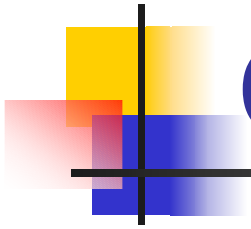
the 58th IETF

Threat Analysis for NEMO

draft-jung-nemo-threat-analysis-01

November 12, 2003

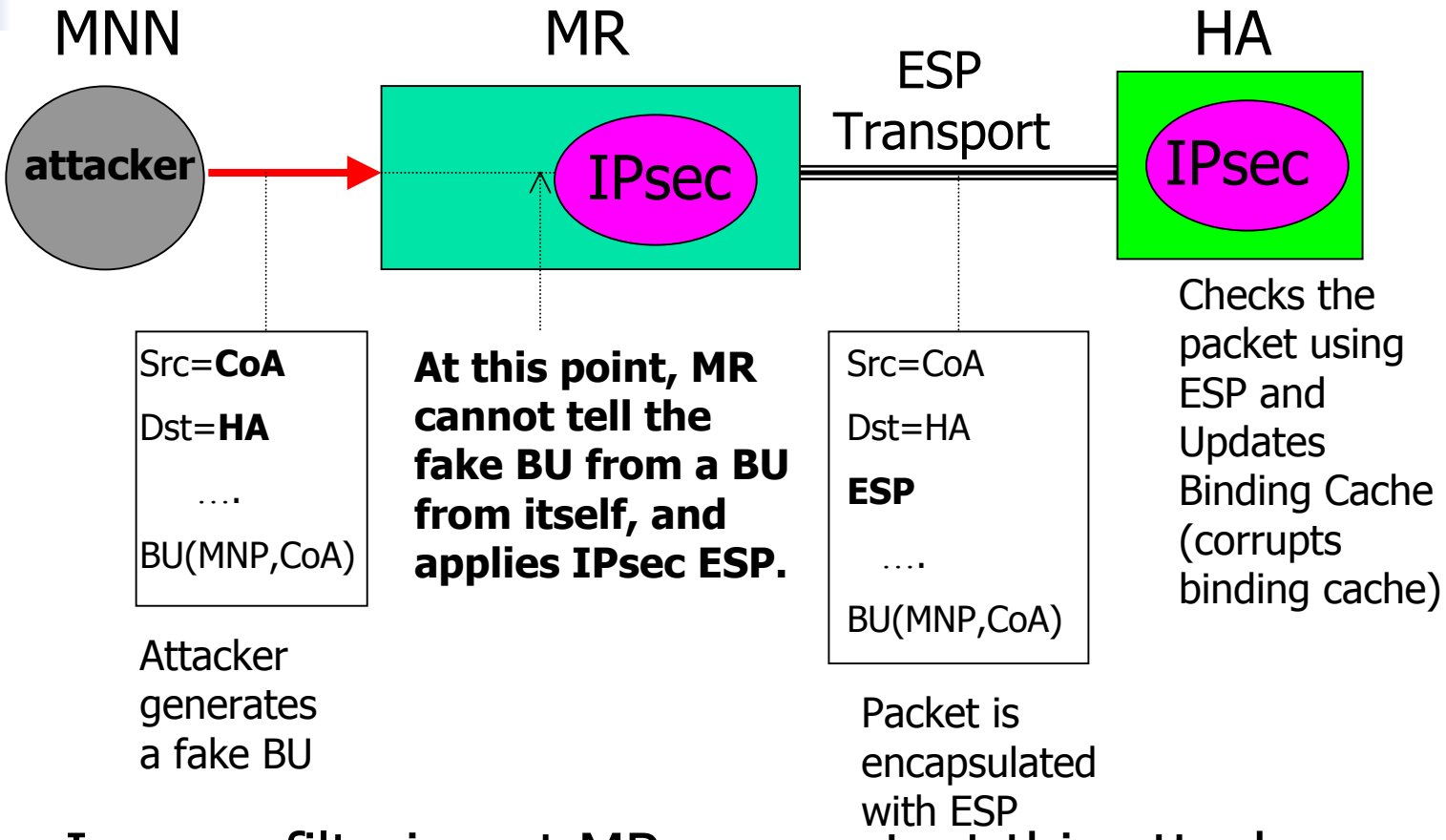
Souhwan Jung, Soongsil University, Korea
Fan Zhao, S. Felix Wu, UC Davis, USA
HyunGon Kim, SungWon Sohn, ETRI, Korea
souhwanj@ssu.ac.kr



Outline

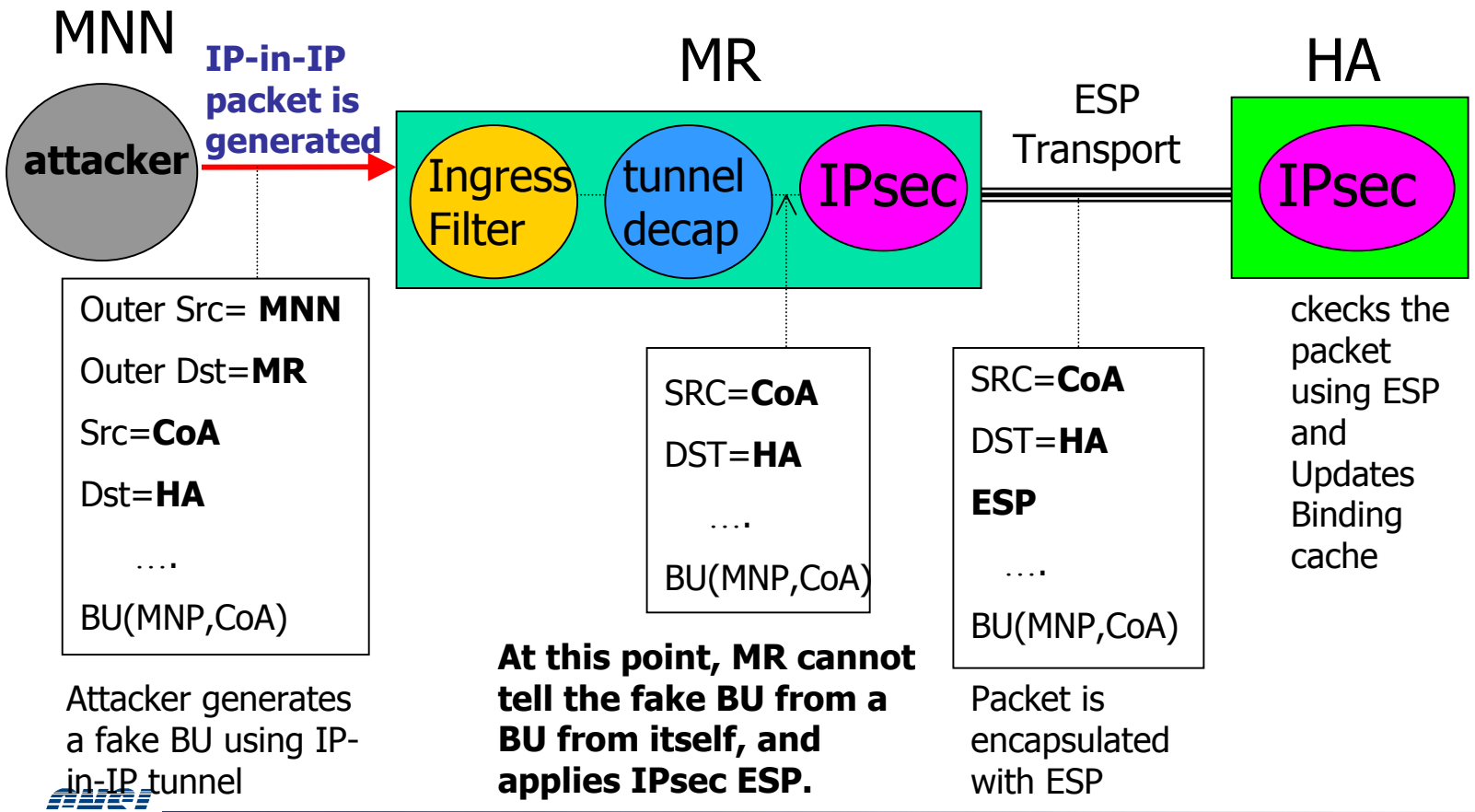
- Threats specific to NEMO basic protocol (MR-HA tunneling)
  1. MNN spoofs BU of MR
  2. Attack using HA as a stepping stone
- Next steps

1. MNN spoofs BU of MR: without ingress filtering at MR



- Ingress filtering at MR can protect this attack.

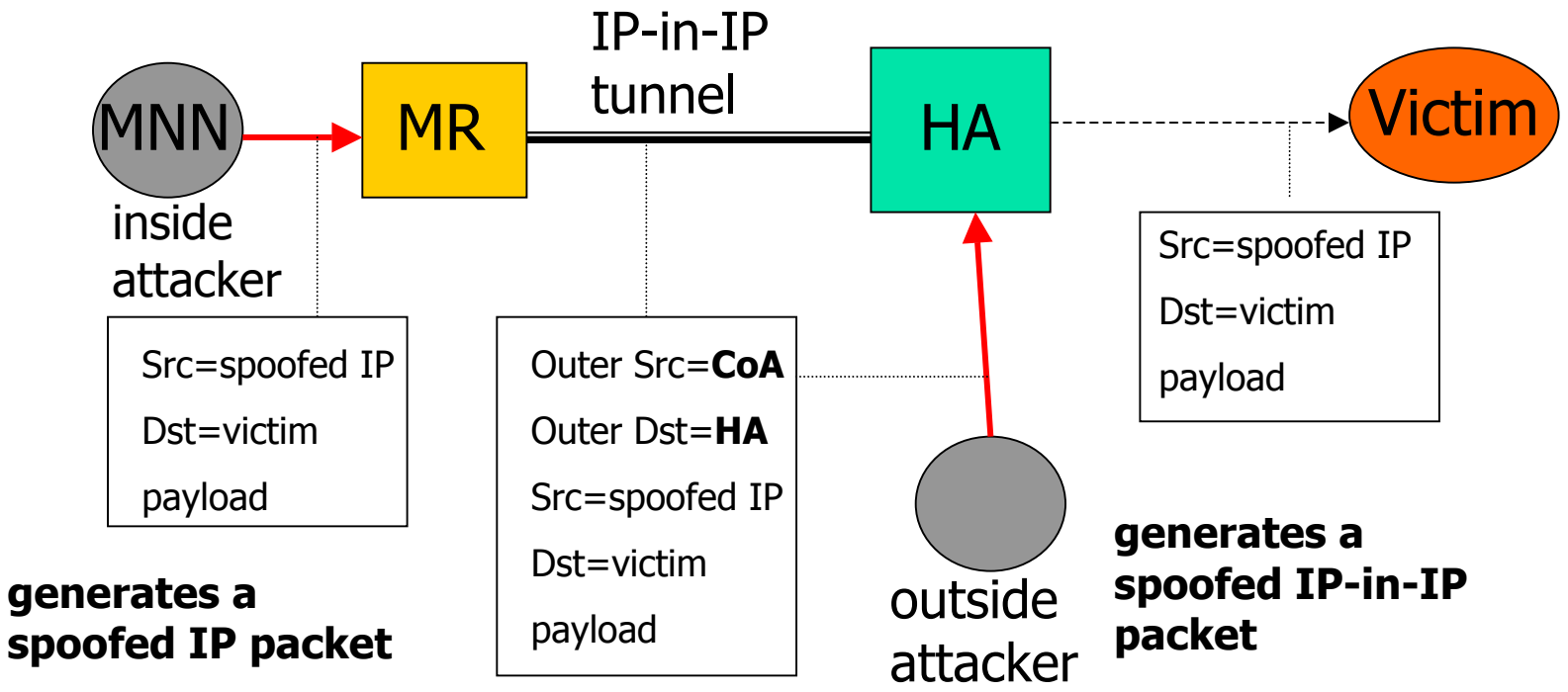
MNN spoofs BU of MR (2): with ingress filtering at MR



Protection against the threat

- This threat does not exist in Mobile IP.
- We checked with two major vendor products that are exposed to this threat.
- The problem is that the default mode of many routers does not turn on ingress filtering before people activate it.
- Implementors of MR should be informed of this potential threat. (implementation issue)
- It is recommended for MR to distinguish L2(from MNN) packet stream from L4 stream (from itself).
- possible solutions
  - MR checks ingress filtering after decapsulating tunneled packet. (not 100% safe, though due to the NAT complication)
  - Use separate buffers to distinguish L2 from L4 stream

2. Attack using HA as a stepping stone



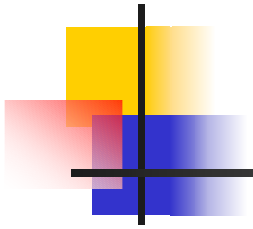
Potential threats are IP spoofing and DoS attack.

Protection against the threat

- IP-in-IP tunneled packet can cause problems.
- In MIP, IPsec tunnel mode can be used to secure IP-in-IP packet between MN and HA.
- The problem in NEMO is that IPsec may be too heavy to MR for this purpose.

Next steps

- Rework on my draft towards
  - Remove many general threat stuff
  - Be more specific to NEMO base protocol
  - Include more realistic threats related to
    - bi-directional tunneling
    - nested MR
    - multi-homing
  - will appreciate more comments and discussion on these items in ML.



Thanks!