Multi-Path Secret Sharing for QKD Key Relay in IP Networks

draft-li-ipsecme-qkd-multipath-secret-sharing-00

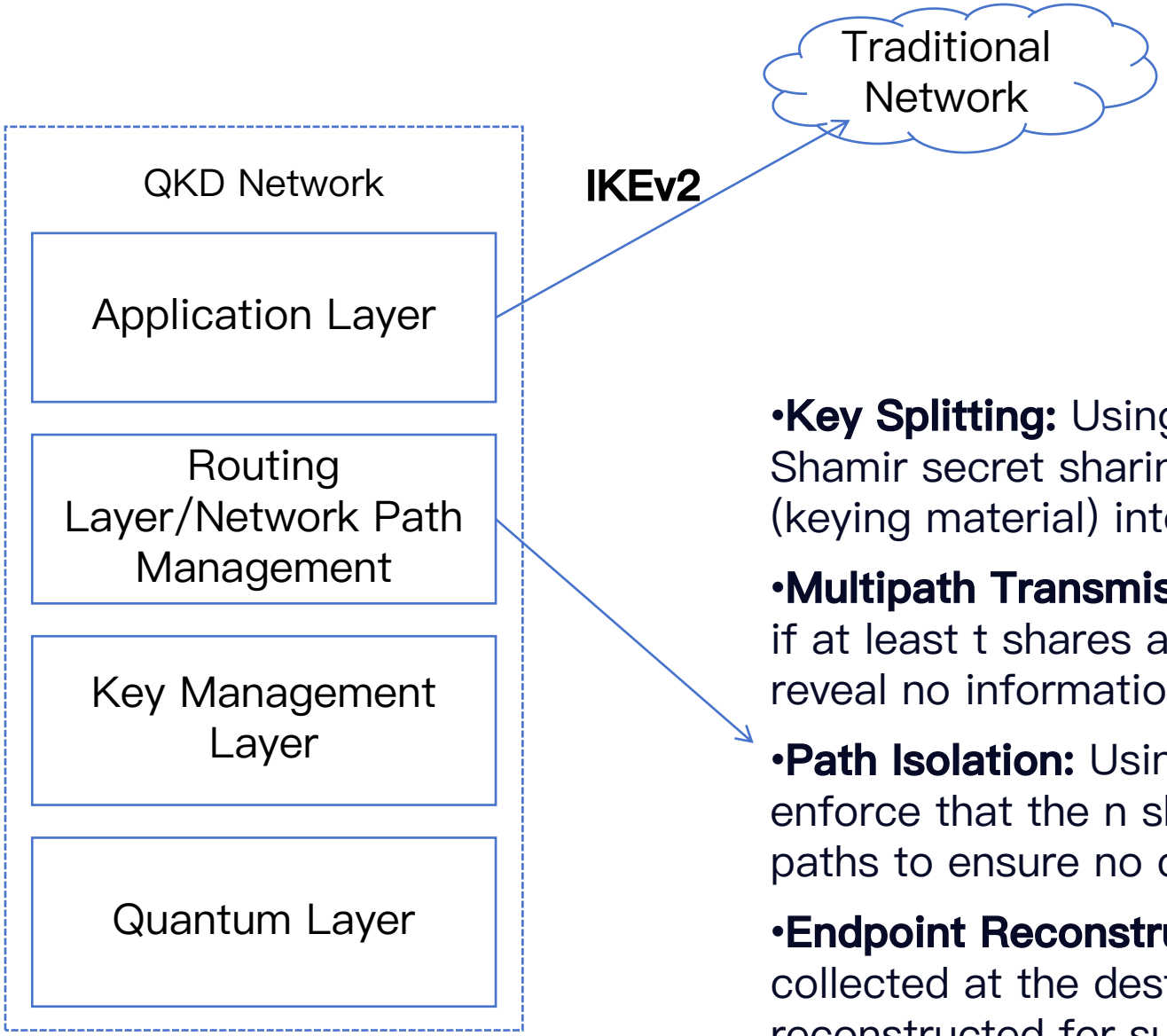
Jinming Li (China Mobile)
MengMeng Li (China Mobile)

IETF 125

Motivations

- **QKD Trusted Relay Problem**
  - –Leveraging the physical properties of quantum states, it is possible to achieve "any eavesdropping will be detected and the key cannot be copied". Its security is guaranteed by the laws of quantum mechanics and does not depend on computational complexity.
  - –In long–distance QKD networks, due to physical distance limitations, it is necessary to rely on intermediate "trusted relay nodes" to forward keys. At these nodes, the keys exist in plaintext (decrypted and then re–encrypted).
- **Challenges**
  - –This is an "all–or–nothing" security model. As long as any relay node on the path is compromised (whether through physical intrusion or logical vulnerabilities), the entire end–to–end key will be completely leaked. As the network scale expands, the probability of node compromise increases significantly.

Solution: Multi-Path Secret Sharing



This draft proposes a solution that transforms the security model from "single-point trust" to "threshold security". In the QKD network, SRv6 multipath planning is combined with key splitting to mitigate the "trusted node" problem.

- **Key Splitting:** Using a threshold secret sharing scheme (e.g., Shamir secret sharing), split the generated random number seed (keying material) into n shares.
- **Multipath Transmission:** The original key can only be recovered if at least t shares are collected (where $t \leqslant n$). Fewer than t shares reveal no information about the key.
- **Path Isolation:** Using SRv6 (Segment Routing IPv6) technology, enforce that the n shares are transmitted over n physically disjoint paths to ensure no common relay nodes.
- **Endpoint Reconstruction:** Only after sufficient shares are collected at the destination node can the full key be reconstructed for subsequent IPsec communication.

Next Steps

- Seeking broader review and feedback from WG
- Draft solution within or without the scope of the working group charter?

Thanks!