Principles of Ad Hoc Networking

Michel Barbeau and Evangelos Kranakis

November 12, 2007

Wireless security challenges

Network type	Challenge
Wireless	Open medium
Mobility	Handover implies change of security parameters
Ad hoc	Infrastructure based security not applicable
Sensor	In-network processing

Signature

1. Unforgeability: proof that the signer signed the document
2. Authenticity: convincing of the document's authenticity
3. Unreusability: signature cannot be "moved" elsewhere
4. Unalterability: document cannot be changed after signing
5. Unrepudiatability: signer cannot later claim: did not sign the document

Digital signature

- Set of messages: P; Set of signatures: A; Set of keys: K
- Signing algorithm: $Sig_k : P \to A$, with $k \in K$
- Verification algorithm: $Ver_k : P \times A \to \{true,\ false\}$
- $Ver_k(x, y) = \begin{cases} true & \text{if } y = Sig_k(x) \\ false & \text{if } y \neq Sig_k(x). \end{cases}$

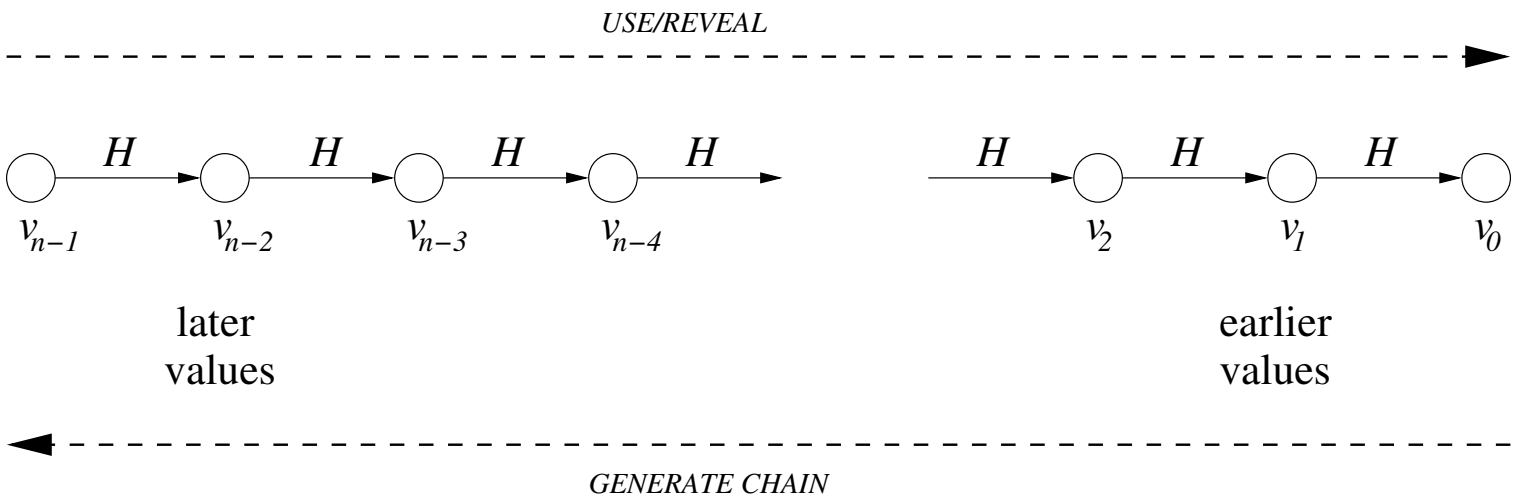
RSA signature

- An integer $n = pq$, the product of two distinct primes p and q
- Two integers e, d such that $ed \equiv 1 \bmod \phi(n)$, $\phi(n)$ is the Euler totient function
- n, e are public; p, q, d are private
- Signature: $Sig(M) \equiv M^d \bmod n$
- Verification: $Ver(M, N) = true \Leftrightarrow M \equiv N^e \bmod n$

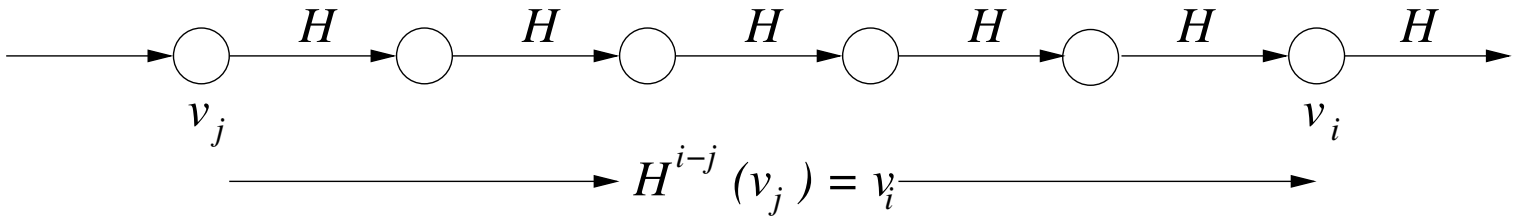
ElGamal signature

-

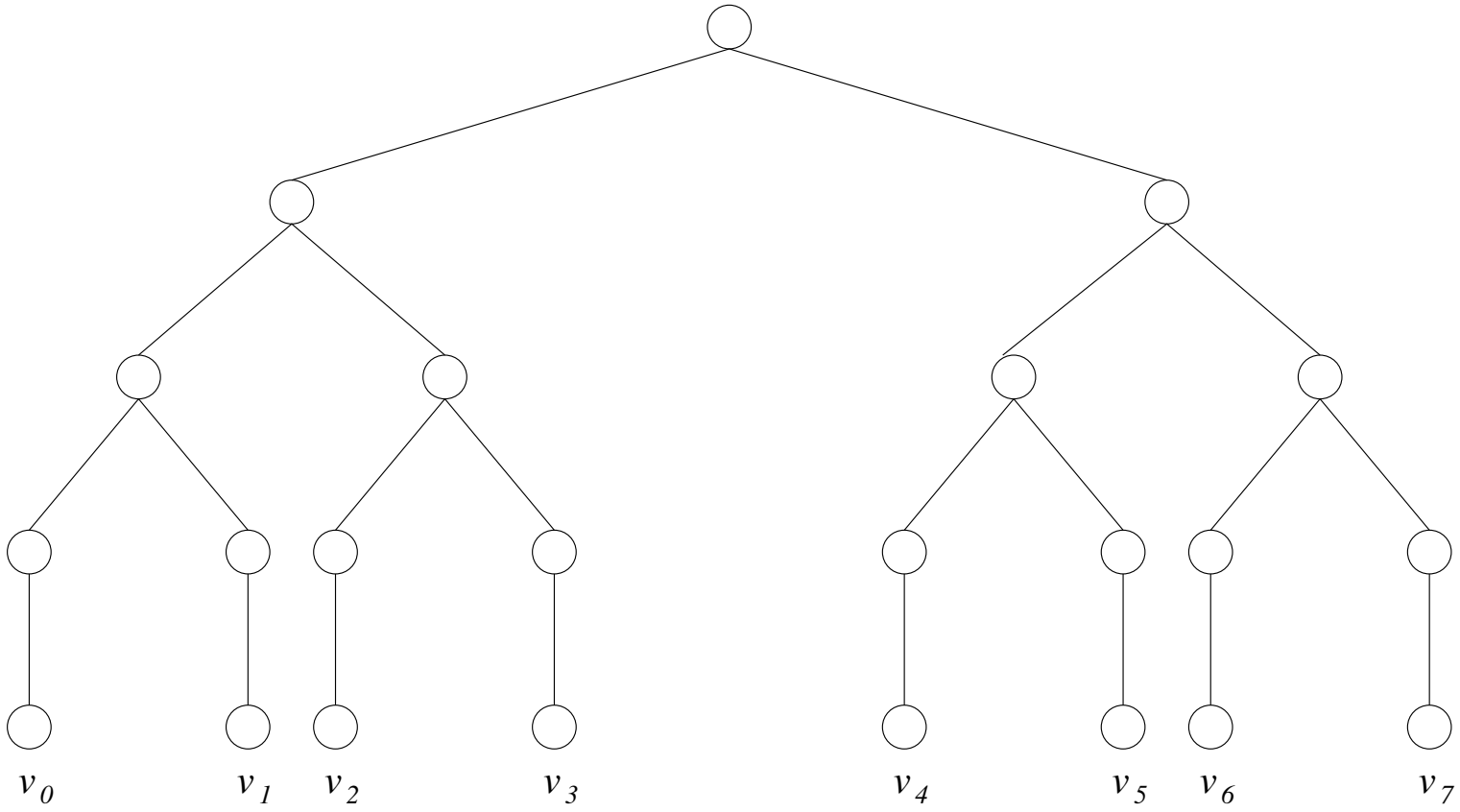
Constructing one-way hash chains



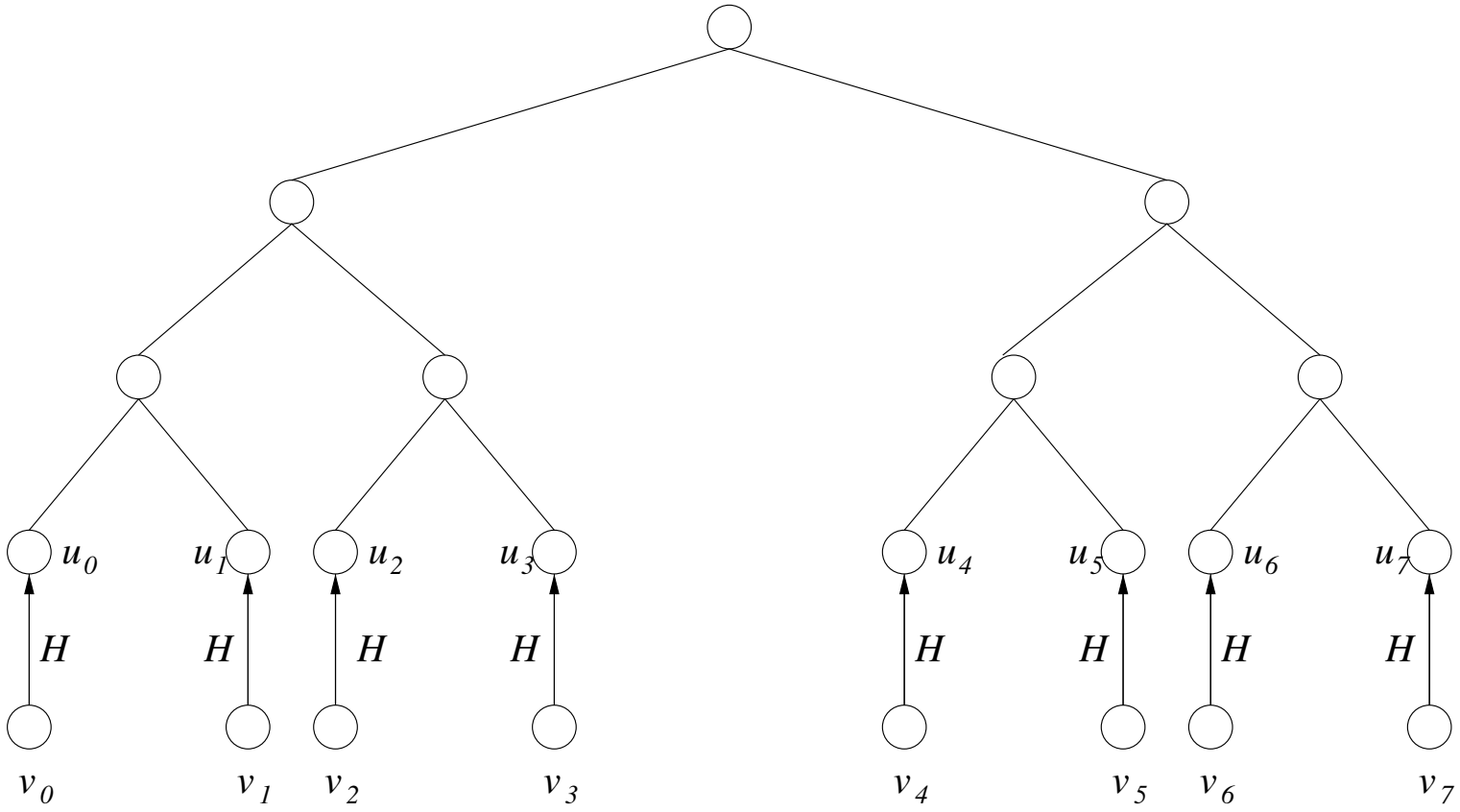
Authentication in one-way hash chains



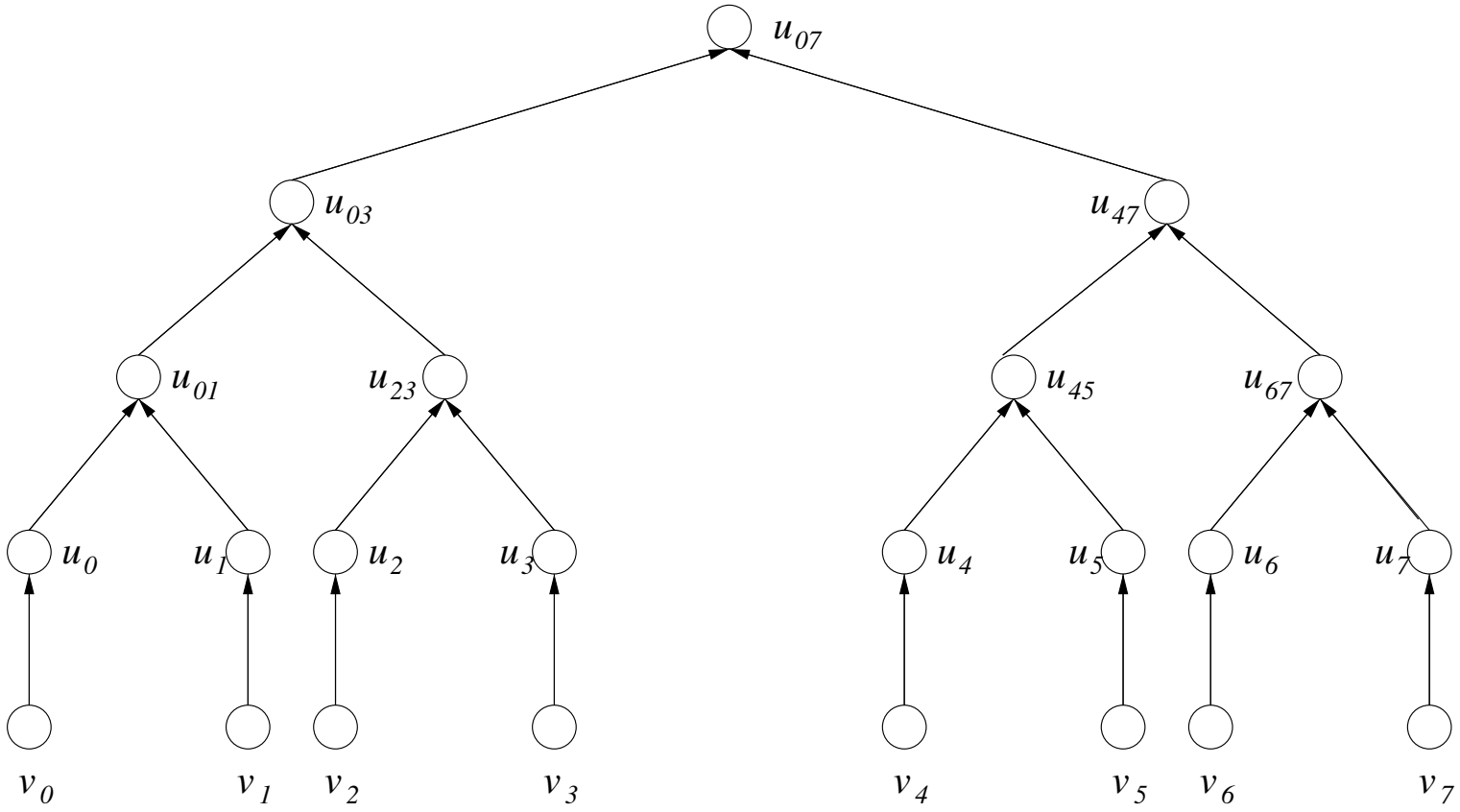
Forming a Merkle tree



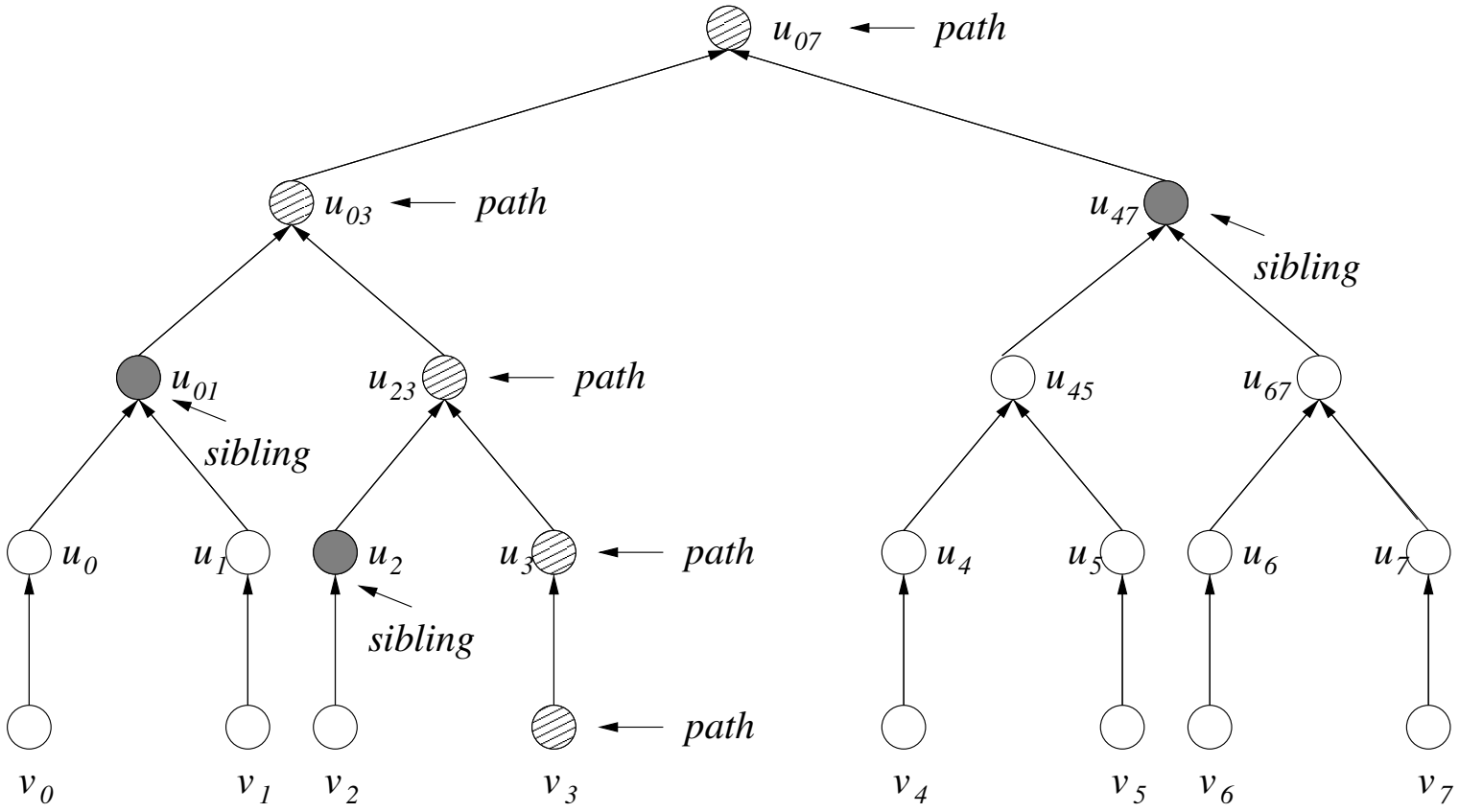
Blinding in Merkle authentication trees



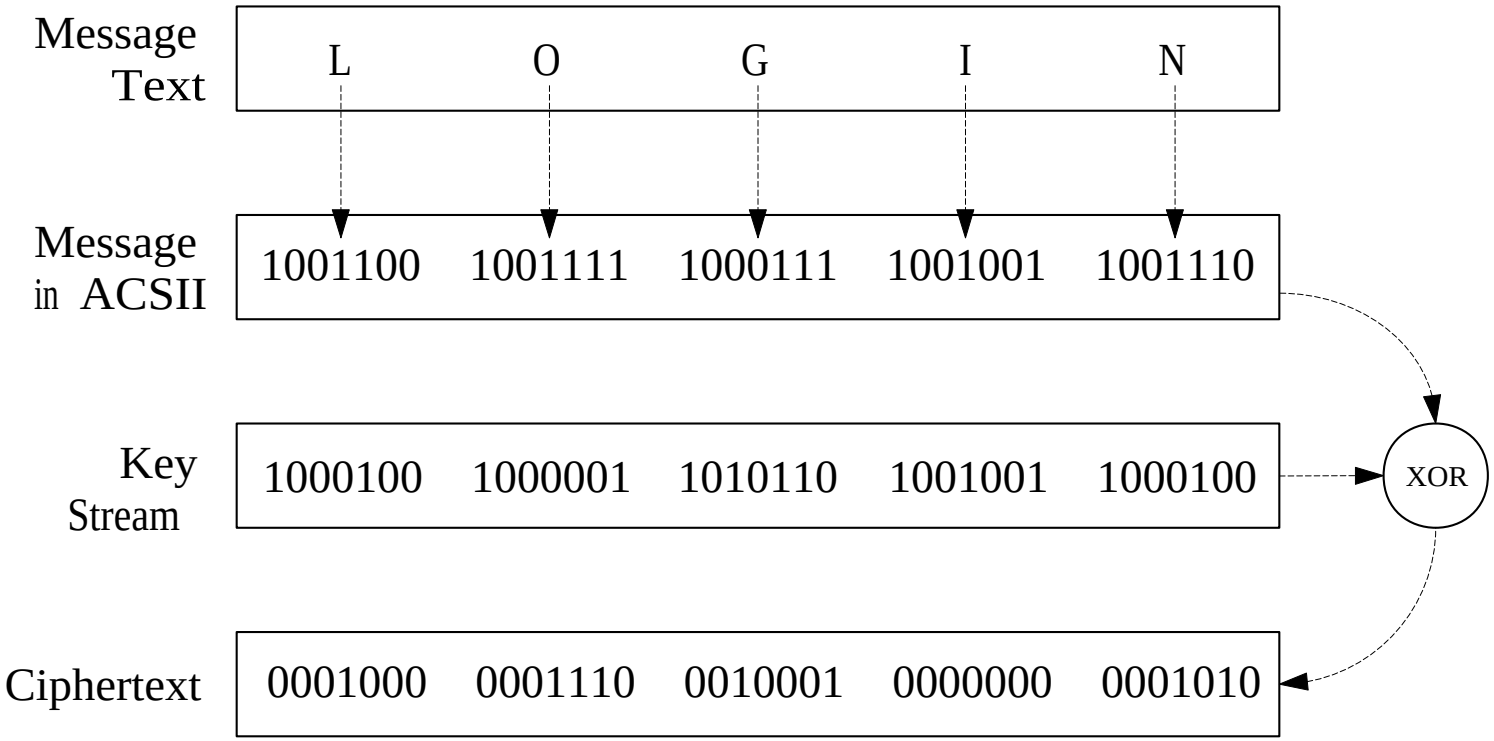
Recursive hashing in Merkle authentication trees



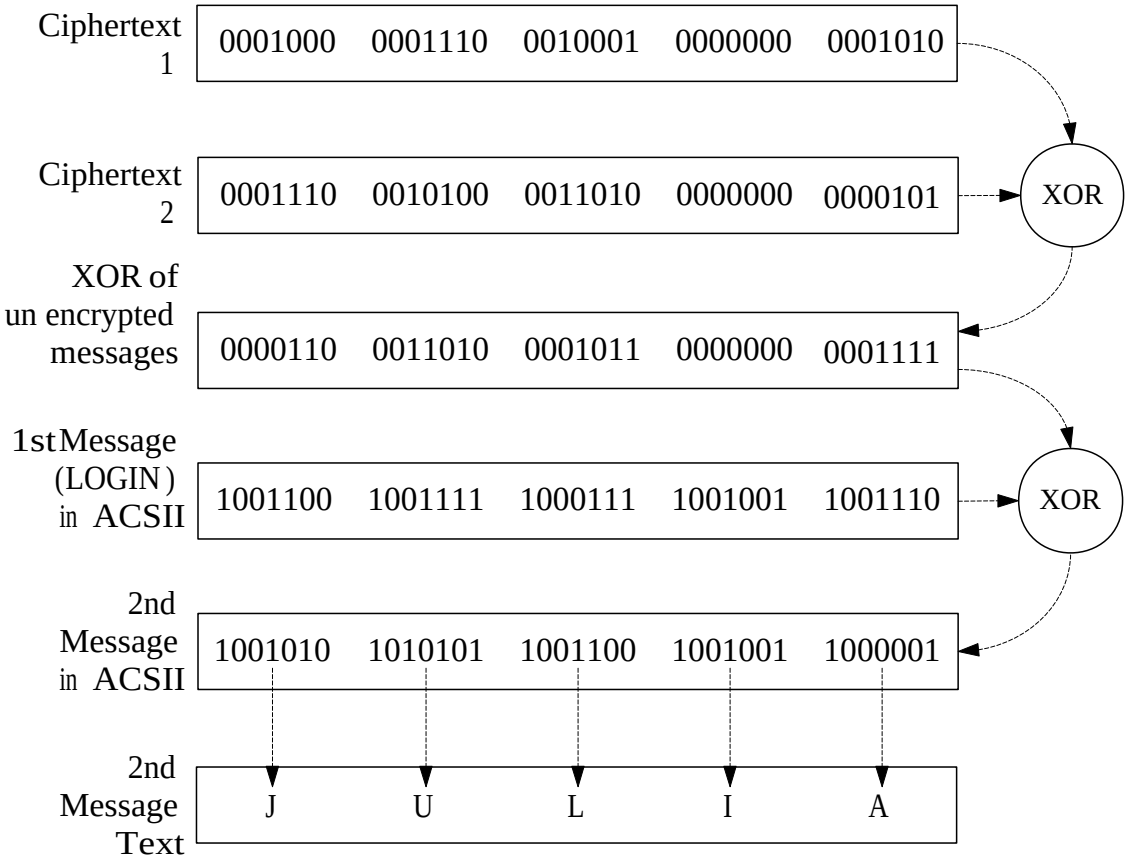
Example of Merkle authentication trees



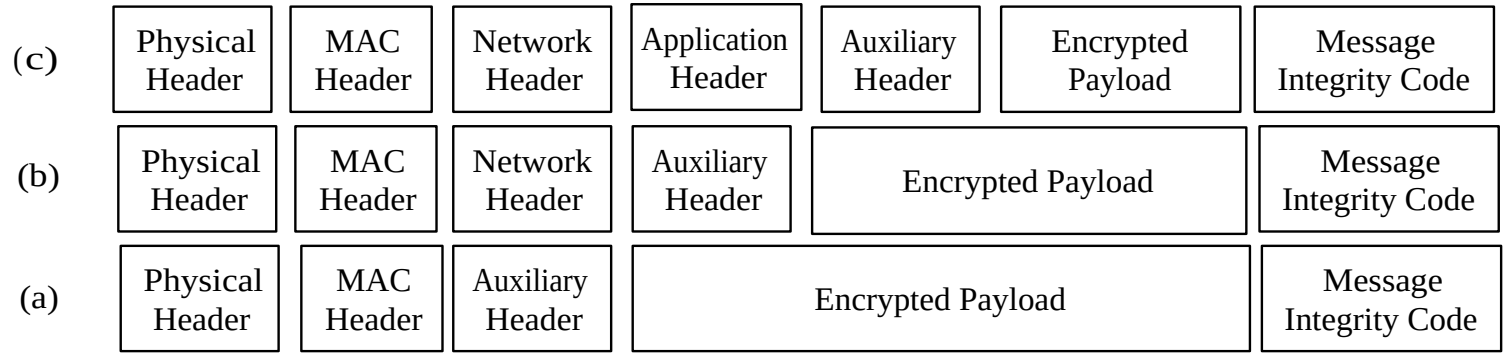
The RC4 encryption



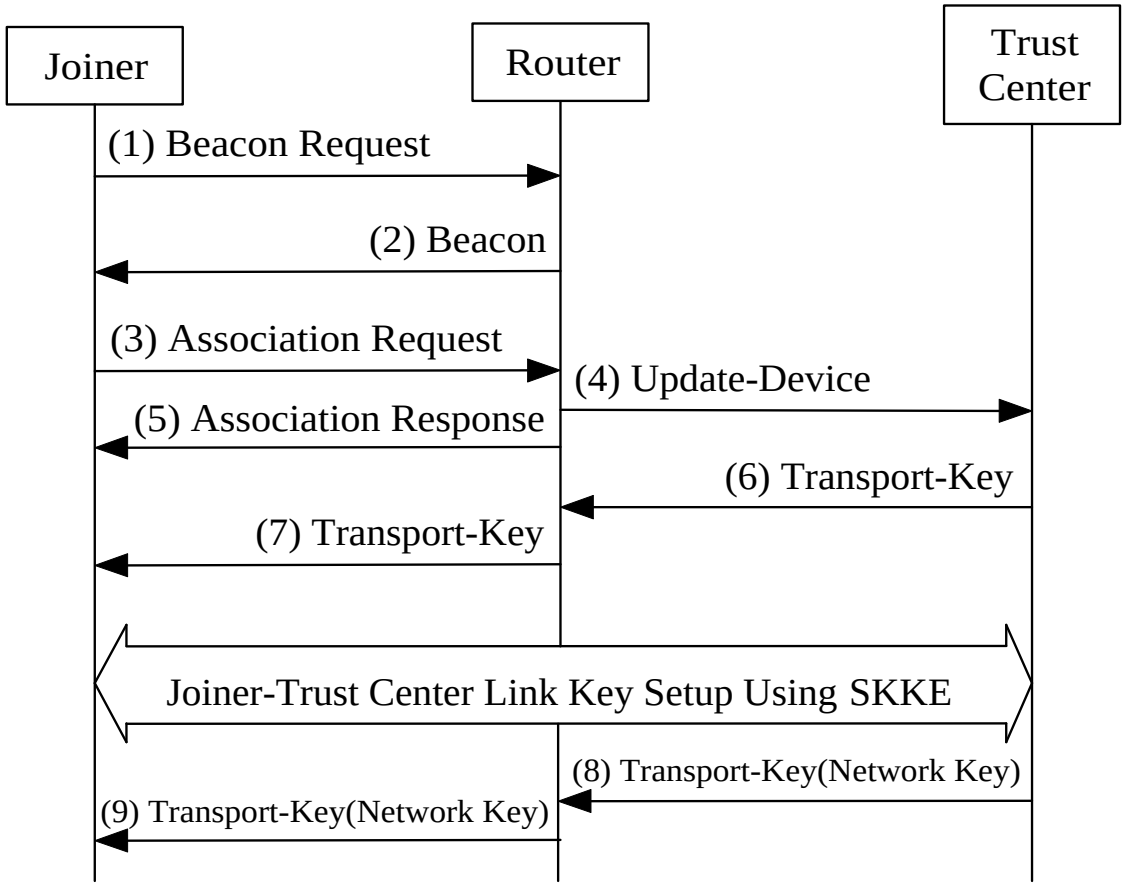
Cracking RC4 messages



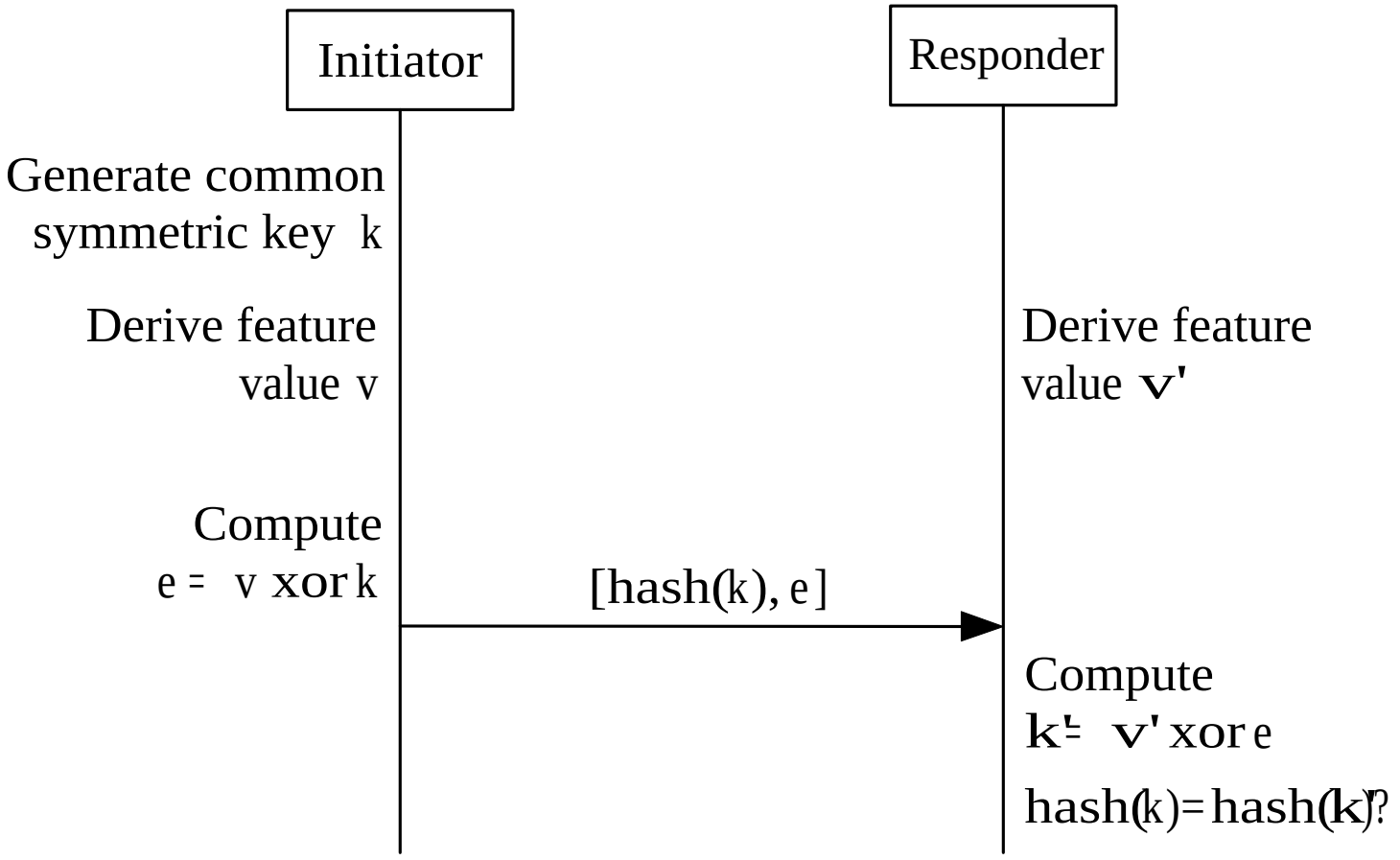
ZigBee frame with auxiliary header



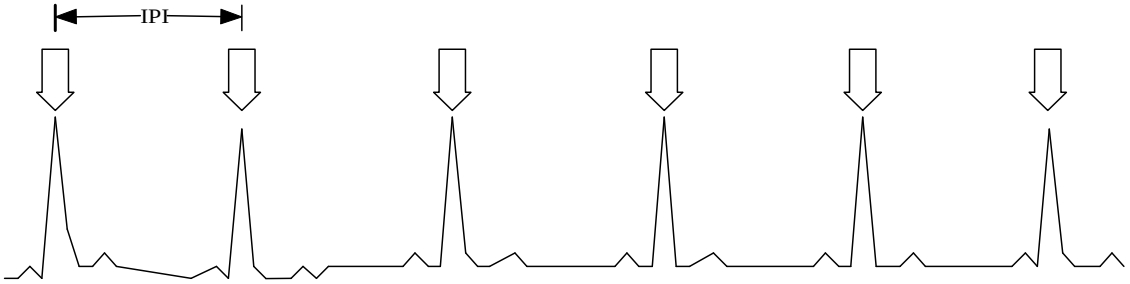
ZigBee network entry



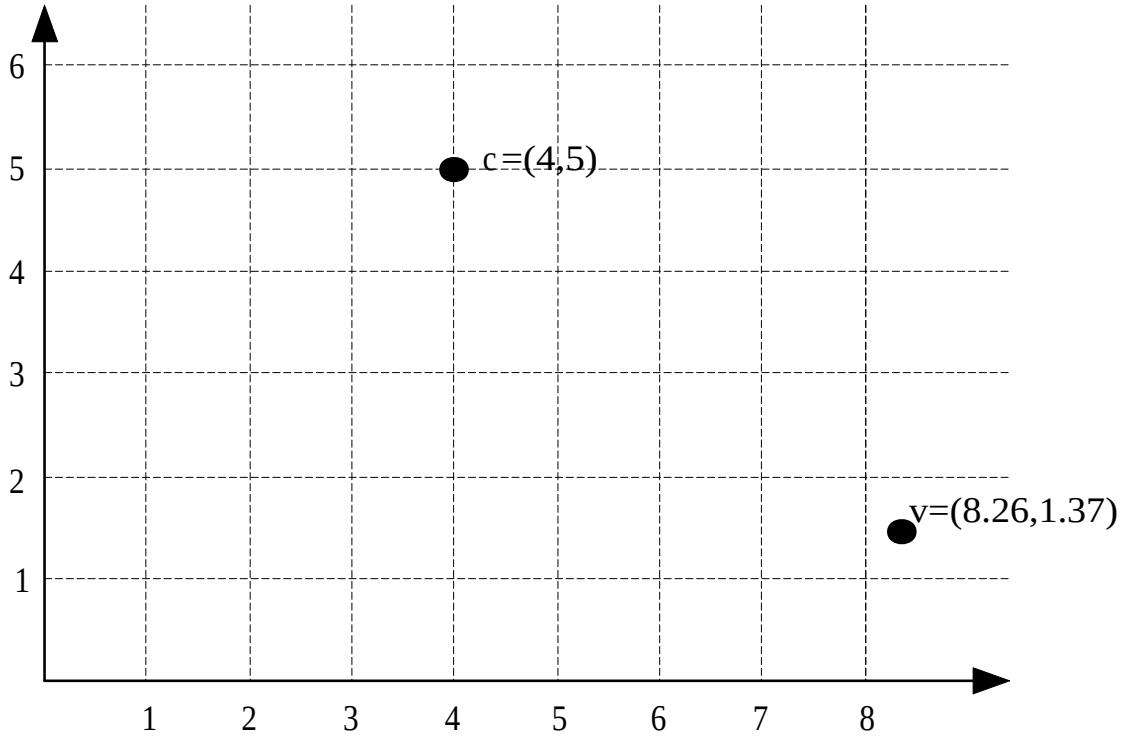
Key establishment using the fuzzy commitment protocol



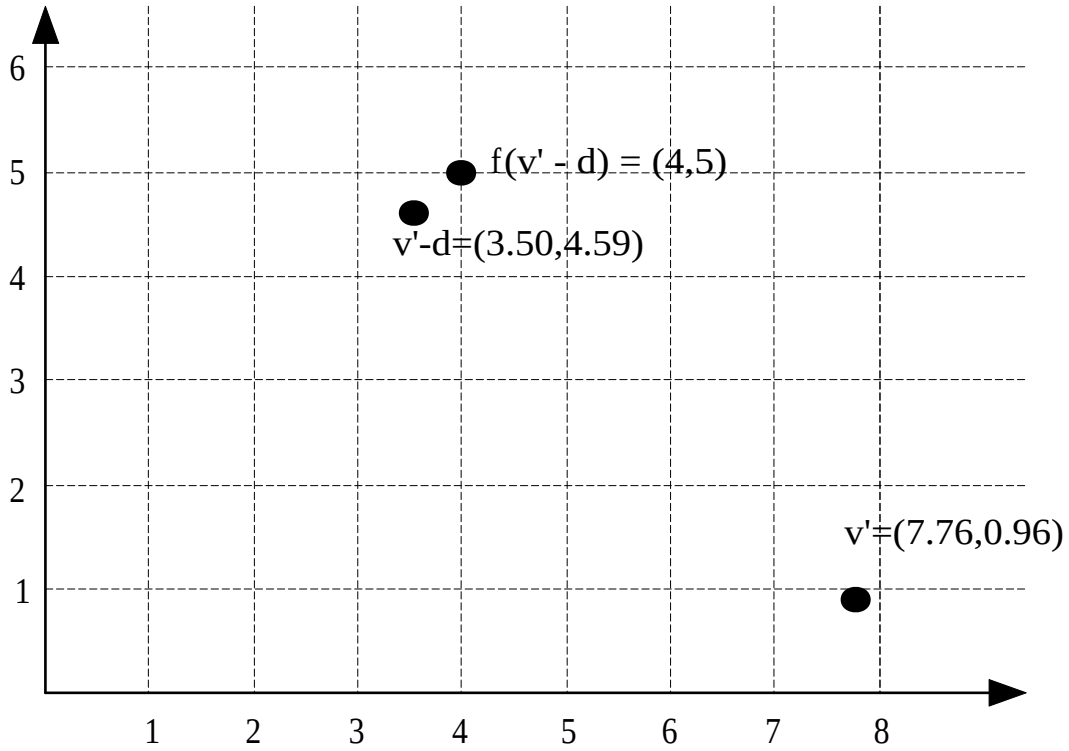
ECG with IPI markers



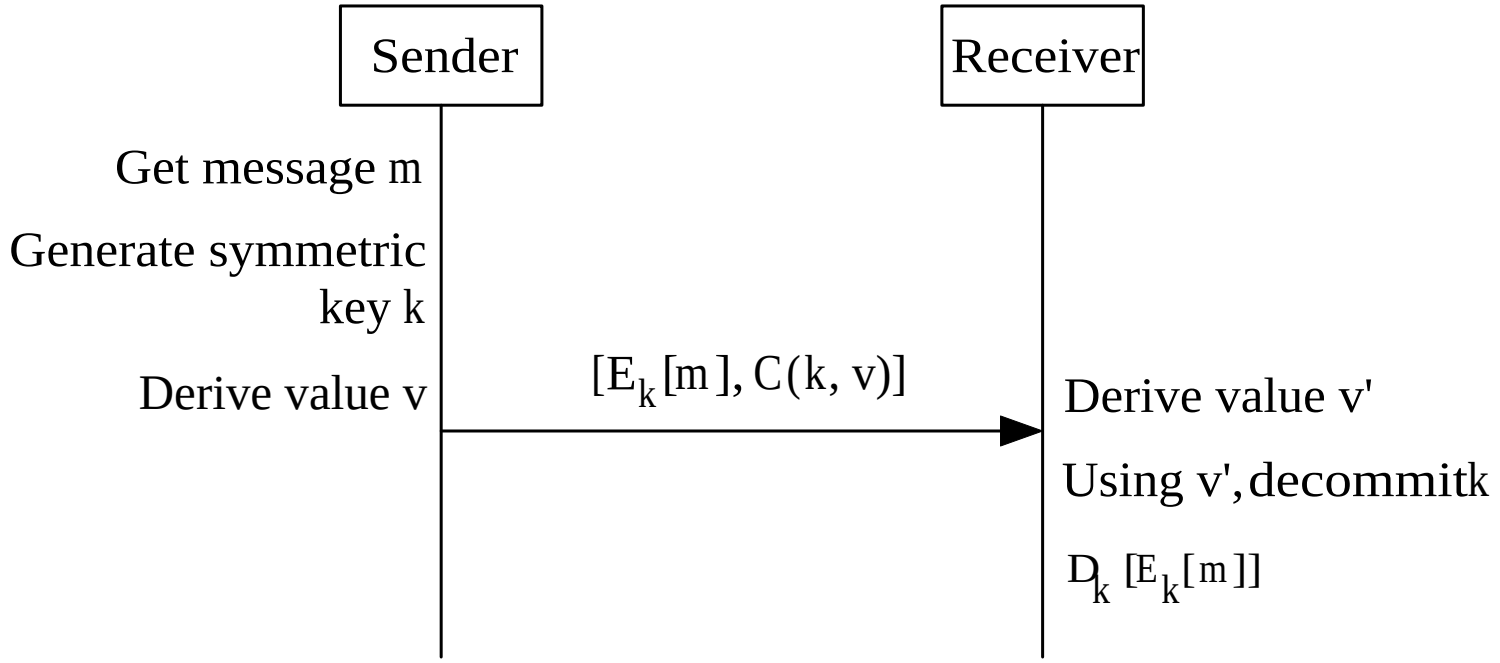
Initiator calculation in the fuzzy commitment protocol



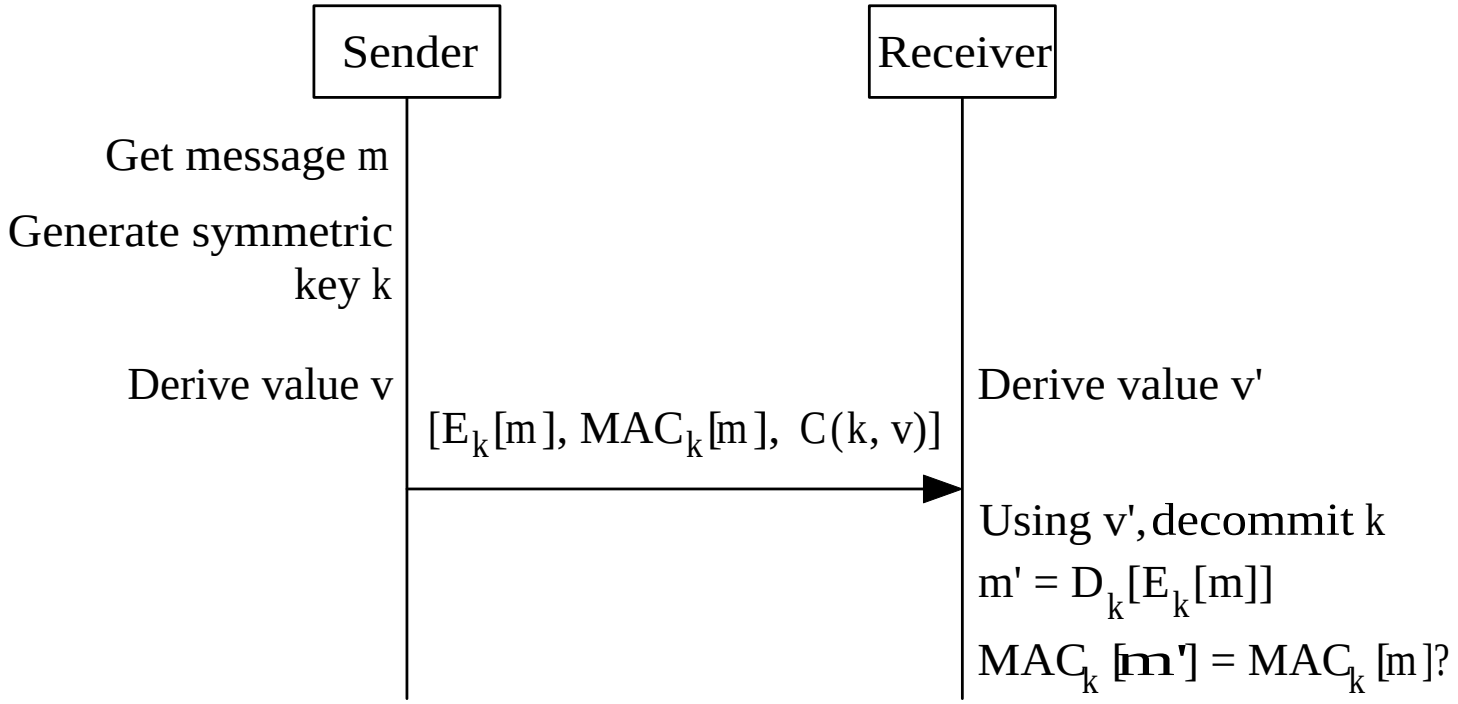
Responder calculation in the fuzzy commitment protocol



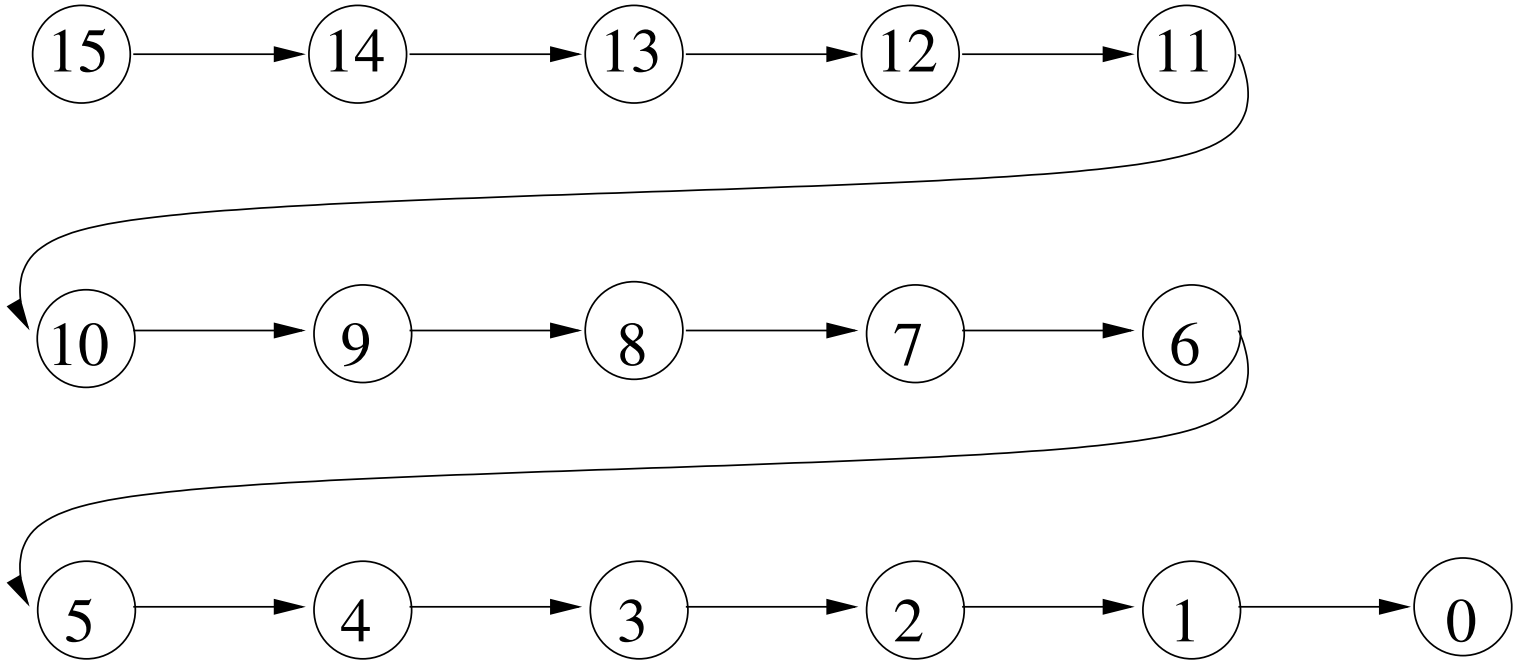
Fuzzy encryption protocol



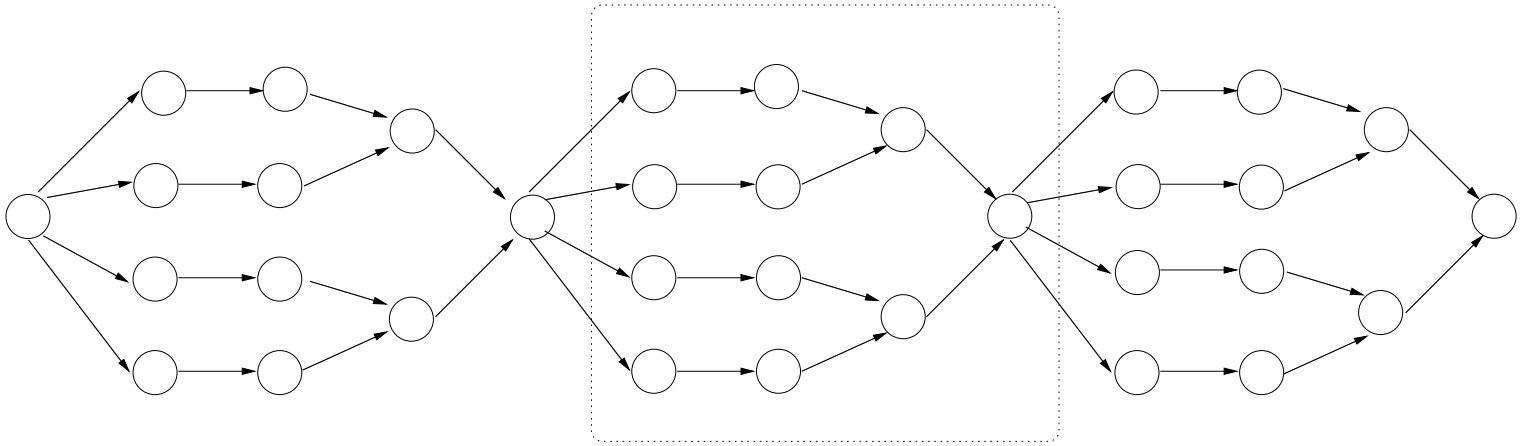
Authentication using the fuzzy commitment protocol



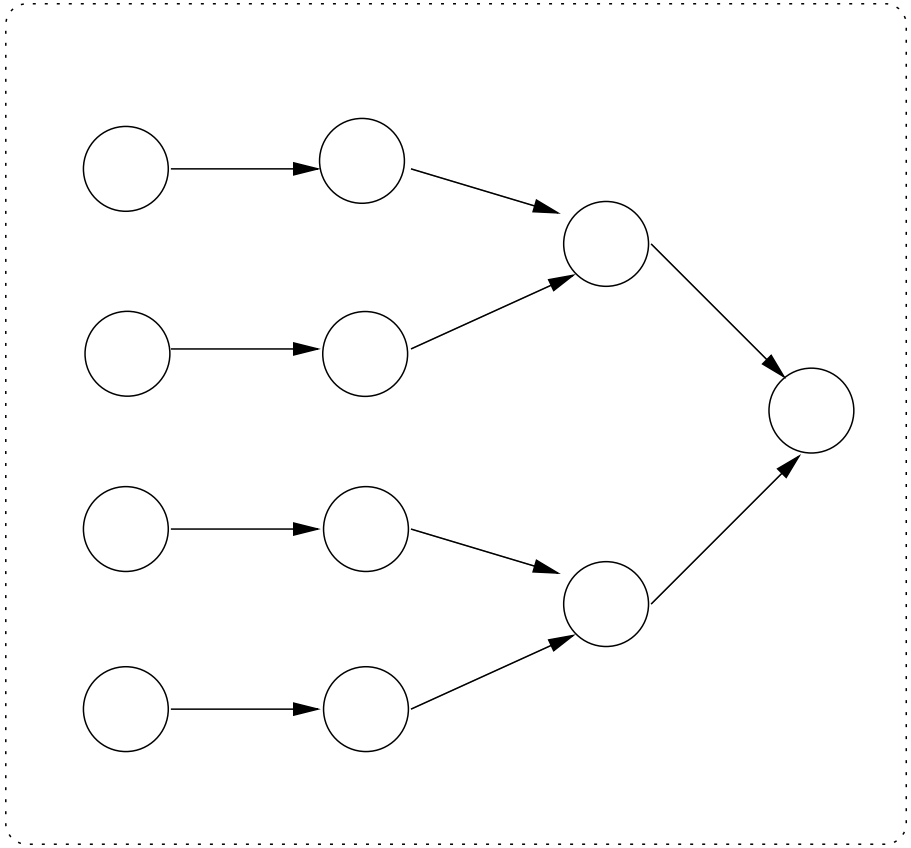
Example of SEAD implementation (only indices are depicted)



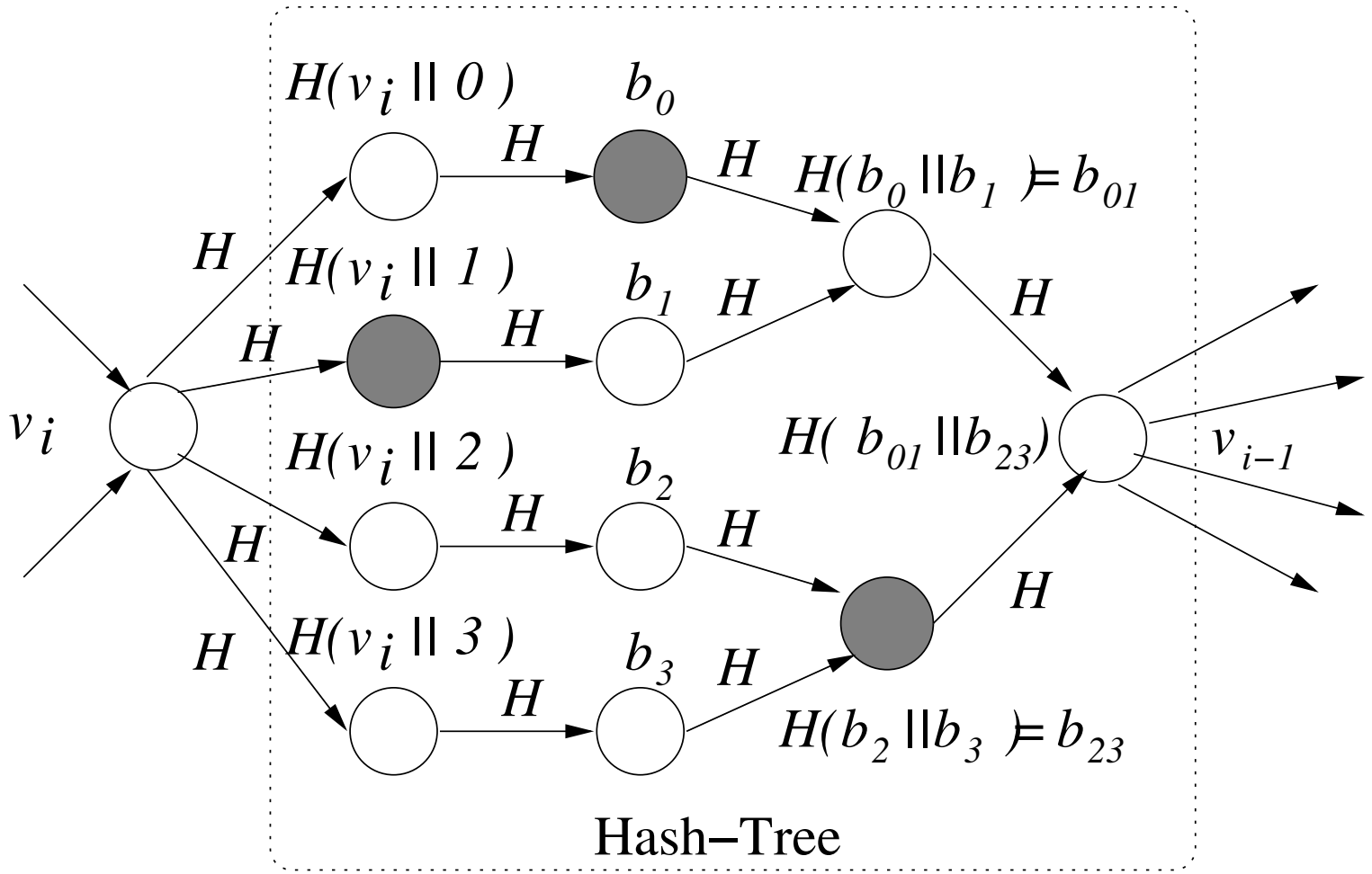
Example of hash tree chain. One-way chain generation



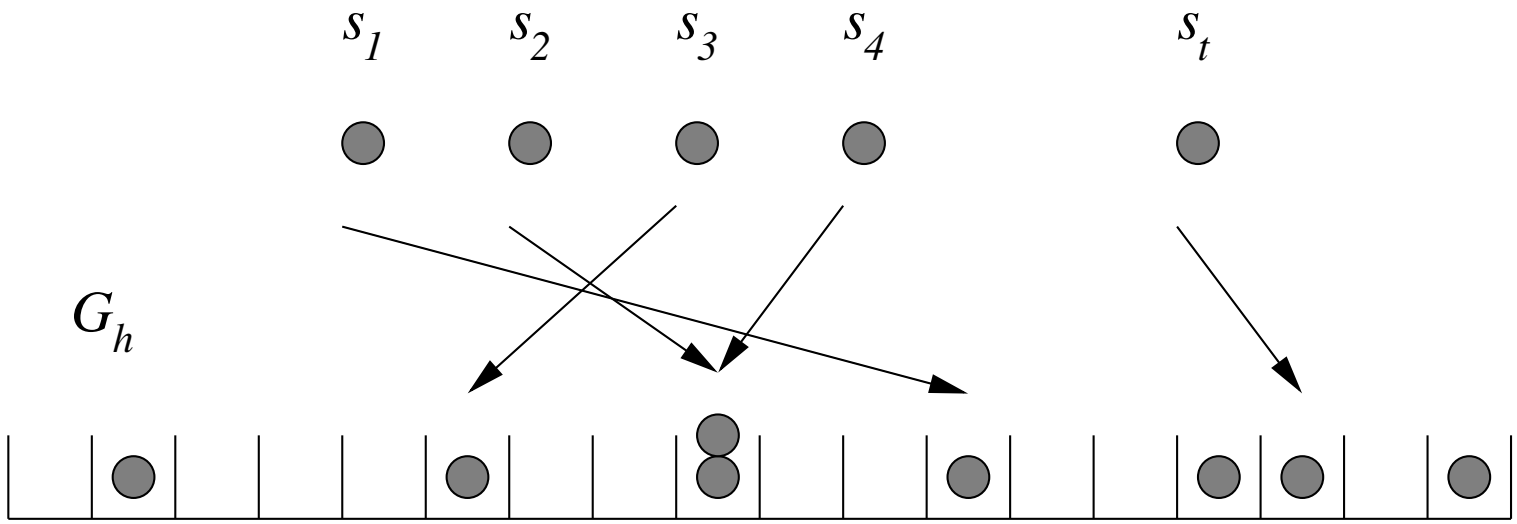
Merkle tree



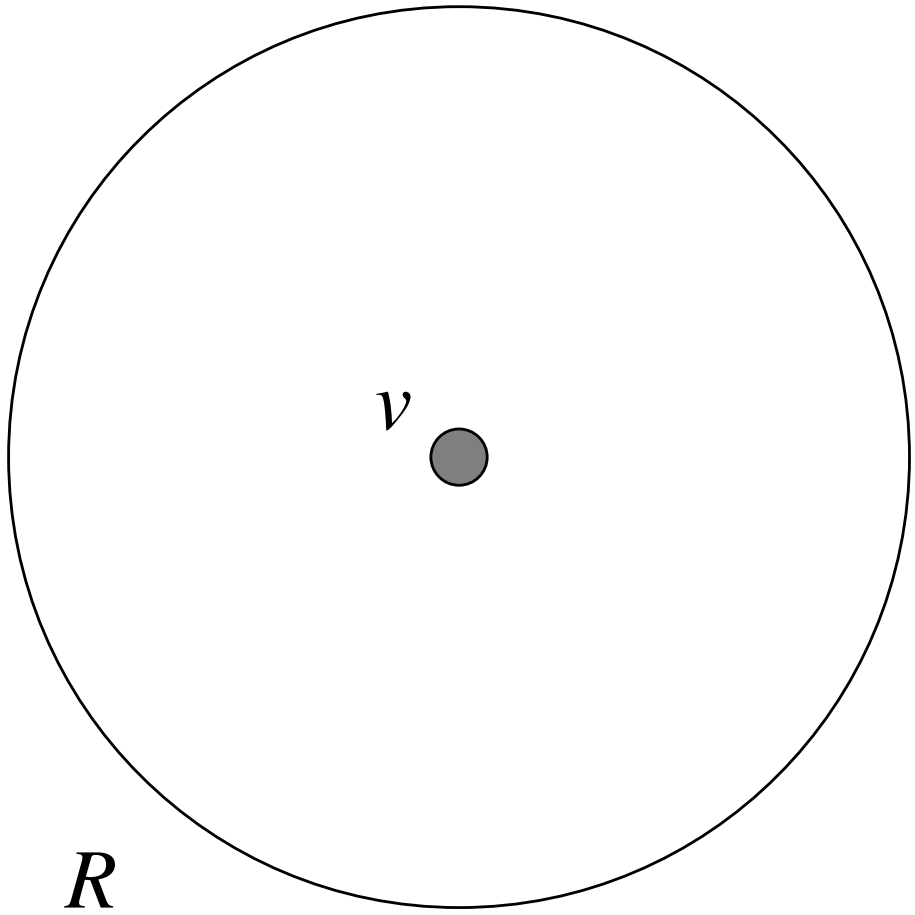
Example of using the hash tree chain



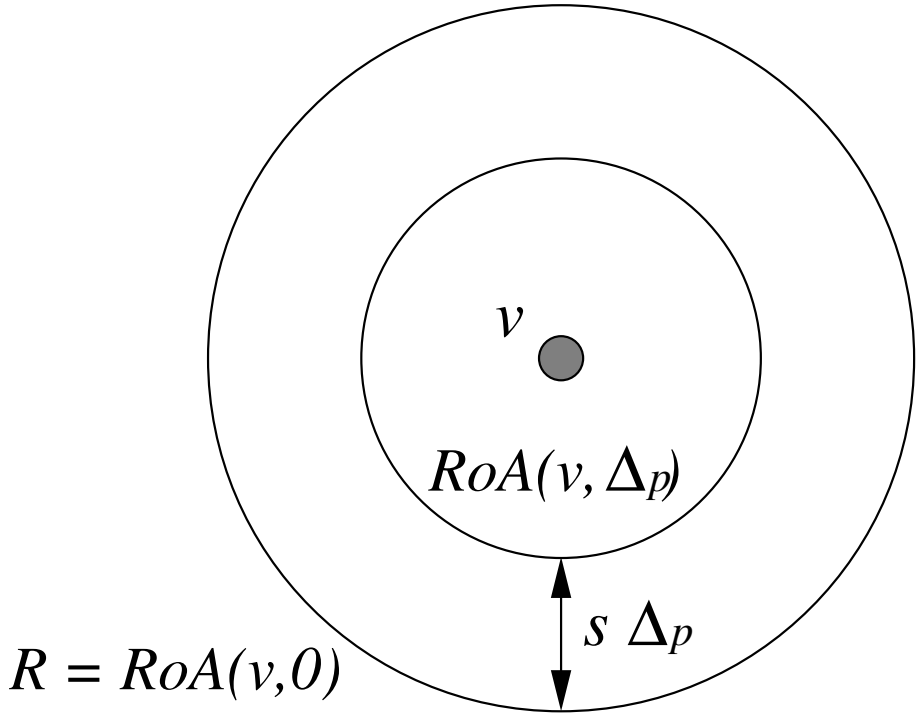
The bin-and-balls signature scheme



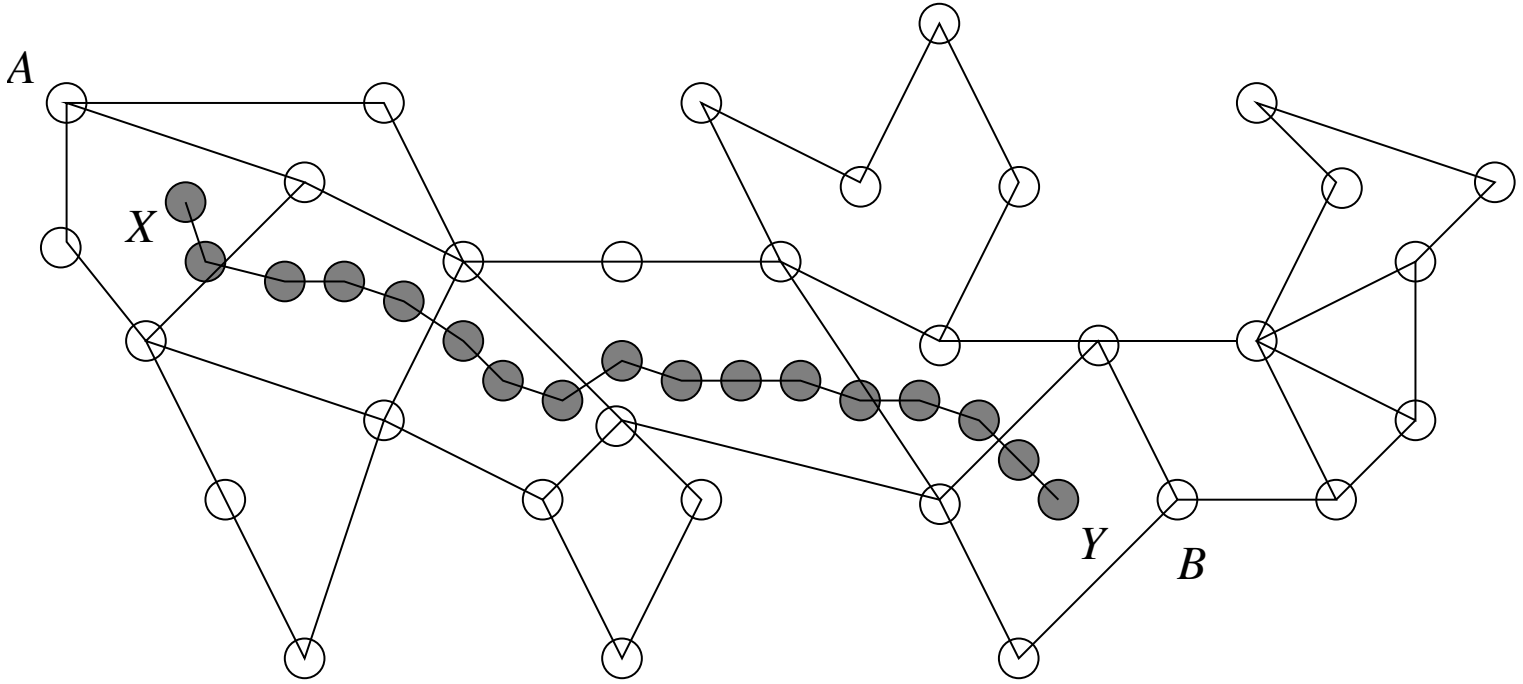
A single verifier v (inside region R) and a prover p (not depicted)



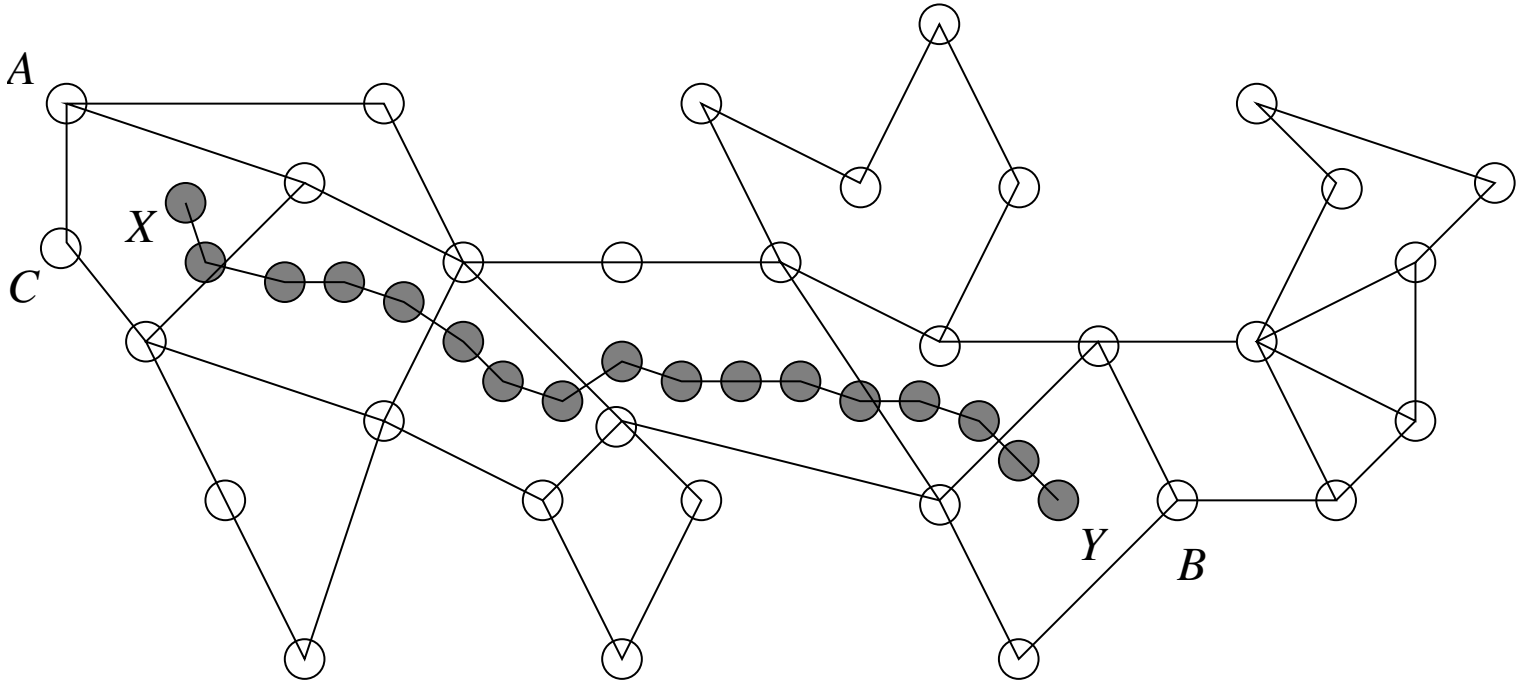
A single verifier at the center of a circular region R where there is an upper bound of Δ_p on the processing delay



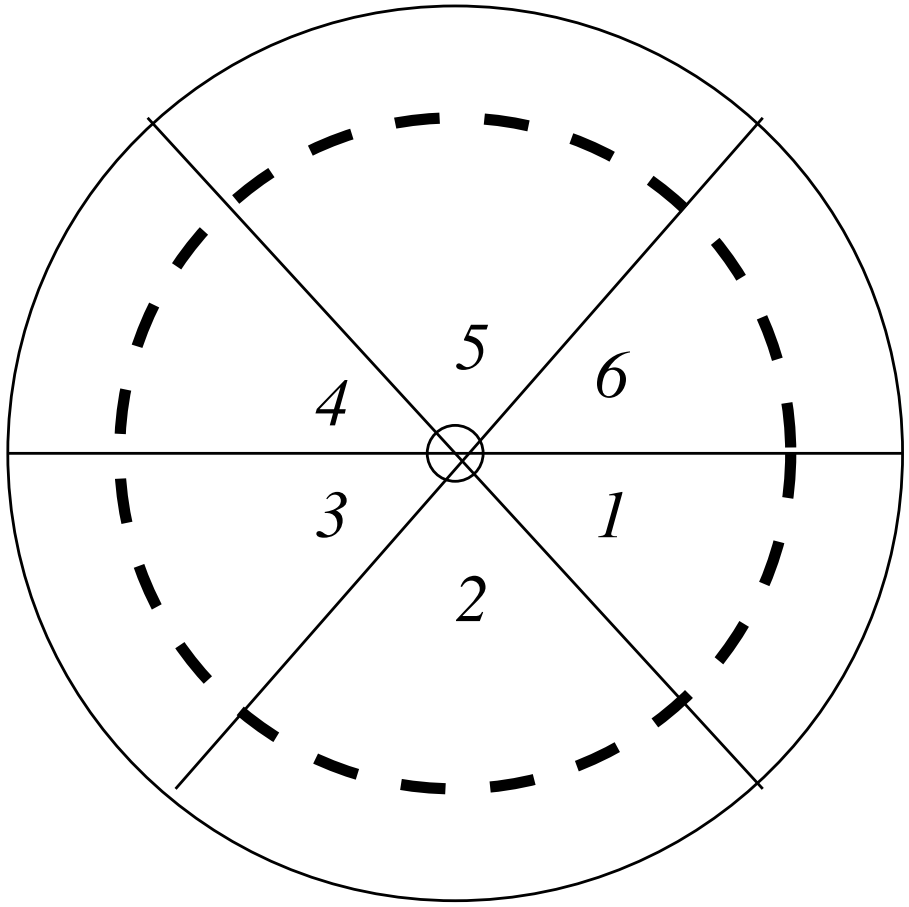
Wormhole attack



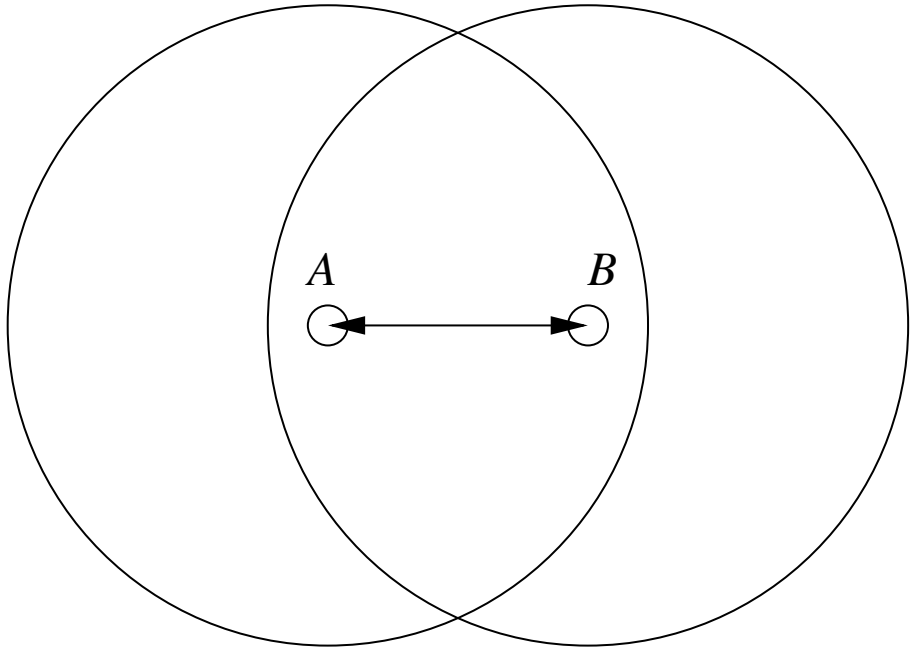
Impact on routing protocols: one hop tunneling



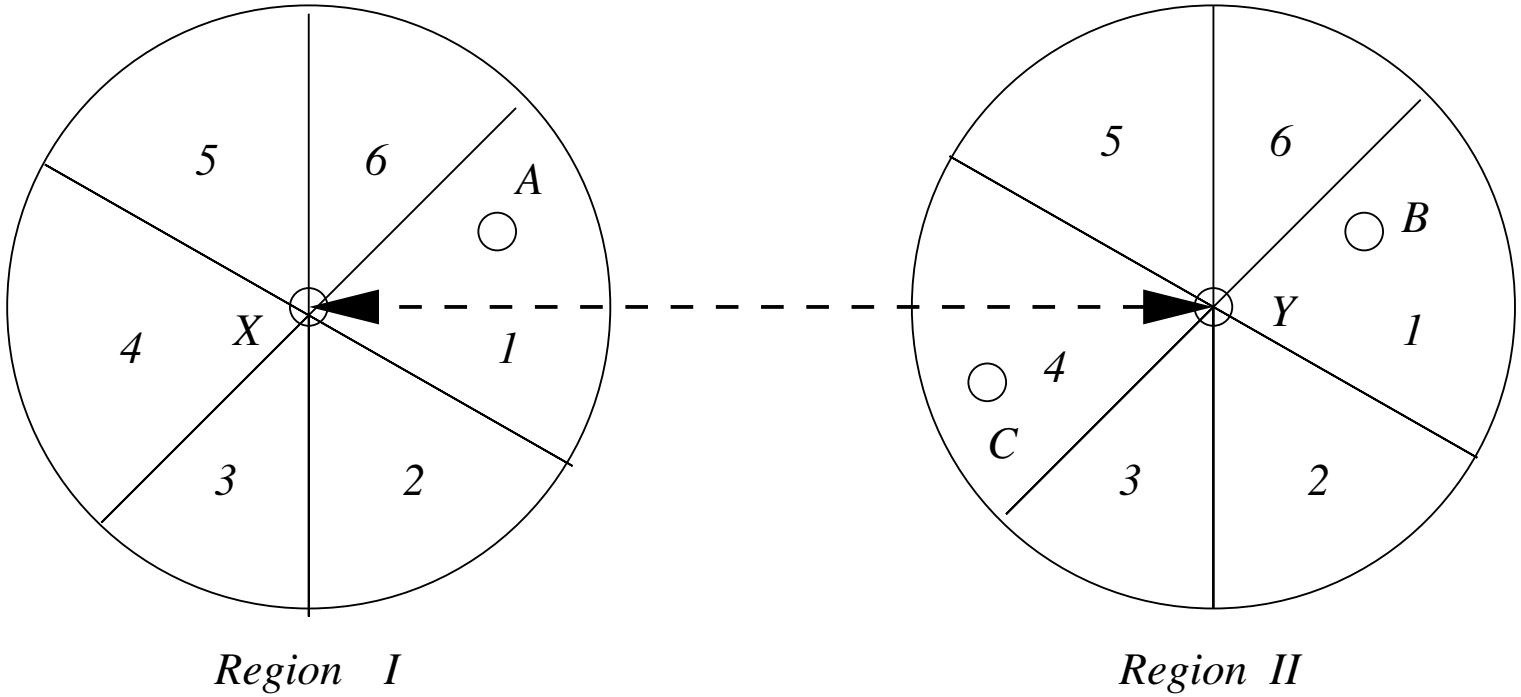
Partitioning the range of the sensors into six zones numbered $1, 2, \ldots, 6$ clockwise



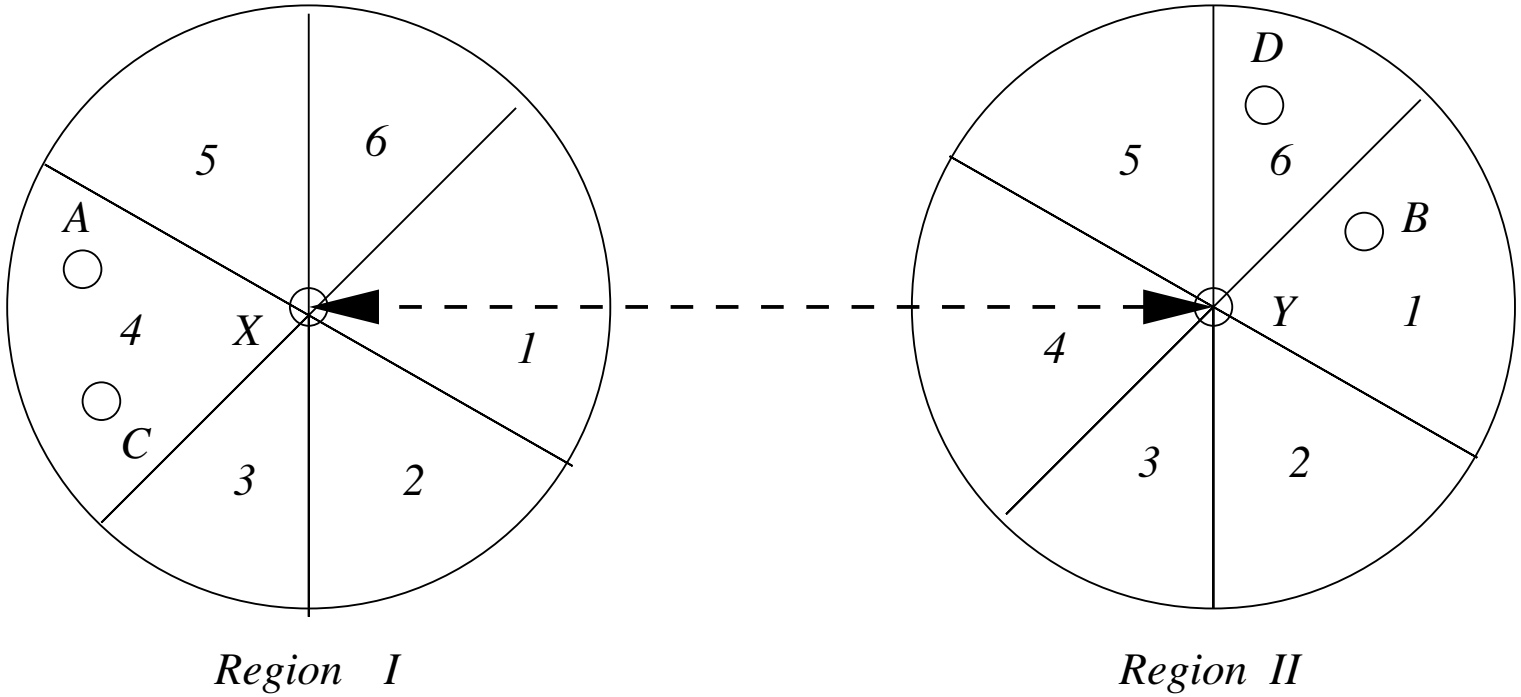
Bidirectional communication link



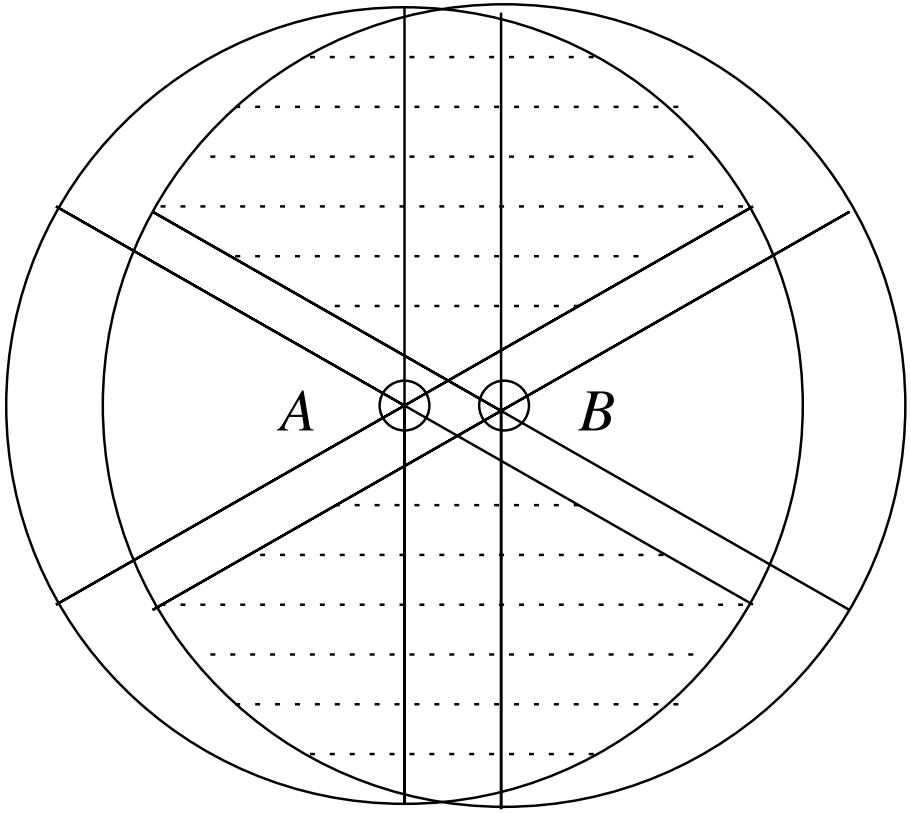
Wormhole vulnerability in the first protocol



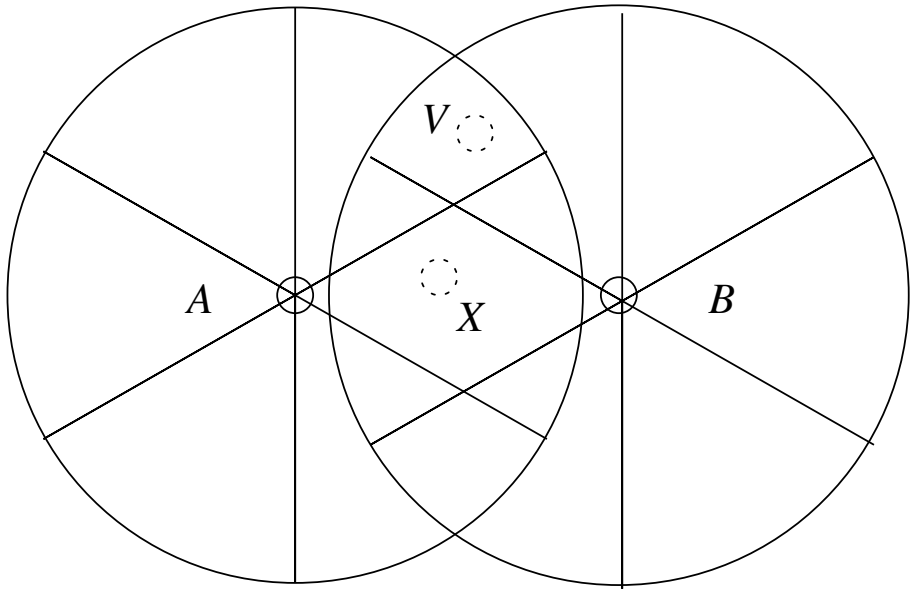
Cooperating with neighbors to prevent protocol vulnerabilities



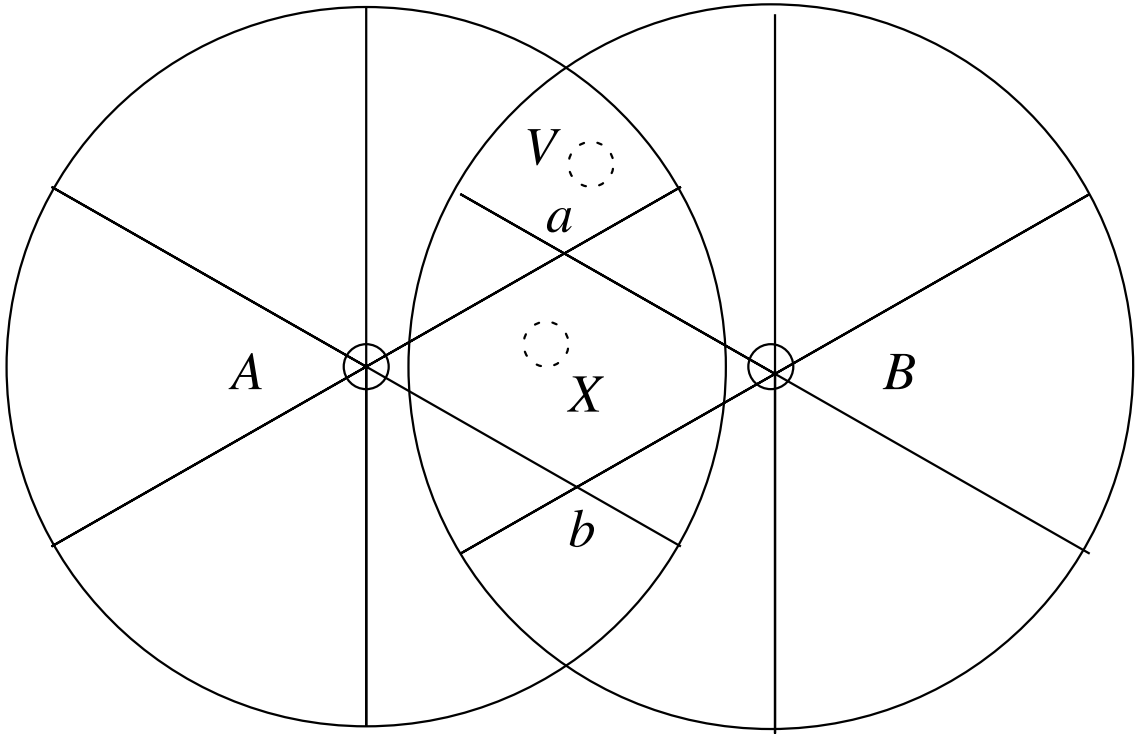
Verifier region



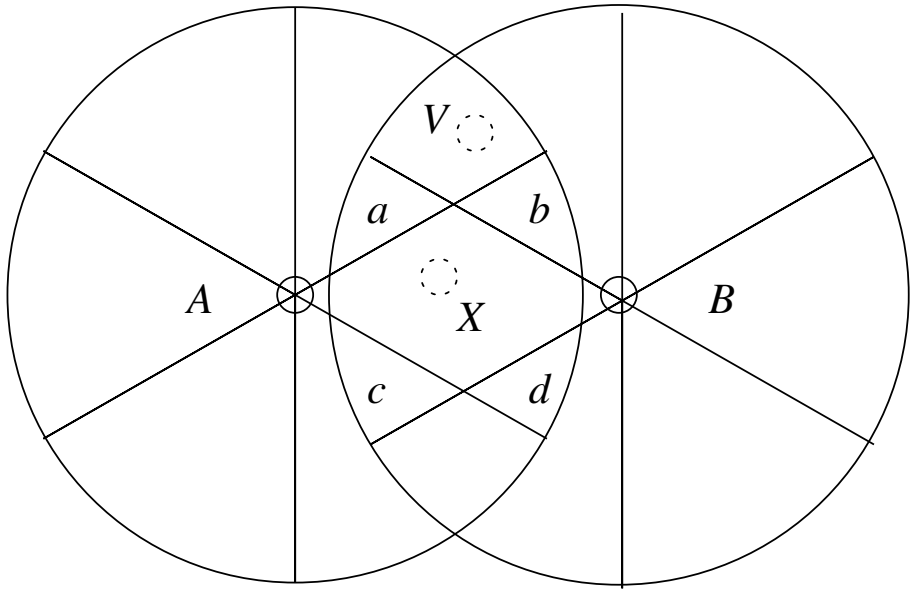
Worawannotai attack



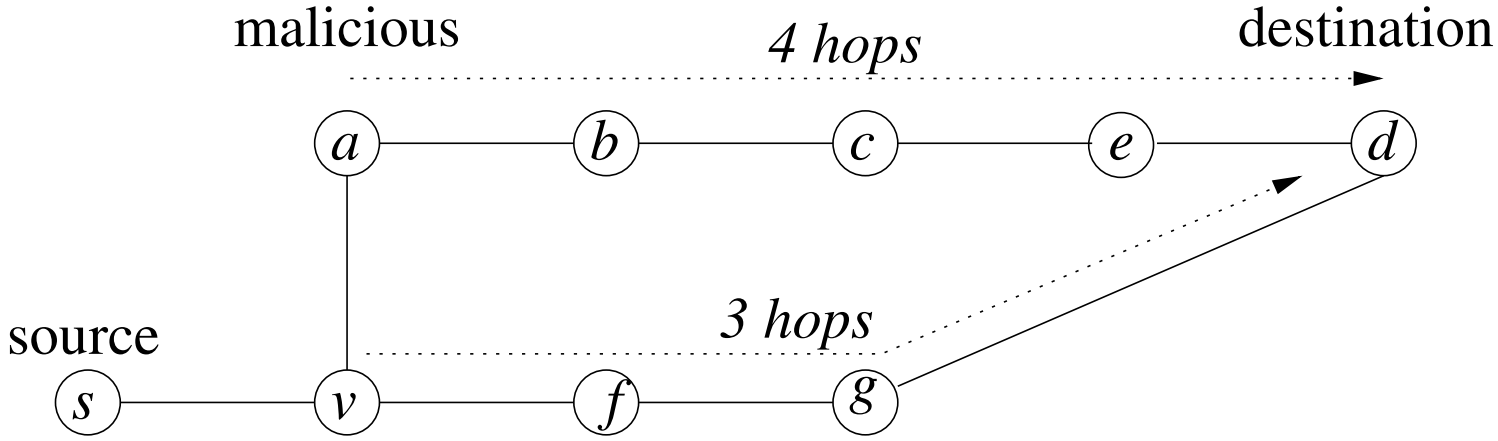
Preventing the Worawannotai attack



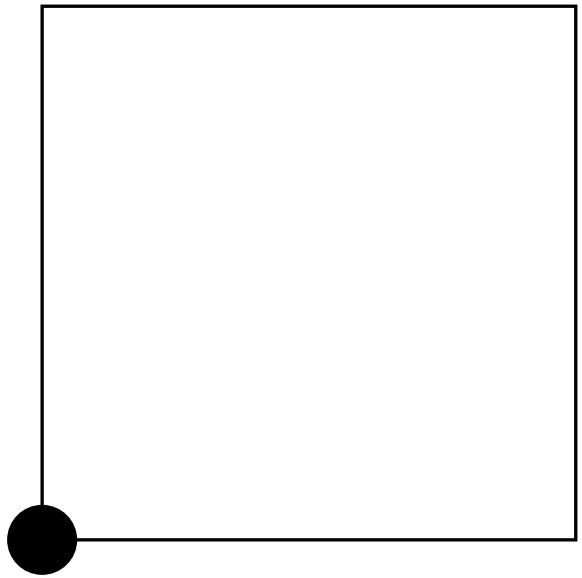
Verifier region

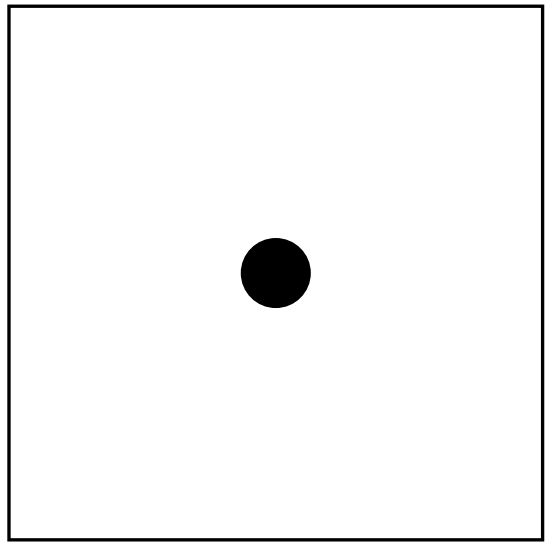


Sequence number attacks

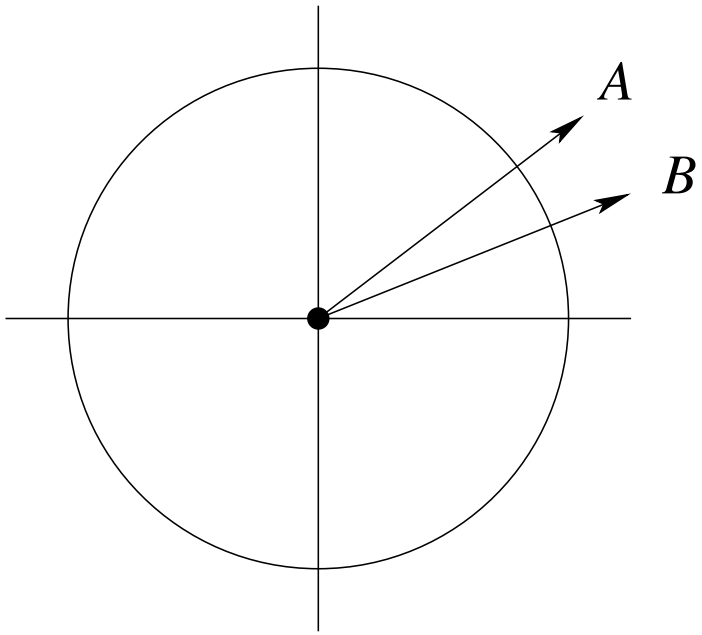


Impact of location of base stations on disrupting traffic in a sensor network delimited by a square region

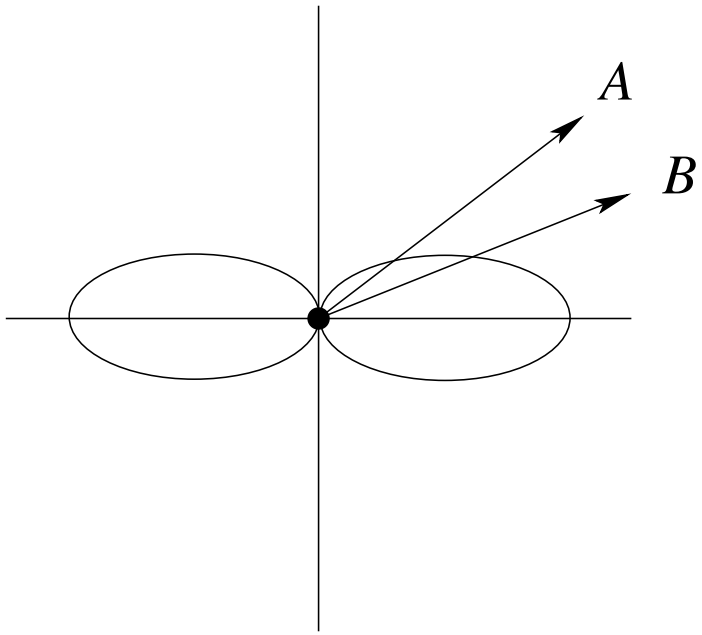




Omnidirectional and directional antennas



Omnidirectional



Directional