UNIVERSITÄT KLAGENFURT

Multipath Use Case and Requirement for Security

draft-rass-panrg-mpath-usecase-00

S. Rass (presenter)
Universitaet Klagenfurt
stefan.rass@aau.at

Yingzhen Qu, Lin Han
Huawei
yingzhen.qu, lin.han@Huawei.com

Security should be, but is not, easy…

Confidentiality, Integrity, Availability + Authenticity (CIA+)

Today mostly by asymmetric crypto, which is…

expensive

computationally heavy

cumbersome/difficult
(certificate (renewals), …?)

Work-arounds

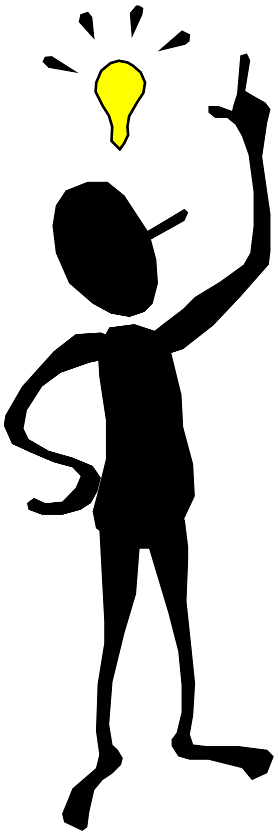
Usable Security

CIA+ Security can be achieved

- Only using symmetric crypto
  → no certificates (cheap)
  → faster (computationally lightweight)
- Using only point-to-point shared secrets
  → only device pairing required
- Without much user involvement (beyond device pairing)
  → transparent

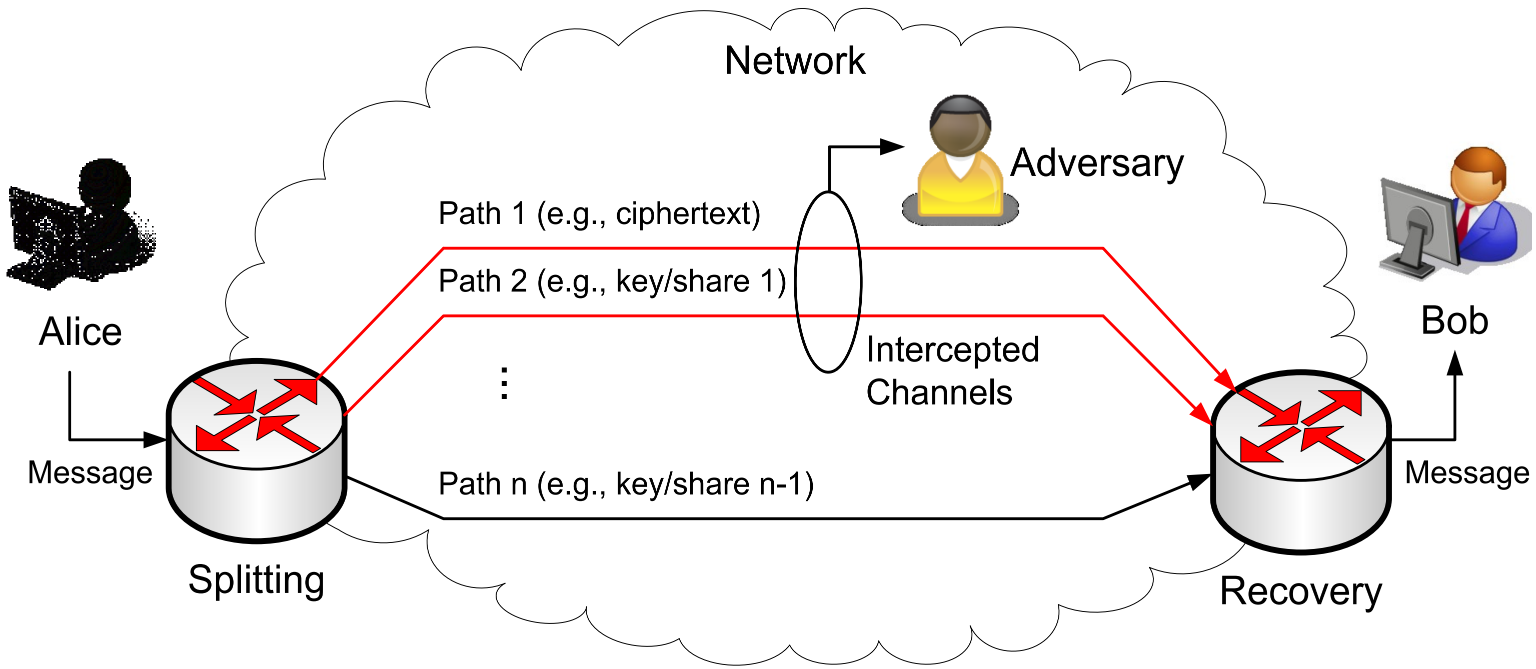
Method: multipath transmission

- Use multiple transmission paths chosen at random
- Perfect security via a moving target defense
- Trade computational complexity and intractability for certain network topological features



Secure Multipath Routing

- Split the message into parts (e.g., via secret sharing)
- Transmission over disjoint paths at random → security by a moving target defense[1]
- Achieves Confidentiality, Availability & Authenticity (with integrity implied by auth.)



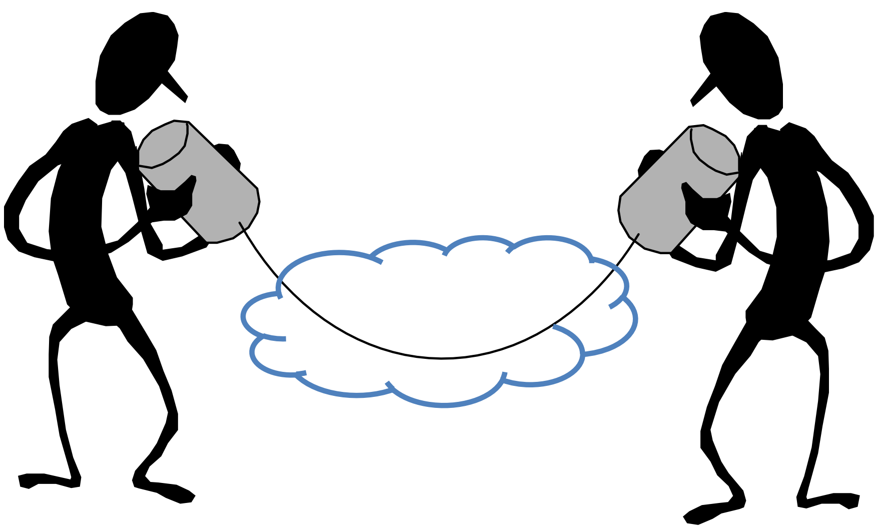
Special case: 2-path transmission ≅ symmetric encryption

[1] S. Rass, B. Rainer, M. Vavti, J. Göllner, A. Peer, S. Schauer: *Secure Communication over Software-Defined Networks*, Springer J. on Mobile Networks and Applications, 2015 , 20 , pp. 105-110

Requirements for the Use Case 1

- Reliable and up-to-date topology information
  - No. of paths
  - Path elements
  - Reliability of packet to stay on a path (probabilistic assurance)

```
3.1. Multi-path Service and User-
     Network Interface
3.2. Path and Routing Reliability
```

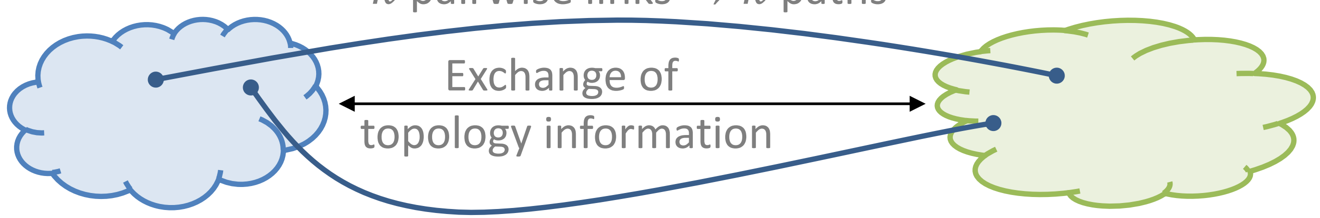


Requirements for the Use Case 2

- Cross-Domain aspects
  - Exchange of topology information between networks, also upon updates/changes (in either network)
  - Pairwise point-to-point joins of networks ($\rightarrow$ preservation of multi-paths)

3.3. Cross Domain Path Reliability
3.4. Cross Domain Network Connections
3.5. Updates upon Changing Network Topologies

k pairwise links $\rightarrow$ k paths



- Crypto keys established by simple device pairing

3.6. Enforced Device Pairing and De-Pairing

Questions?

Appendix

draft-rass-panrg-mpath-usecase-00

S. Rass (presenter)
Universitaet Klagenfurt
stefan.rass@aau.at

Yingzhen Qu, Lin Han
Huawei
yingzhen.qu, lin.han@Huawei.com

Security (by Game Theory)

- Multipath transmission admits a simple game-theoretic formulation (matrix game)
- Risk ρ (saddle-point value of the multipath transmission game model) upper-bounds the likelihood for a successful attack:

$$\Pr(\text{eavesdropping} \mid \text{known adversarial action space}) \leq \rho$$

- Theorem[2]: Let ρ be the game-theoretic risk. Then, every $\varepsilon > 0$ admits an efficient protocol (with an overhead that is polynomial in $\log(1/\varepsilon)$) such that the risk (likelihood) of eavesdropping is $\leq \varepsilon$, if and only if, $\rho < 1$.

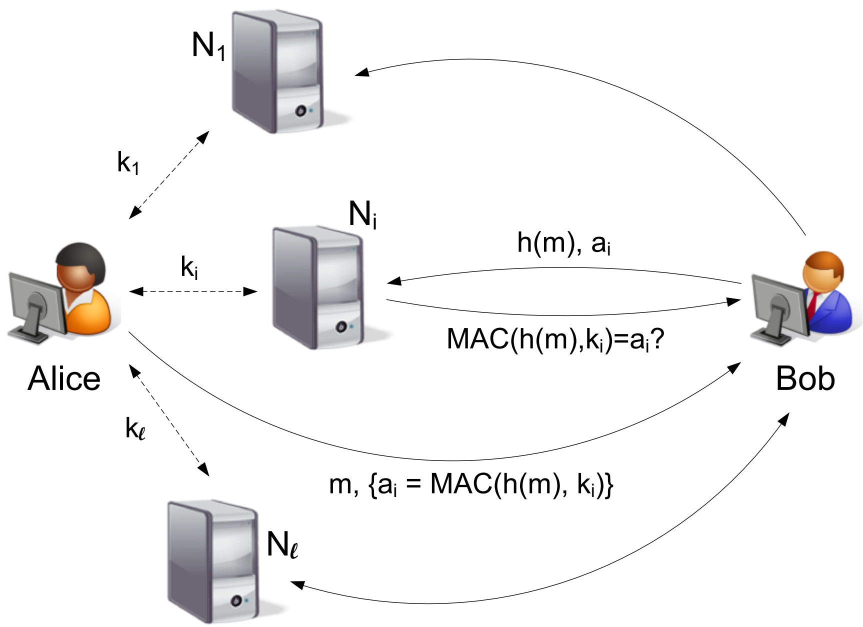
- This even holds under the relaxed assumption that the attacker can fiddle with the routing (to a limited extent)

- Industrial research project „RSB“ by the Austrian Institute of Technology

[2] S. Rass, S. König: *Indirect Eavesdropping in Quantum Networks*, ICQNM 2011, XPS Publishing Services, p. 83-88, available @ ThinkMind (open access)

Multipath Authentication[3]

- Sender „signs“ a message using secrets shared with direct neighbors
- Receiver asks these neighbors to verify the message authentication code (MAC)
- Implementable
  by segment or **preferred path routing**



- Security analysis and –guarantees like for SMR (previous slide).
- Industrial research project „RSB“ by the Austrian Institute of Technology

[3] S. Rass, P. Schartner: *Multipath Authentication without shared Secrets and with Applications in Quantum Networks*, Proc. of the Int. Conf. on Security and Management (SAM), CSREA Press, 2010 , 1 , pp.111-115

Prototype Implementation[1]