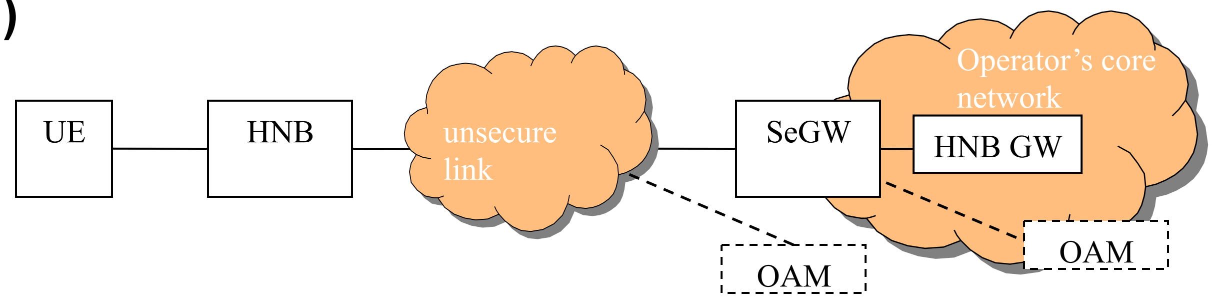
5/10/11

IPsec Synchronization Requirements

IPsec in Mobile Backhaul

- **Mobile Backhaul normally is a closed network but exceptions exist (e.g. femtocell);**
- **In case of a closed network only insiders, i.e., people who have direct access to the Mobile Backhaul network can initiate attacks.**
- **IPsec is being considered in some mobile applications, especially in case of « unsecure links » being involved (e.g. femtocells, see 3GPP TS 33.320)**



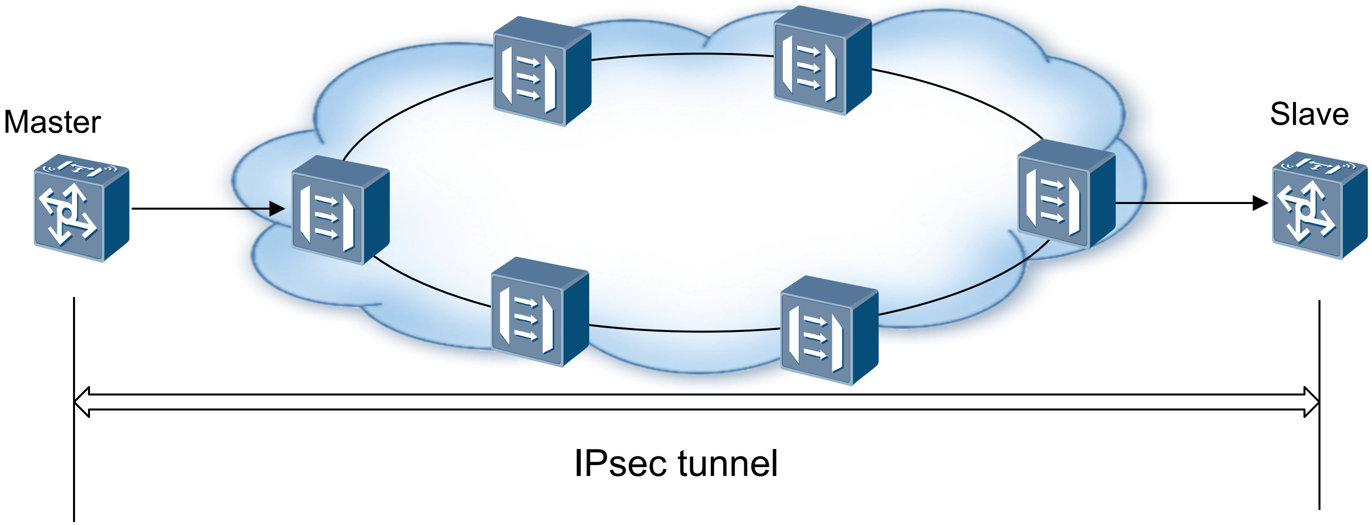
- **IPsec can provide: authentication, confidentiality, integrity**

IPsec for synchronization

- **Tictoc has discussed the advantageous to identify the content of a IPsec tunnel as “special” packets from a timing perspective, the conclusion is:**
  - This may allow a specific handling of the packet both for **intermediate nodes** and slave
  - The problem is how to identify the timing packet when the content of the timing packet is encrypted

IPsec for E2E synchronization

- **In end to end synchronization, the intermediate node does not have to support time protocol, could the intermediate nodes know the identifier for timing packet or not?**



Discussion

- **The intermediate nodes should know the identifier:**
  - The identifier should be designed as fixed value
- **The intermediate nodes should not know the identifier:**
  - The identifier should be private value negotiated between master and slave

Proposal

- **Proposal 1:**
  - The slave and intermediate nodes identify the time packet with explicit identifier in WESP header which are integrity protected
- **Proposal 2:**
  - The master and slave identify the time packet with the pre-negotiated privatization identifier.

Thank you