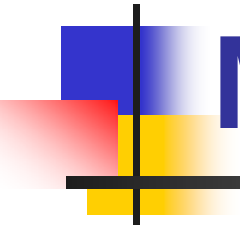


Mobile Multi-Layered IPSec

Advisors: Prof. Tom La Porta and Prof. Guohong Cao

Heesook Choi & Hui Song
CSE Department

PENNSTATE

Motivations - Performance

- Performance Degradation in wireless networks
  - High loss rate
  - Delay
  - Handoff
- Performance Improvements in the intermediate nodes
  - SNOOP, I-TCP, Ack Regulator
  - Micro-mobility

Motivations - Security

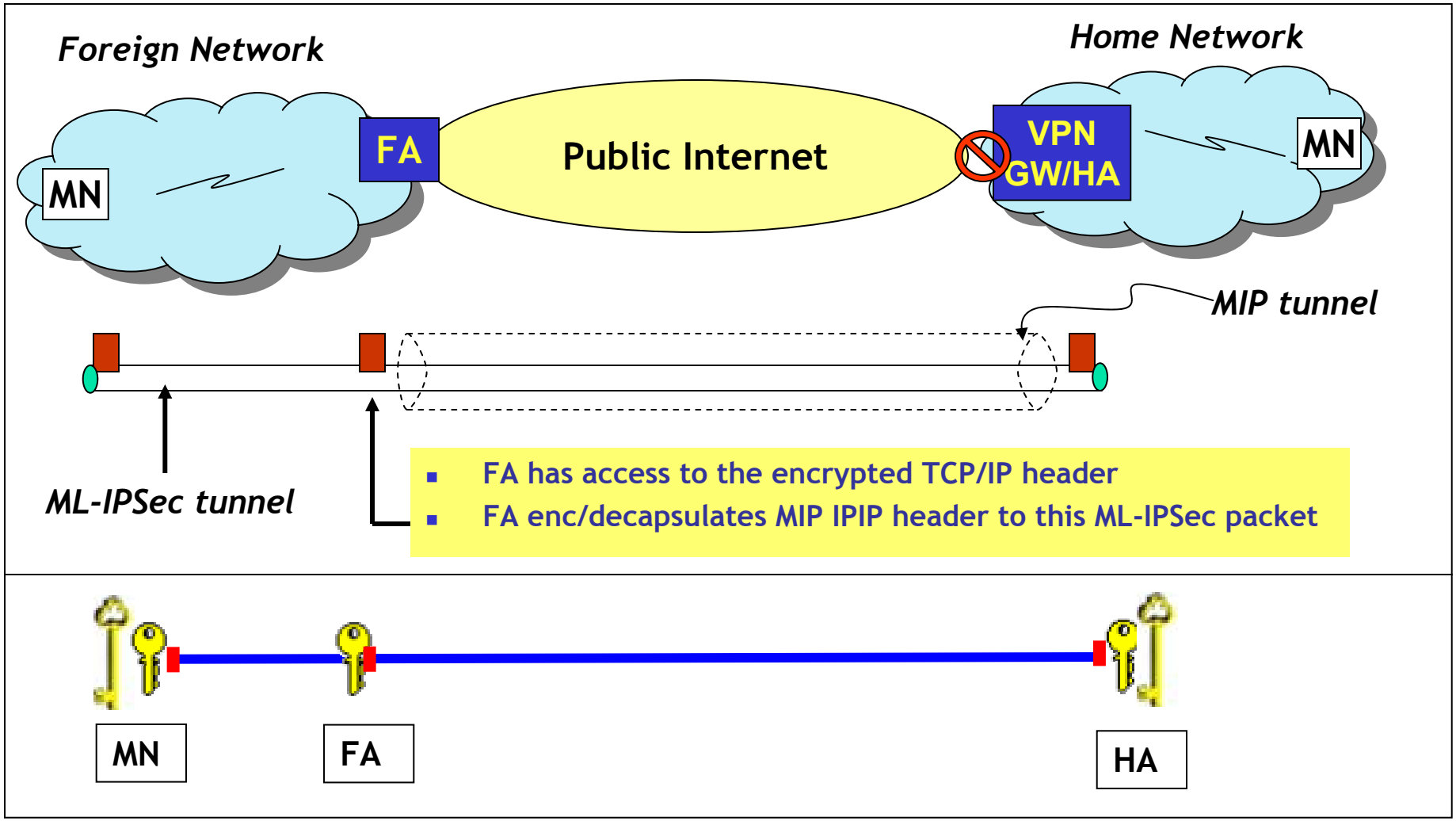
- High vulnerability in Wireless Networks
- End-to-end security (IPSec)
  - Prevents performance enhancements in the intermediate nodes
- Multi-layered IPSec (ML-IPSec)
  - Allows the intermediate nodes to do performance enhancements
  - Manual keying: not scalable
  - Not available

Contributions

- Mobile ML-IPSec (MML-IPSec)
  - Propose effective key exchange protocols
    - Initialization
    - Mobility Support
  - Implement ML-IPSec
- Implement SNOOP
- Integrate SNOOP with MML-IPSec

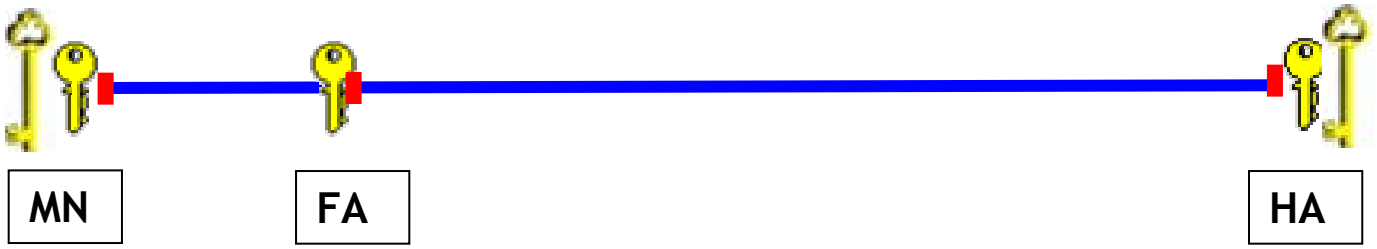
Secure & High Performance Communication in Wireless Networks !

Integration Model (ML-IPSec over MIP)



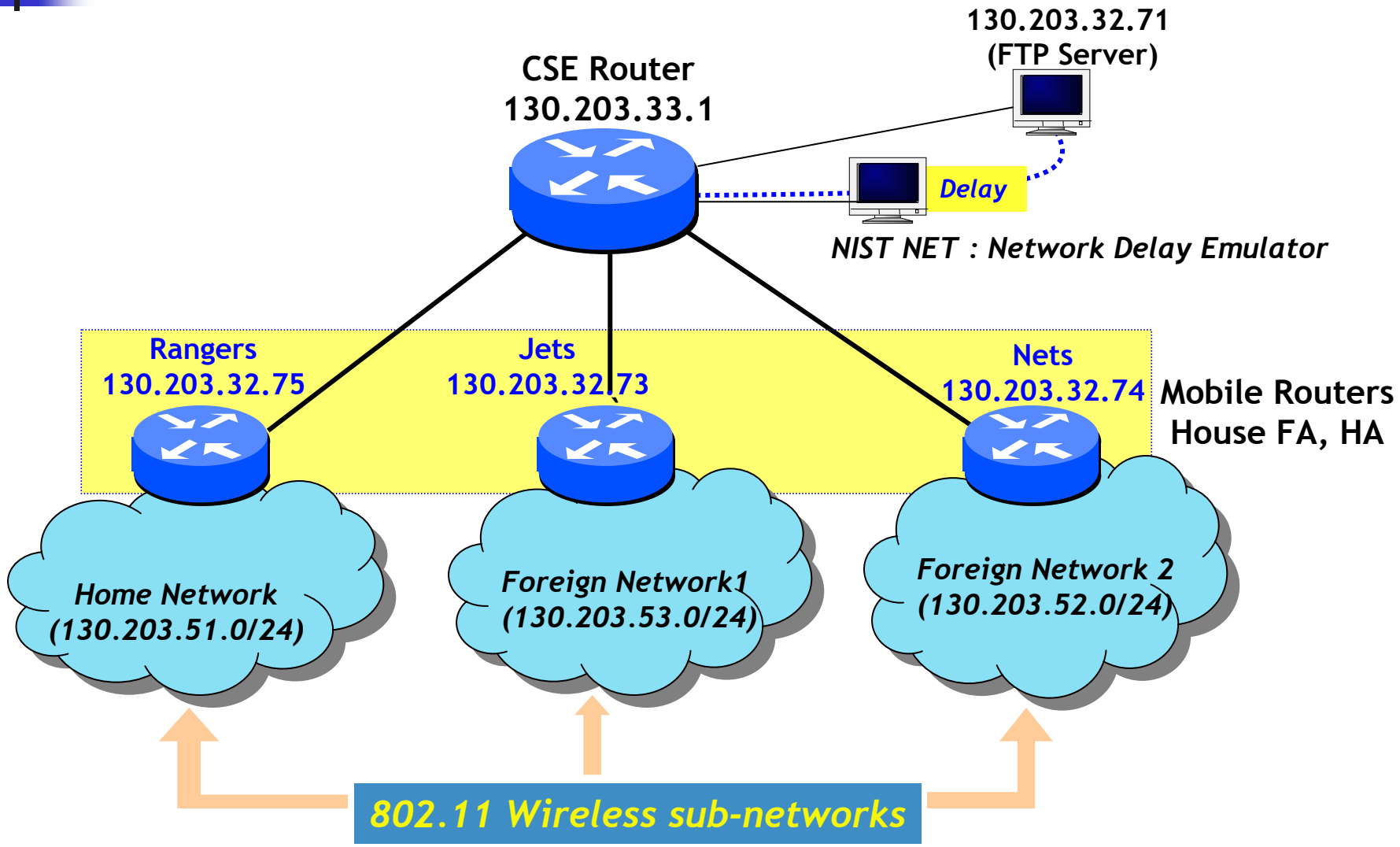
Mobile Multilayer IPSec (MML-IPSec)

- Two zones
  - Zone1: TCP/IP header
  - Zone2: Application data
- One intermediate node (FA) has access to the TCP/IP header (Zone 1)
  - FA needs a security association



Mobile ML-IPsec (MML-IPsec)

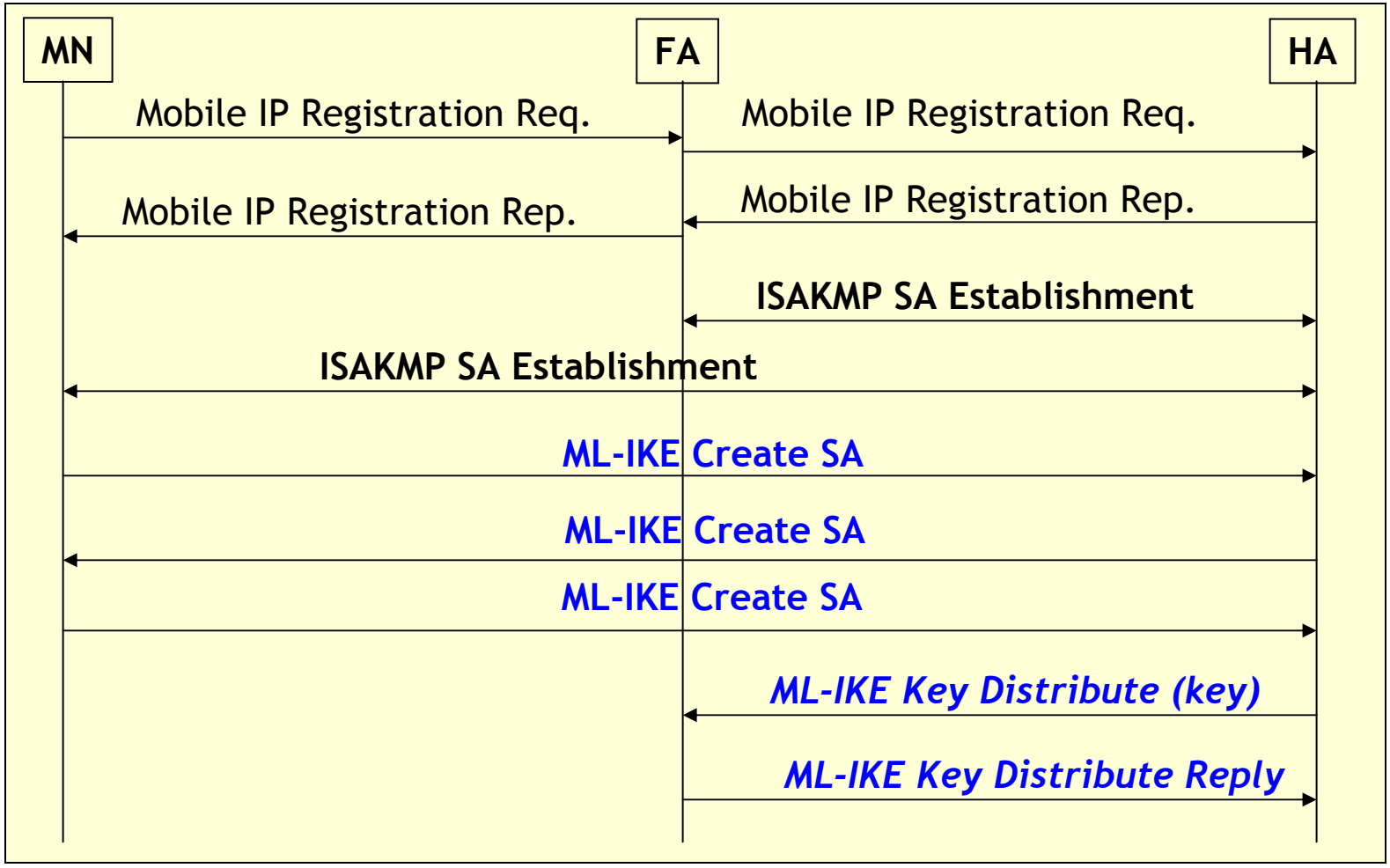
Test Bed


130.203.32.71
(FTP Server)
CSE Router
130.203.33.1
Delay
NIST NET : Network Delay Emulator
Rangers
130.203.32.75
Jets
130.203.32.73
Nets
130.203.32.74
Mobile Routers
House FA, HA
Home Network
(130.203.51.0/24)
Foreign Network1
(130.203.53.0/24)
Foreign Network 2
(130.203.52.0/24)
802.11 Wireless sub-networks

Key Exchange Protocols

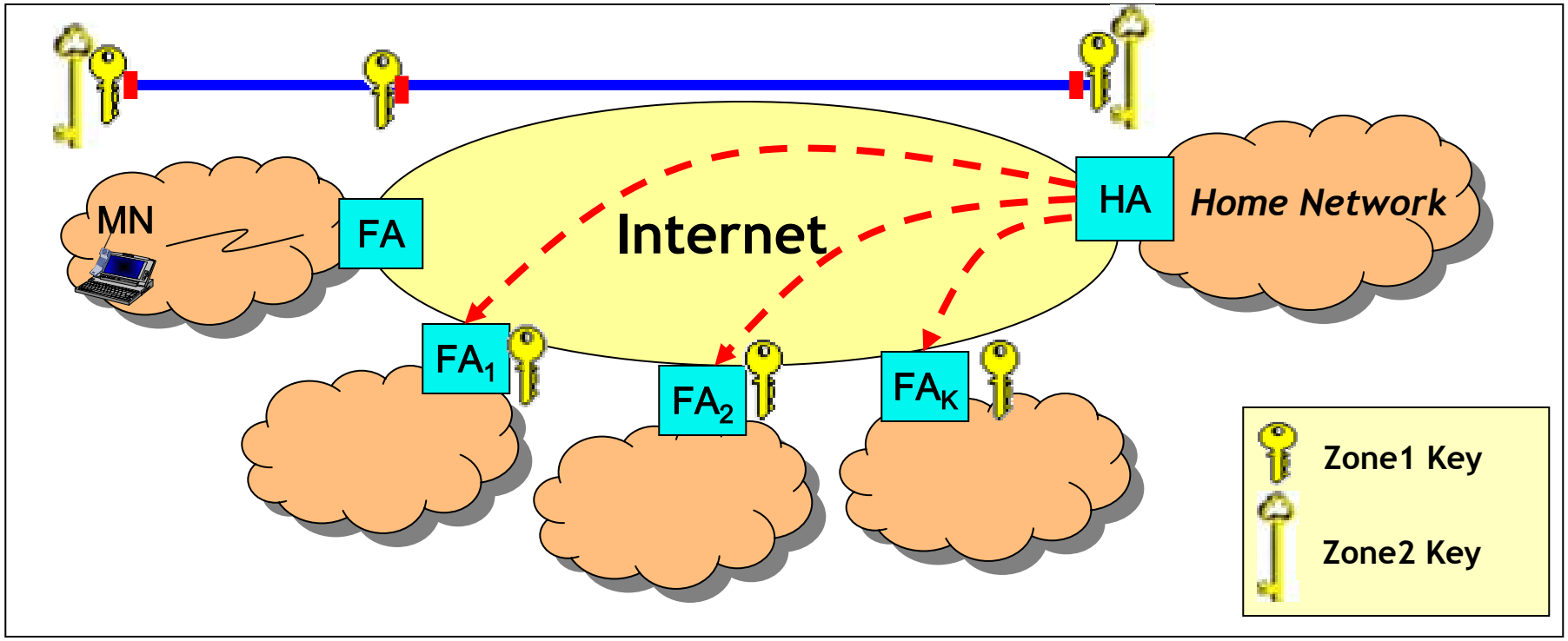
- Automatic establishment of Security Association
- Initialization
- Mobility Support
  - Proactive Key Distribution (PKD)
    - HA distributes key values to neighbor FAs
  - Directed Key Migration (DKM)
    - New FA retrieves key values from the previous FA

Initialization



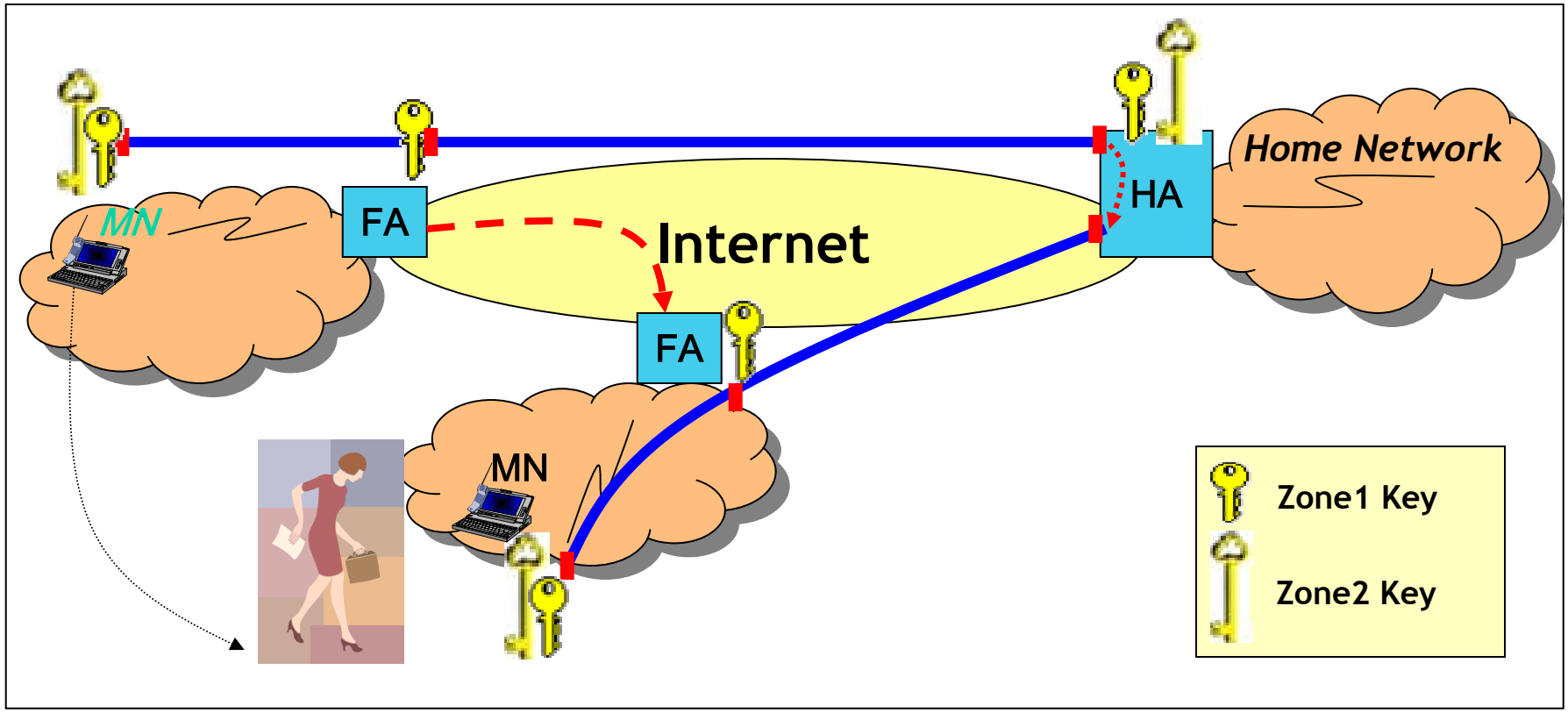
Proactive Key Distribution

HA distributes key values to neighbor FAs



Directed Key Migration

New FA retrieves Key Values from the previous FA



Key Exchange Protocols Overheads

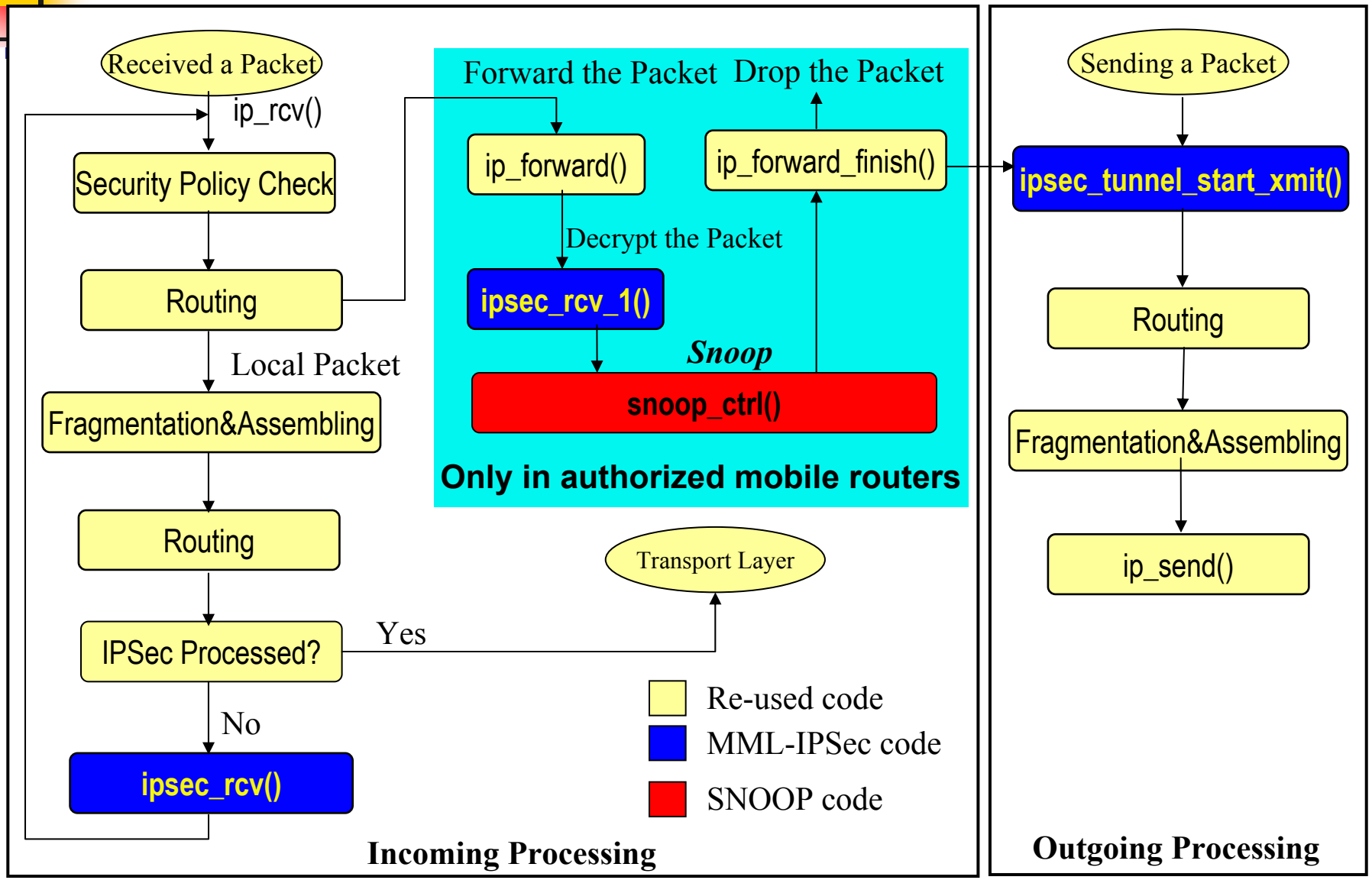
Message Processing Time

Protocols	Processing Time		
	Initiator	Responder	Total
ISAKMP SA	50.0 ms	42.0 ms	92.0 ms
ML-IKE Create SA	45.3 ms	35.7 ms	81.0 ms
ML-IKE Key Distribution	3.3 ms	0.2 ms	3.5 ms
PKD Key Distribution	2.8 ms	0.2 ms	3.0 ms
DKM Key Distribution	9.0 ms	1.2 ms	10.2 ms
Neighbor Notification	0.6 ms	8.3 ms	8.9 ms

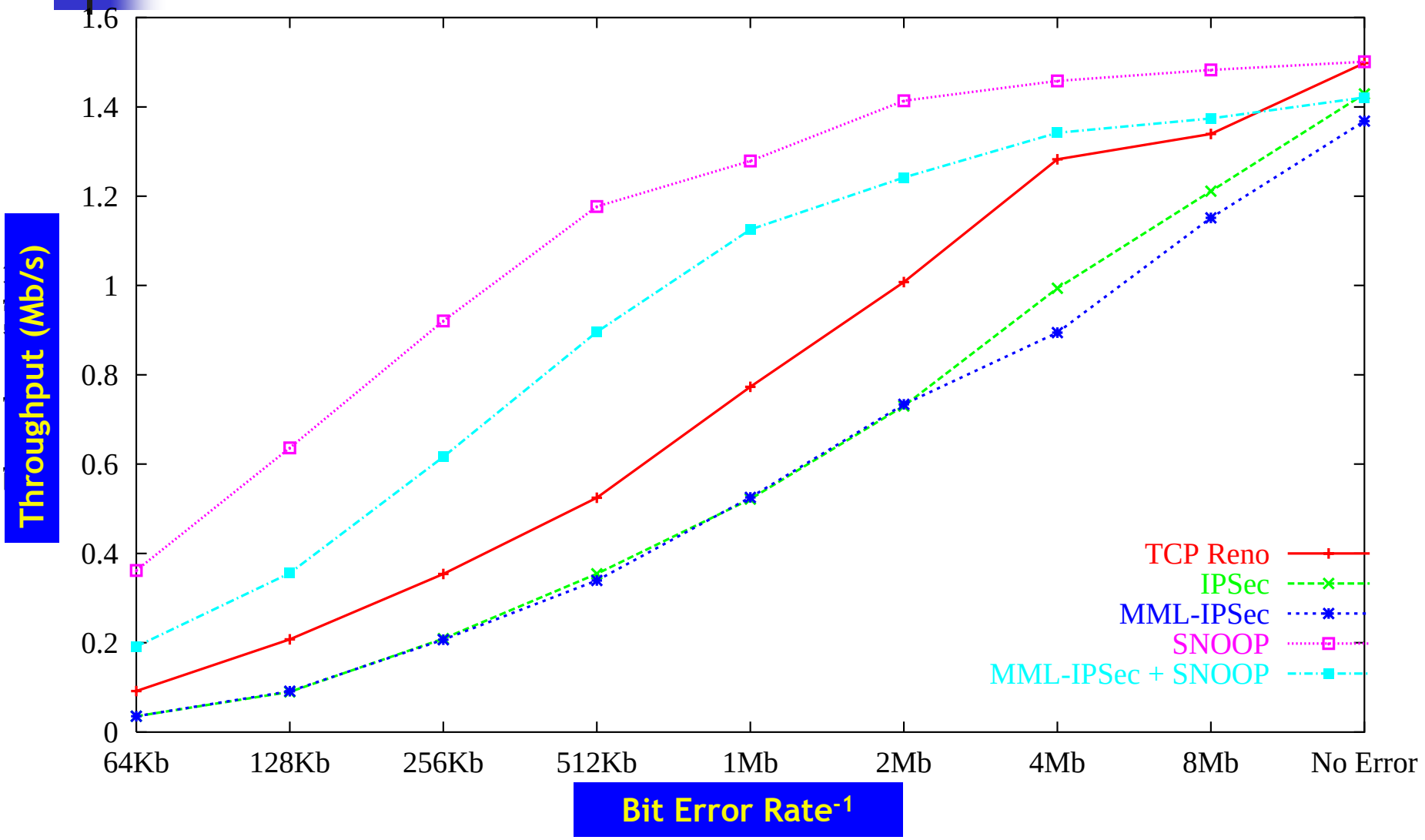
Handoff Delay

Phase	Pure Mobile IP	Mobile IP with IPSec	MML-IPSec	
			PKD	DKM
Initialization	26 ms	375 ms	650 ms	665 ms
Handoff	25 ms	54 ms	56 ms	105 ms

MML-IPSec Transport



Throughput of Different Configurations



Congestion Window Size with/without SNOOP