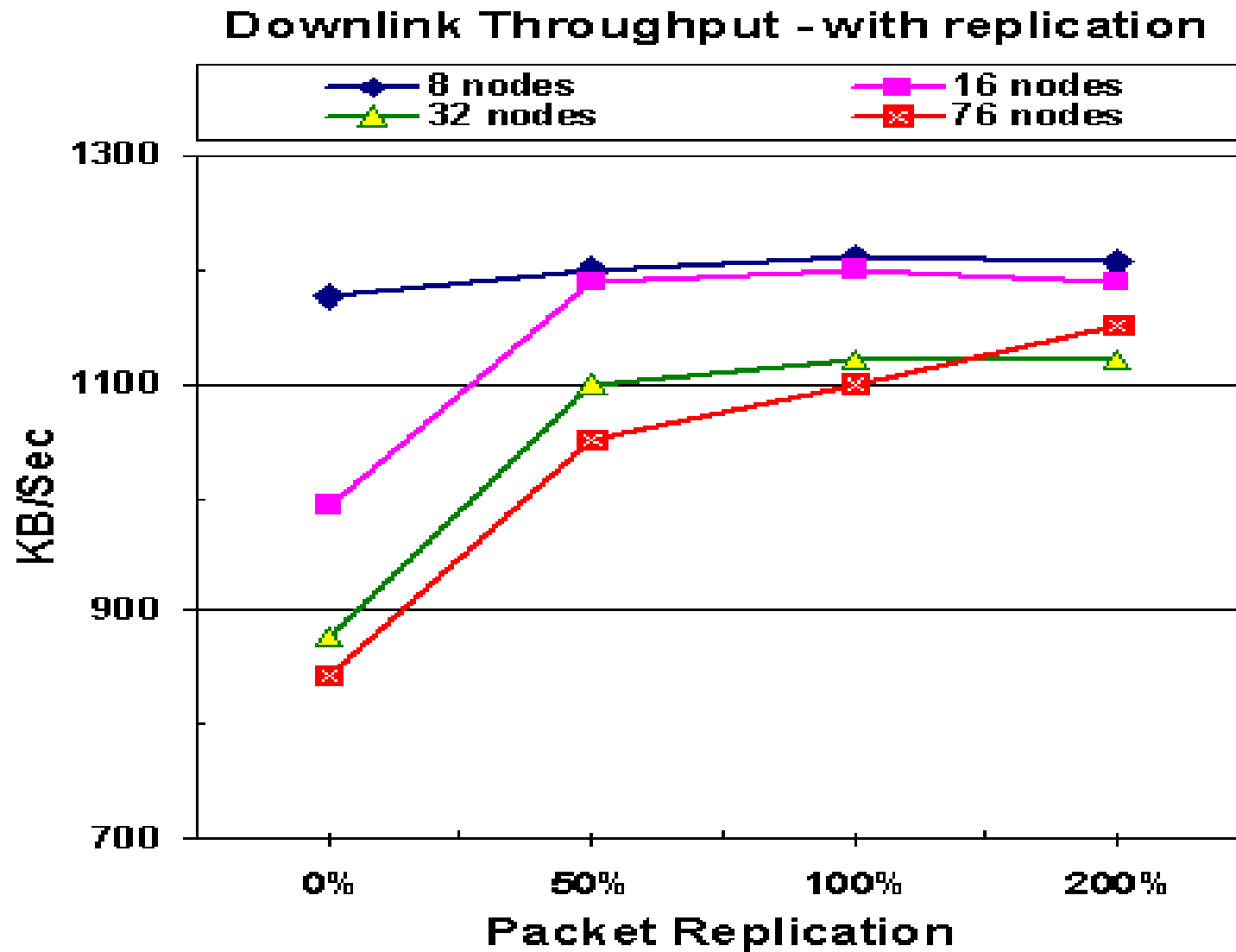
Distributed Ticket/Key Protocol



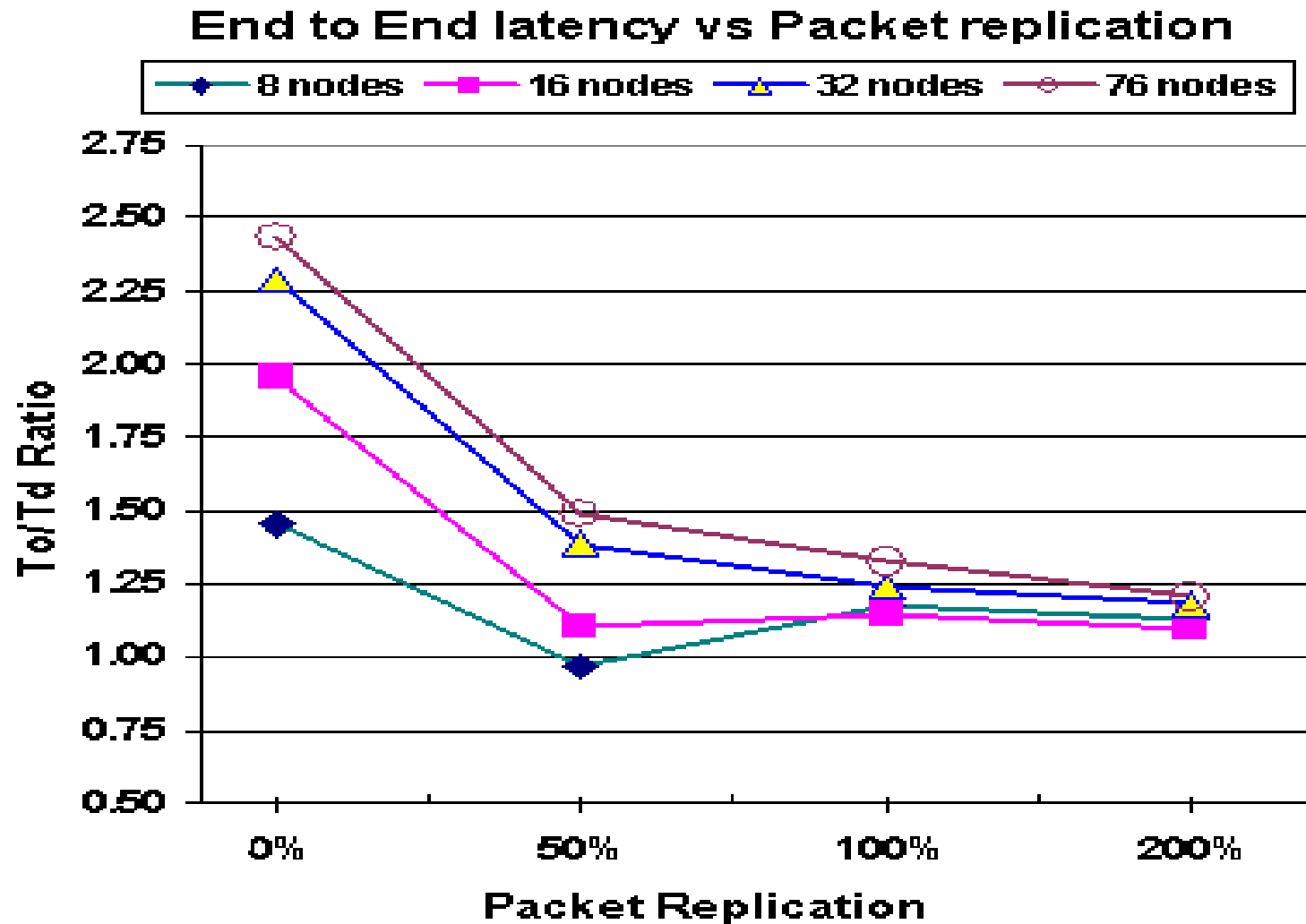
Packet Layout



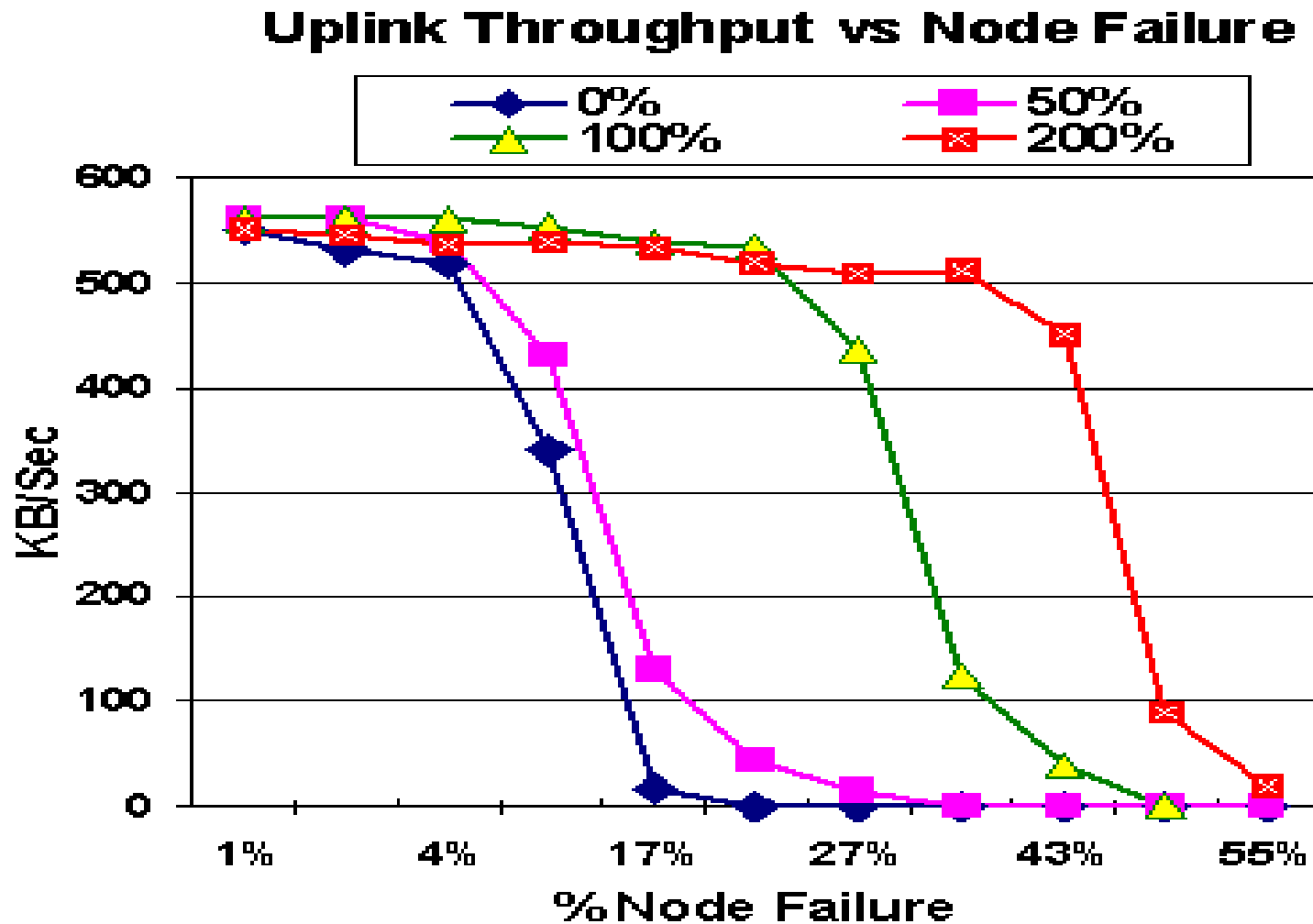
Throughput without DDos



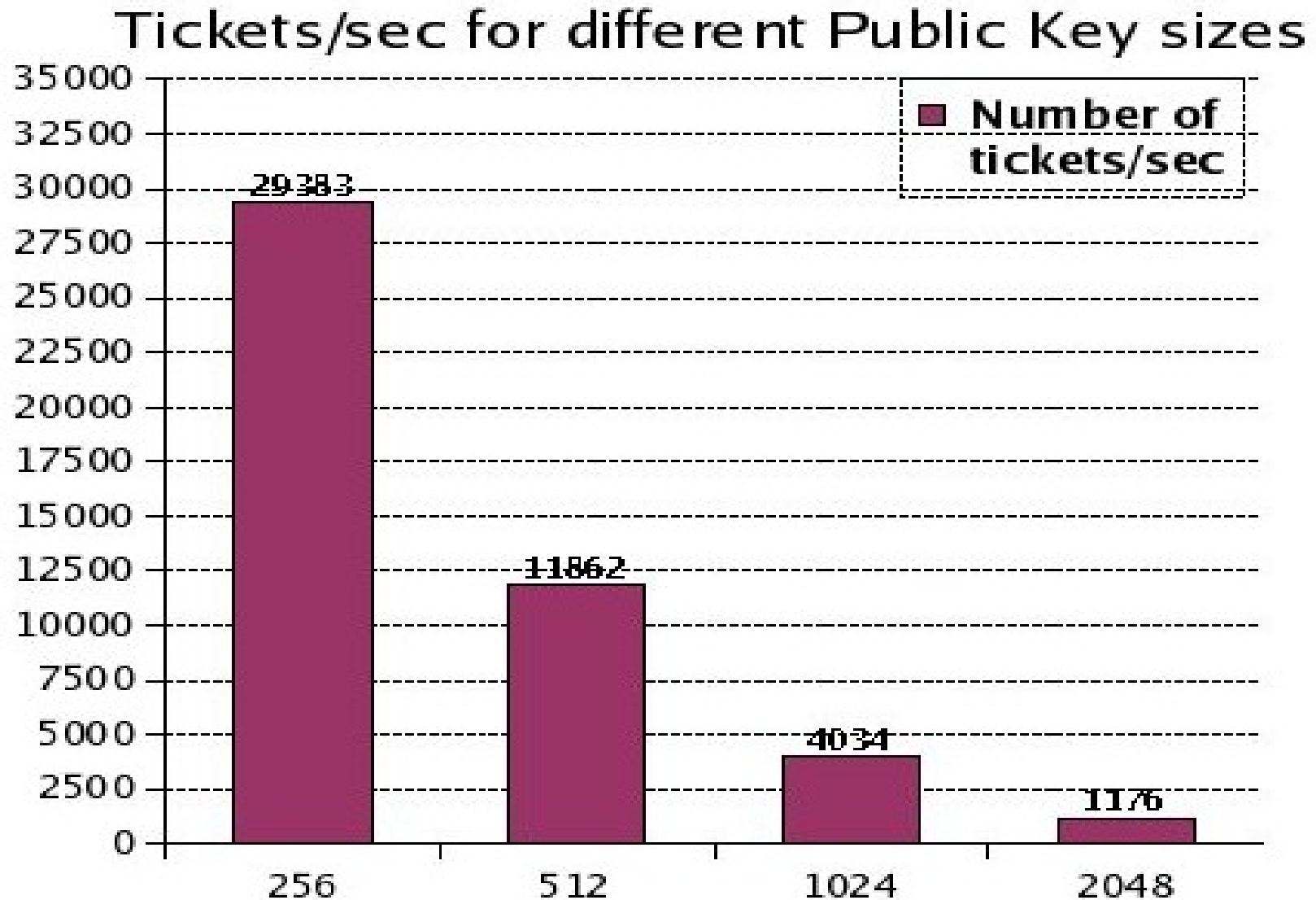
Latency without DDos



Throughput in DDos



Ticket Granting Performance



Questions and Comments 1/2

- Spread spectrum = misleading term?
- Certificate = really a public key?
- What is overlay version?
- Figure 4: extra round-trip could be used by attackers to kill client connectivity?
- Ticket is bound to IP => not mobile
 - Use public key fingerprints and HIP :)
- What is the group management protocol?
 - Usually quite complex...

Questions and Comments 2/2

- UDP encapsulation and fragmentation?
- What is the application identifier?
- Connection request and buffering?
- What is the index used for?
- How does the ticket renewal really work?
- Why do the POP routers drop all non-overlay traffic (consider “transition period”)?
- What is T_o/T_d ratio in figure 6?