

ML-IPsec

A Multi-Layer IPsec Protocol

Bernd Schloer

Advanced Topics in
Computer Networking

SS 2005



Telematics Group

Institute for Informatics

University of Göttingen



Contents

How does IPsec work?

Limitations of IPsec

The Approach of the ML-IPsec Protocol

A Multi-Layer IP Security Protocol TCP Performance
Enhancement in Wireless Networks

Mobile Multi-Layered IPsec



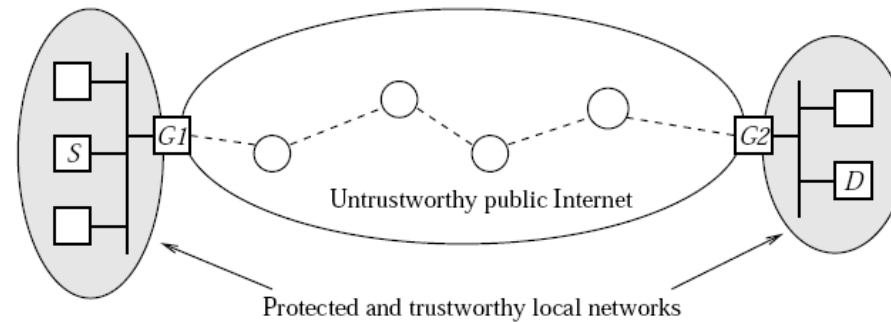
IPsec – What is it?



- standard protocol for secure communication over the Internet
- it protects the entire IP datagram of a packet from end-to-end
- it is used for VPNs and secure remote access
- no intermediate node can access information above the IP layer



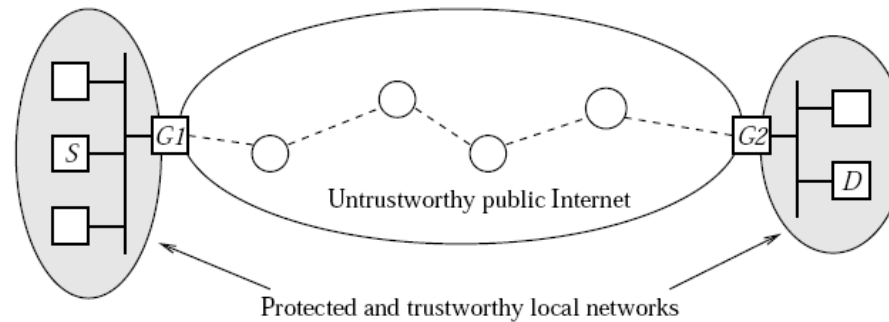
IPsec – how does it work?



- path between source and destination consists of three parts:
 - protected and trusted LAN at the source
 - untrusted public Internet
 - protected and trusted LAN at the destination



IPsec – how does it work?



- G_1 establishes a security association with G_2 using shared secrets
- G_1 encrypts a datagram with an IPsec protocol (e.g.: 3DES, AES256)
- G_2 decrypts the datagram before forwarding it to the destination

Traffic Security

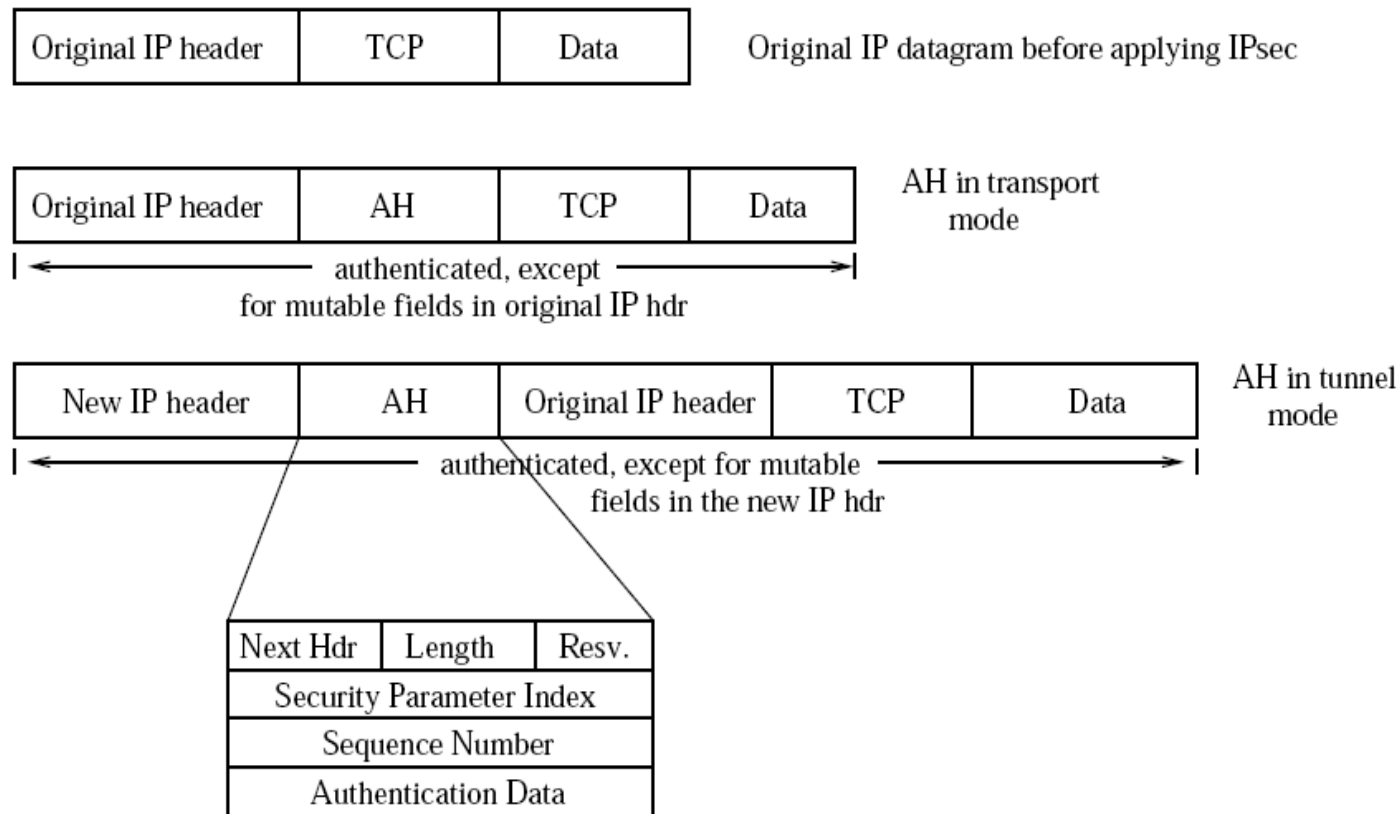
two protocols are used:

- AH – Authentication Header
 - provides integrity and authentication without confidentiality
- ESP – Encapsulation Security Payload
 - provides confidentiality with optional integrity and authentication



The Package Format - AH

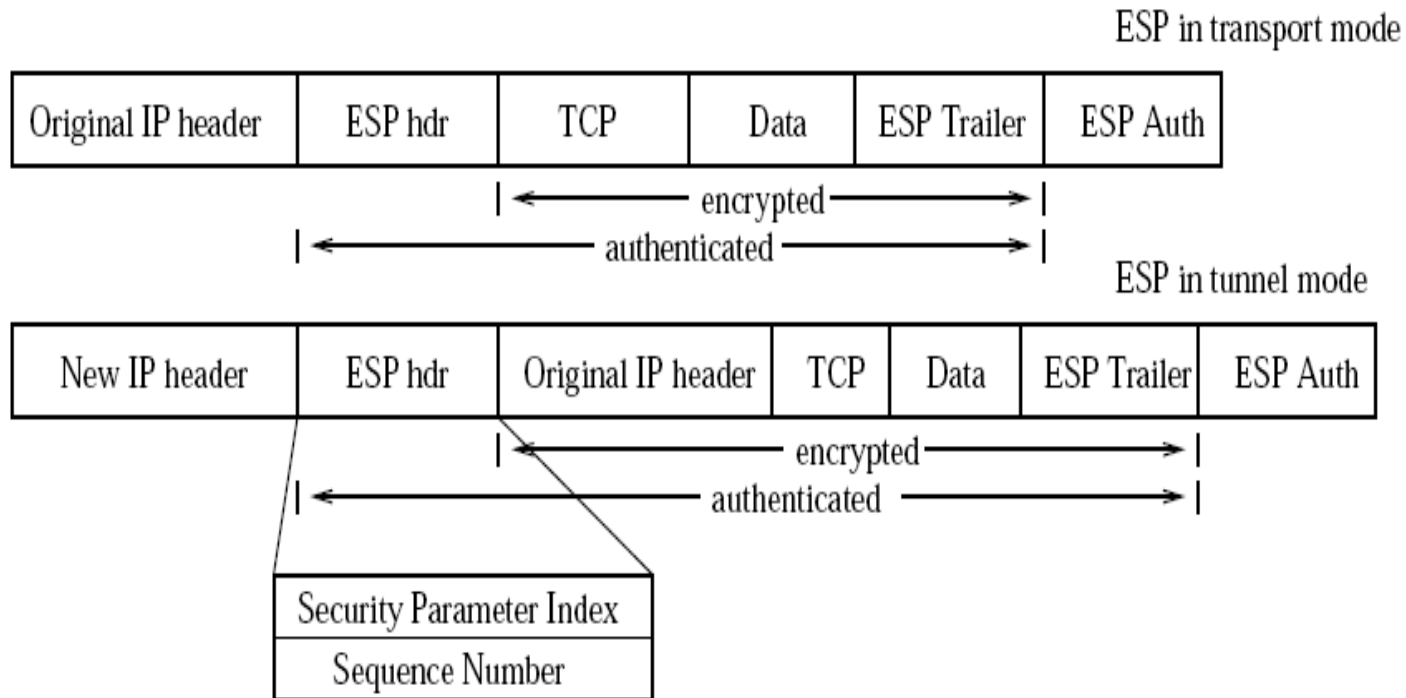
AH = Authentication Header





The Package Format – EPS

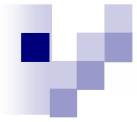
EPS = Encapsulating Security Payload





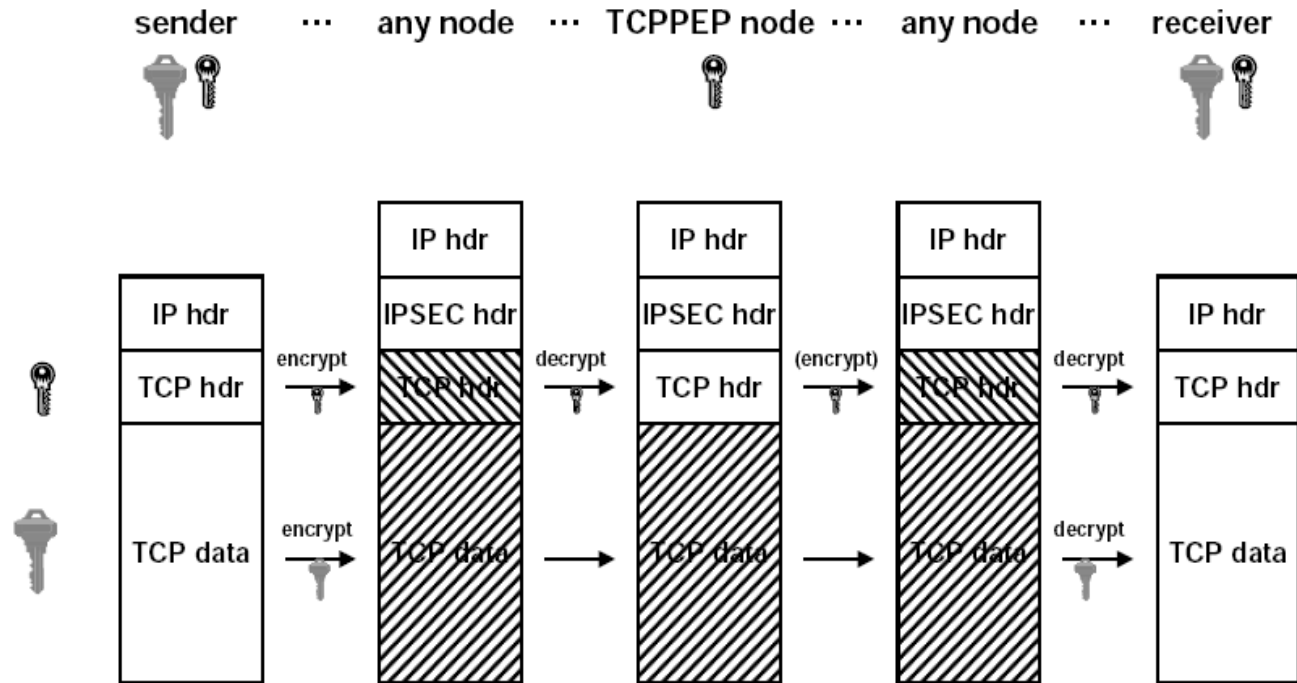
Limitations of IPsec

- Today's routers access not only IP headers but also higher layer information. With IPsec the following is not possible:
 - Internet traffic engineering
 - Transport-aware link layer mechanisms
 - Application-layer proxies/agents
 - Active networks
 - Traffic Analysis



The Approach

- Multi-Layer Security Protection

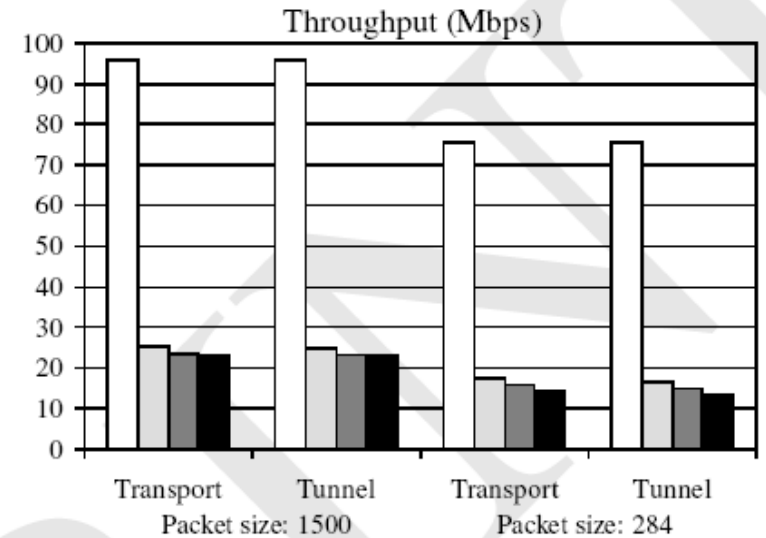
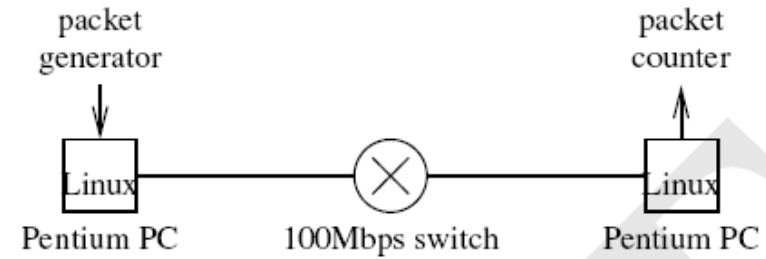
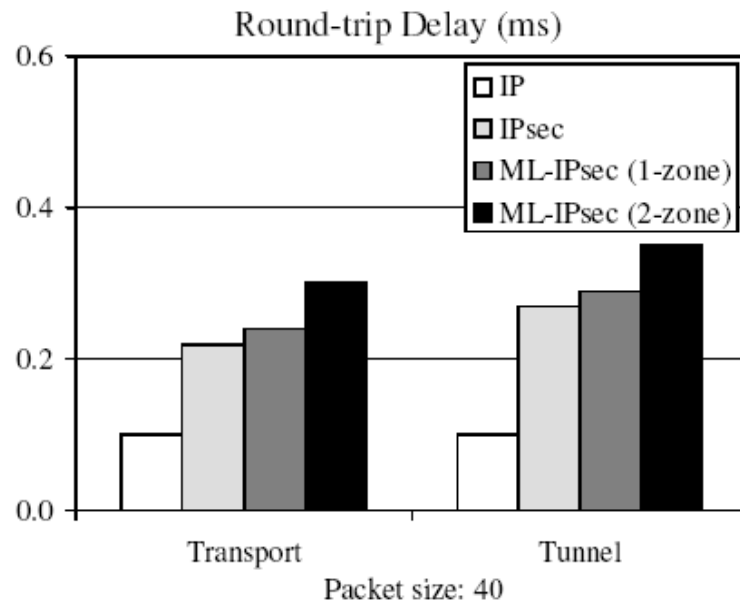


TCP PEP = TCP Performance Enhancement Proxy



Performance

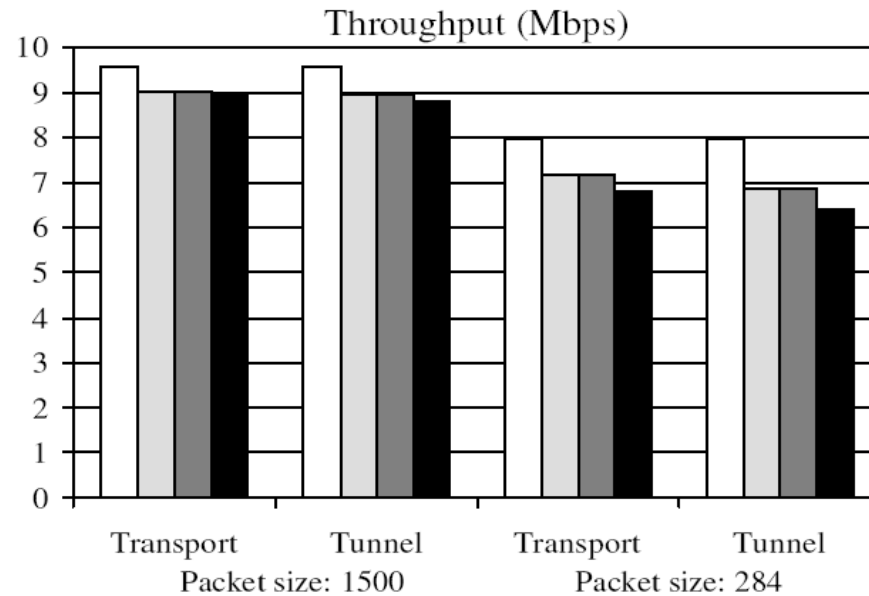
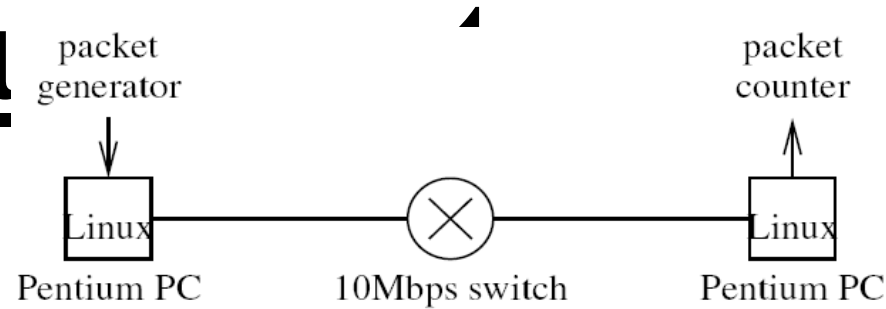
Measurements





Performance

Measur





Protocol TCP Performance

Enhancement in Wireless

- TCP does not perform optimal when operated over wireless networks
- Improvements can be achieved by TCP Performance Enhancement Proxies (TCP PEP)
 - transport-aware link layer mechanisms, like TCP snooping
 - indirect connections
 - explicit notifications, like link failure notifications



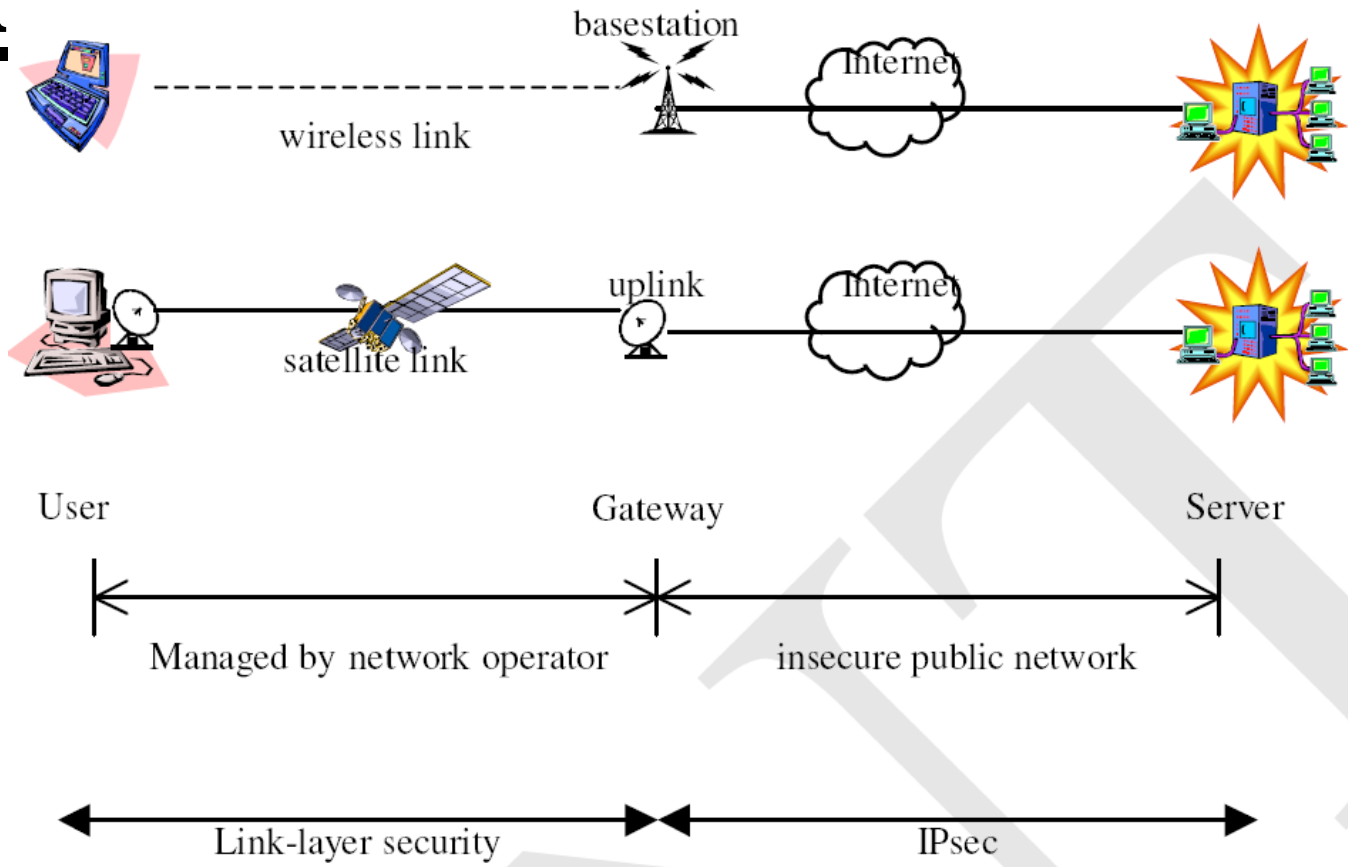
TCP snooping

- the wireless base station inspects TCP packets to detect packet losses
- in case of lost packets the packets are retransmitted and the loss signal is suppressed
- the performance is increased significantly



The Realm of Trust in a

Wireless Network



TCP PEP conflicts with

IPsec

- TCP PEP inspects the TCP header for
 - TCP flow identification
 - sequence number
- IPsec encrypts the TCP header
- ML-IPsec resolves this conflict

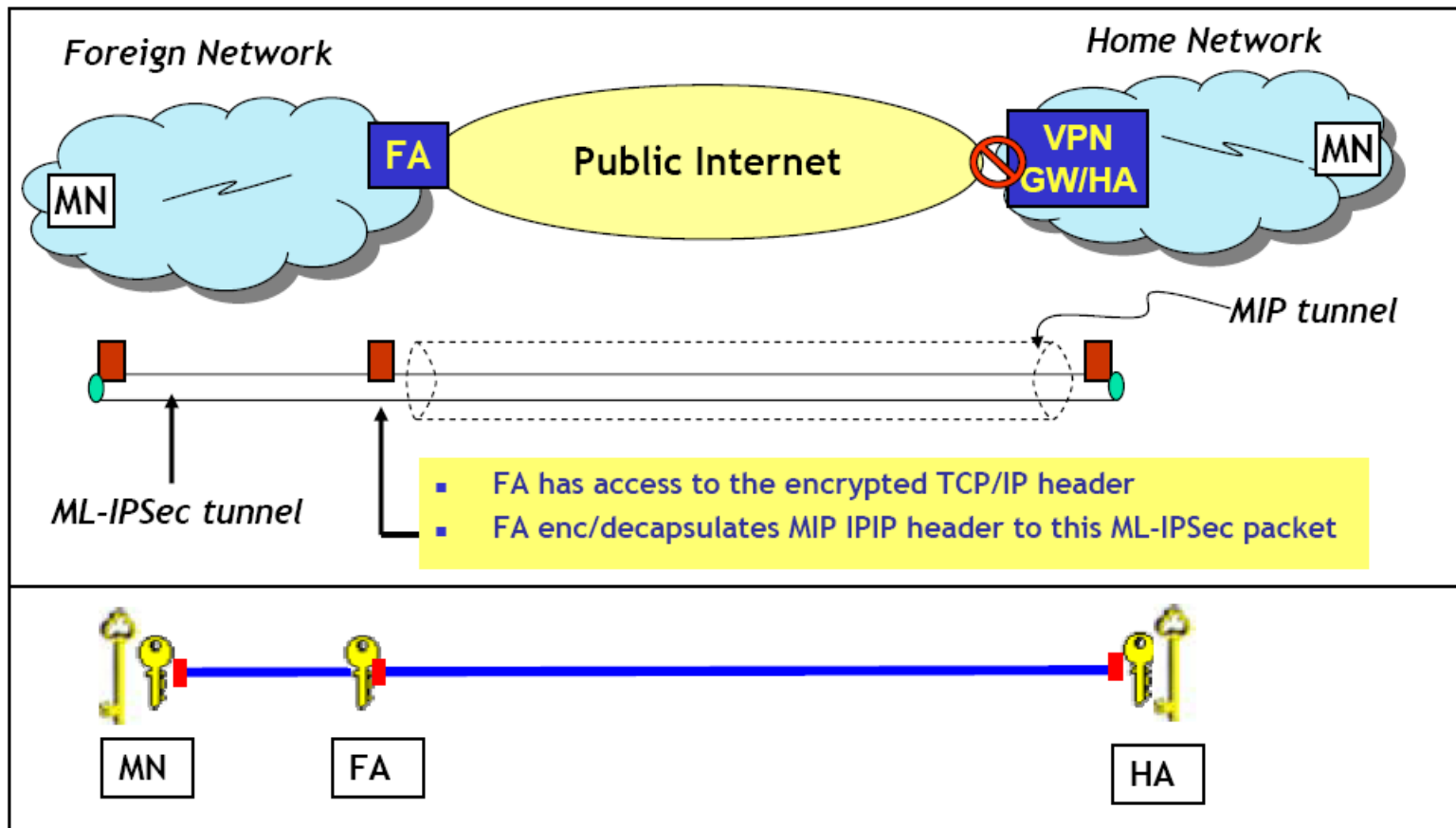
Mobile Multi-Layered

IPsec

- Implementation of ML-IPsec
- effective key exchange protocols added
 - initialization
 - mobility support
- Implementation of Snoop
- Integration of Snoop with MML-IPsec



ML-IPsec over MIP



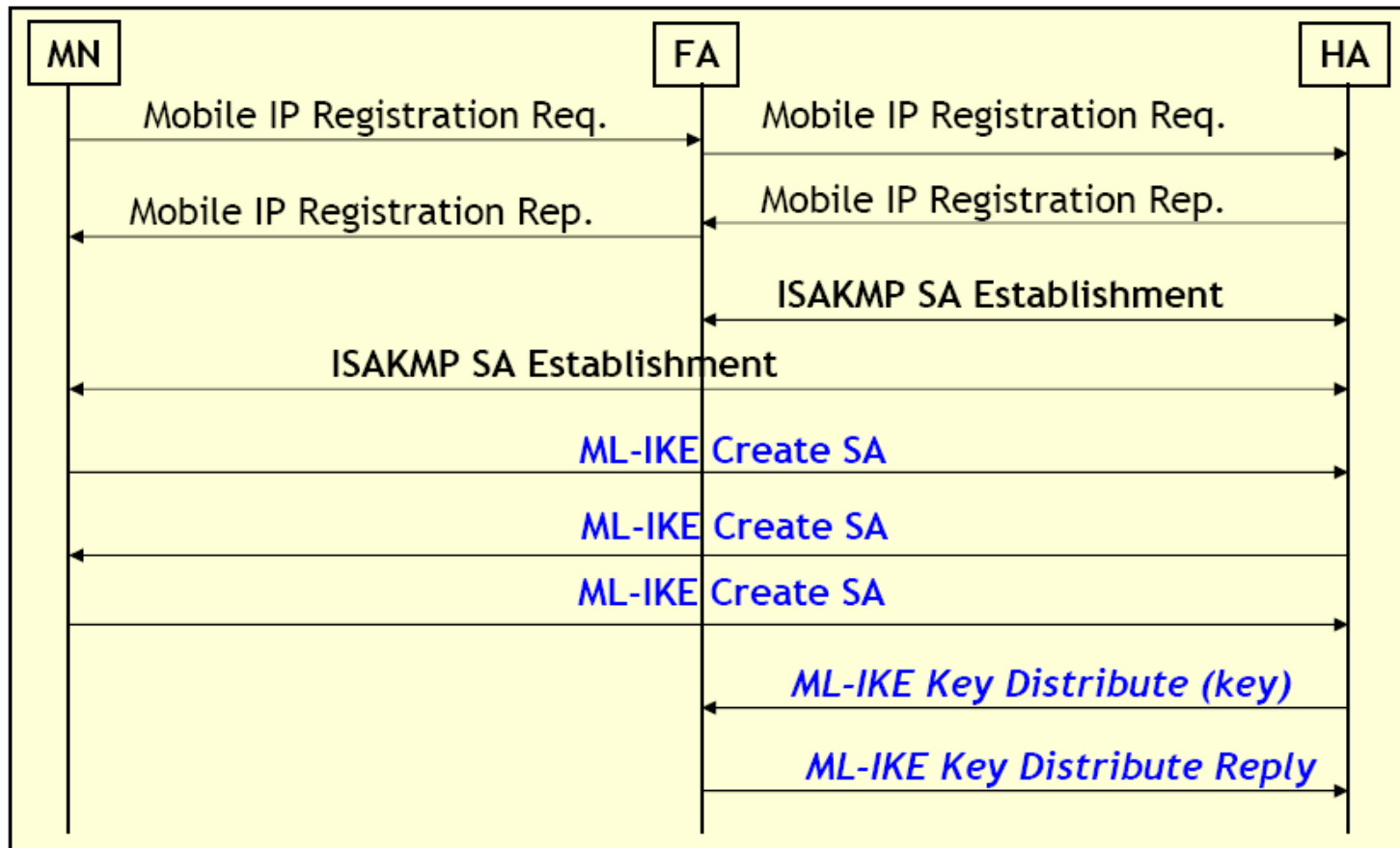


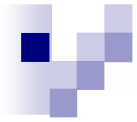
Key Exchange Protocols

- Automatic establishment of Security Association (SA)
- Initialization
- Mobility Support
 - Proactive Key Distribution (PKD)
 - Directed Key Migration (DKM)

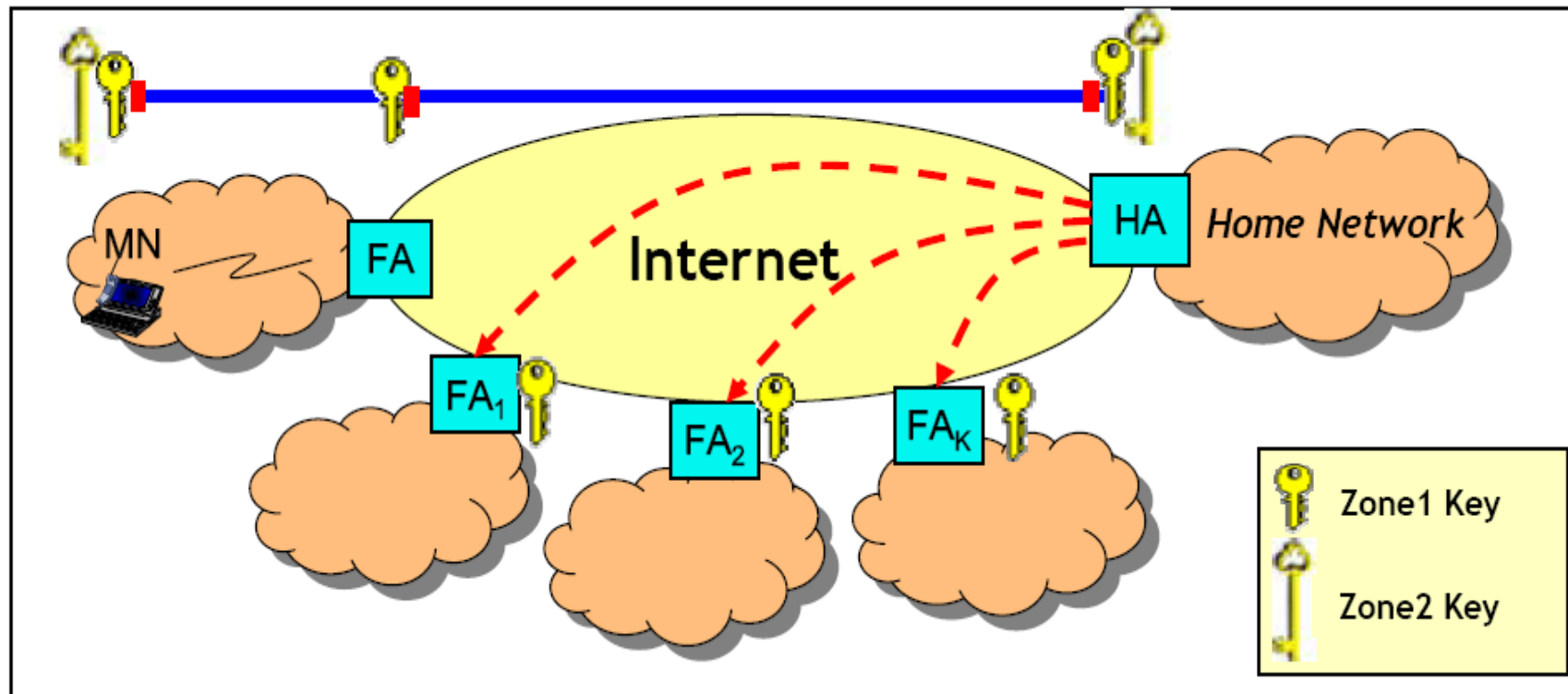


Initialization



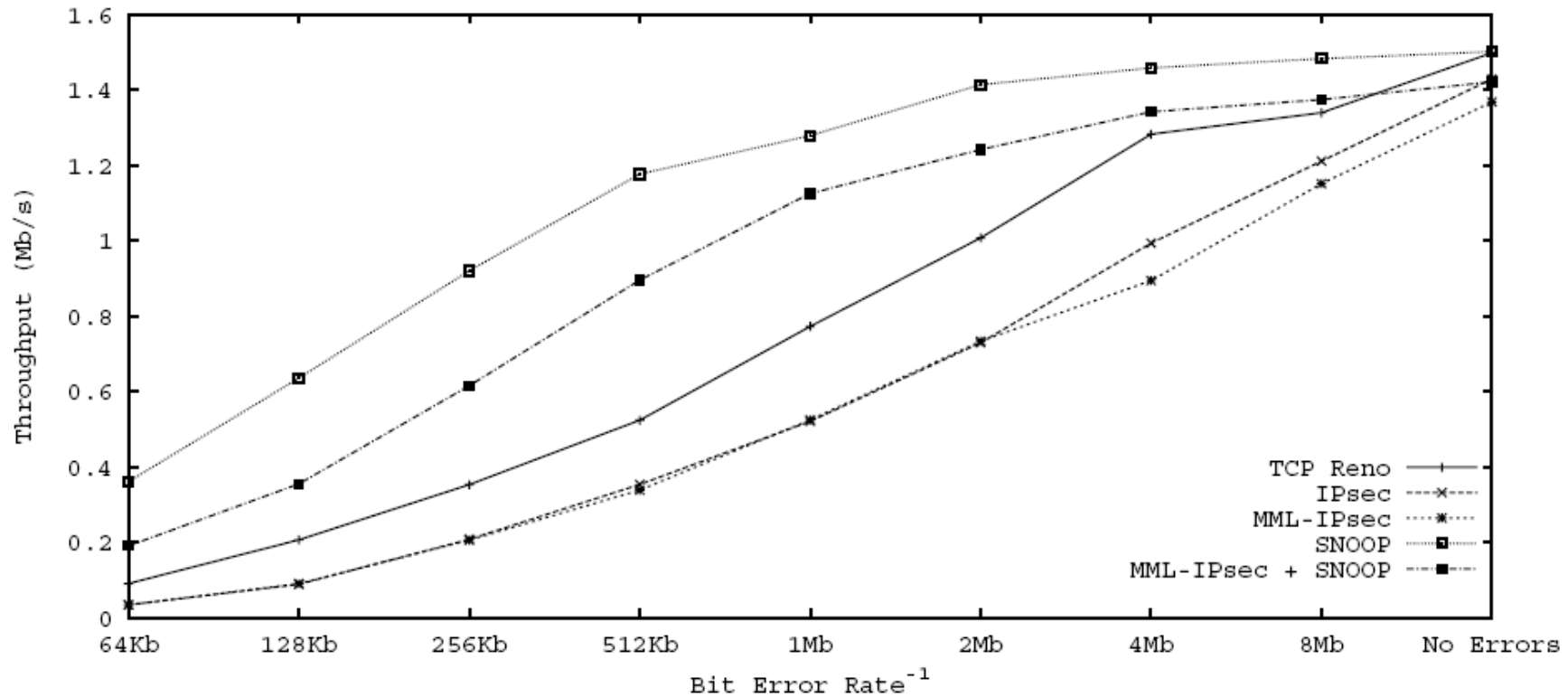


Proactive Key Distribution





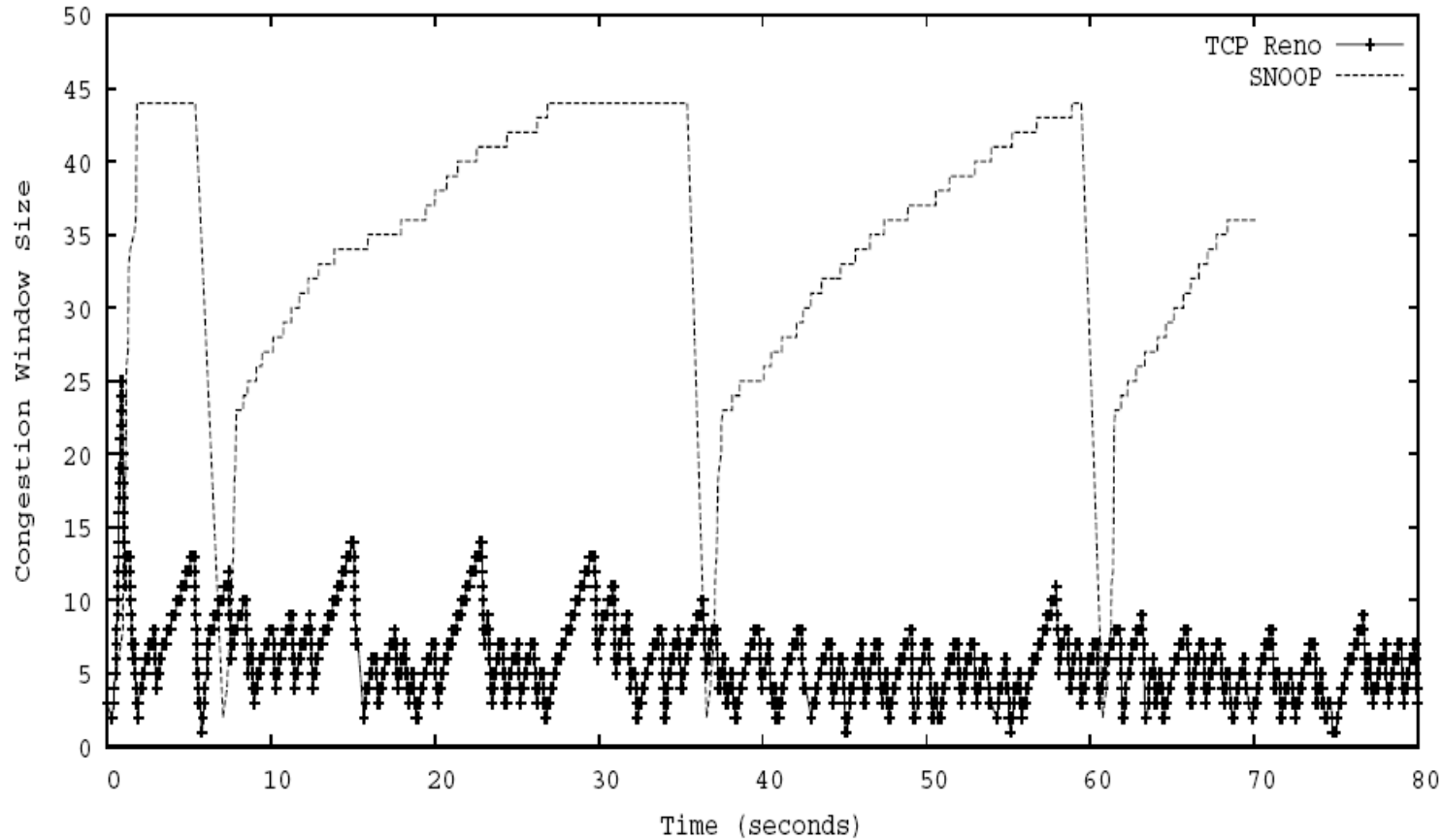
Performance - Throughput





Performance TCP Reno vs.

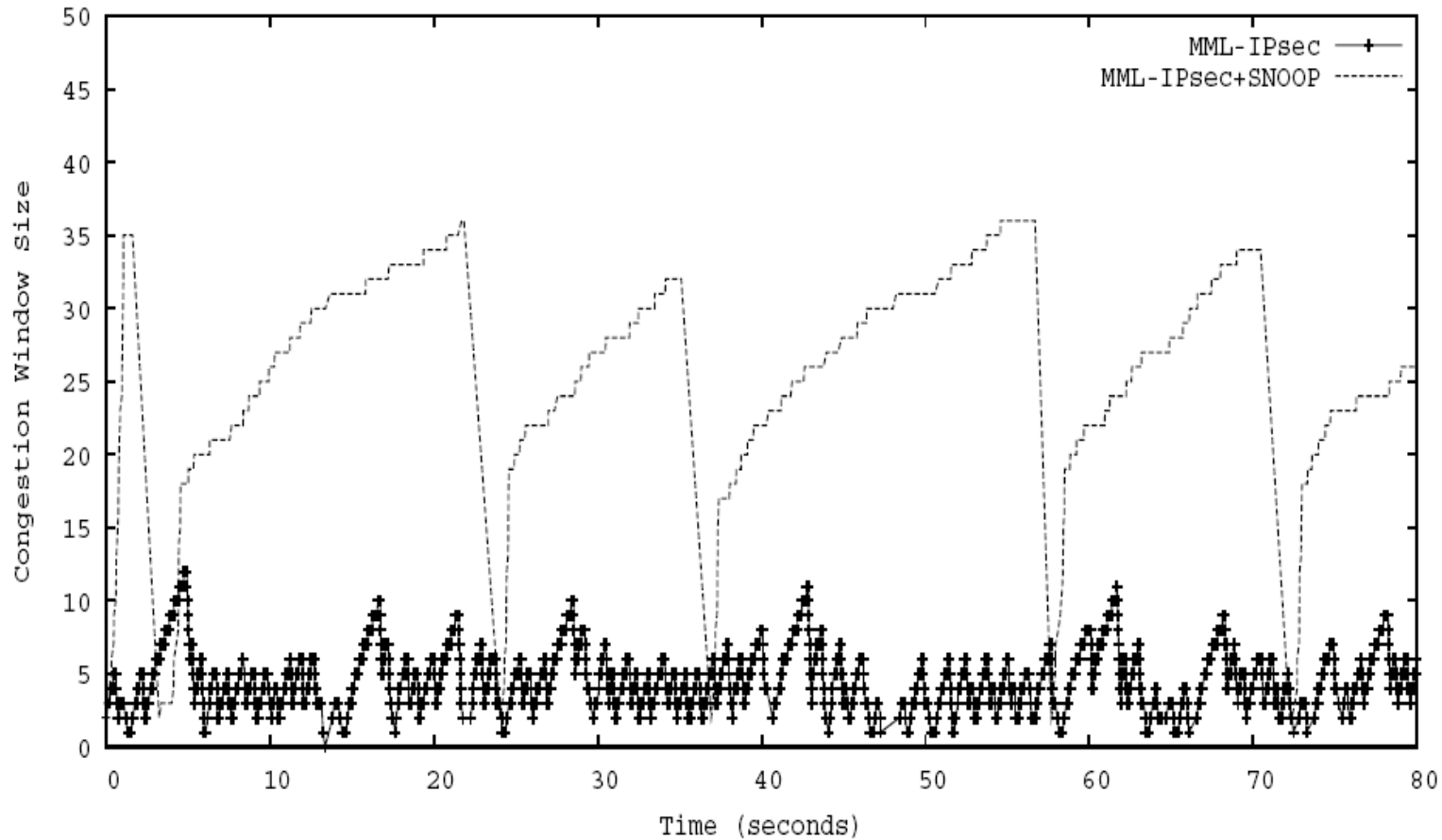
Snoop





Perf. MML-IPsec vs. MML-

IPsec with SNOOP





References

- <http://www.cse.psu.edu/~gcao/paper/song/infocom05.pdf>
- <http://www.cse.psu.edu/~gcao/teach/514/jsac04.pdf>
- http://www.usenix.org/events/sec2000/full_papers/zhangipsec/zhangipsec.pdf
- <http://islab.cis.thu.edu.tw/files/document/13.ppt>
- <http://nsrc.cse.psu.edu/posters/heesook.pdf>





