MANET Security: Background and Distributed Defense

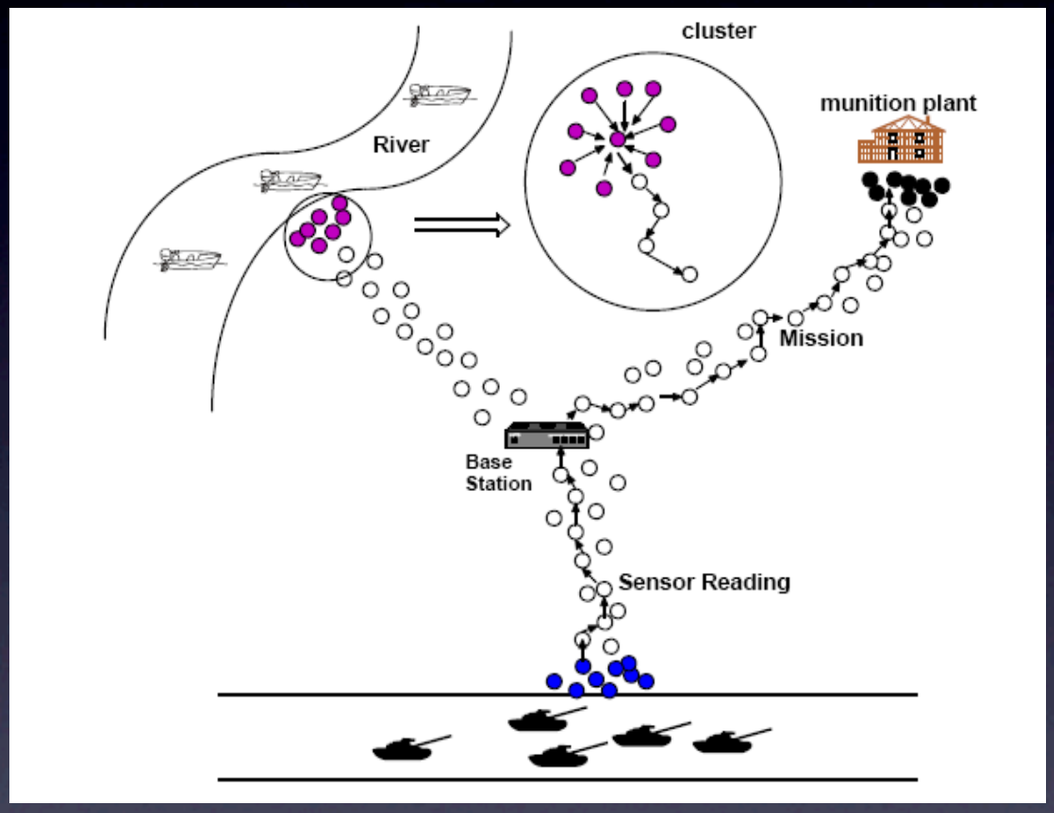
Angelos D. Keromytis
Network Security Lab
Department of Computer Science

MANETs

- Mobile Ad hoc NETworks
  - Mobile nodes communicate using wireless links
  - Nodes can join or leave the network any time
  - Limited resources: Energy and computing

MANETs vs. Sensor Nets

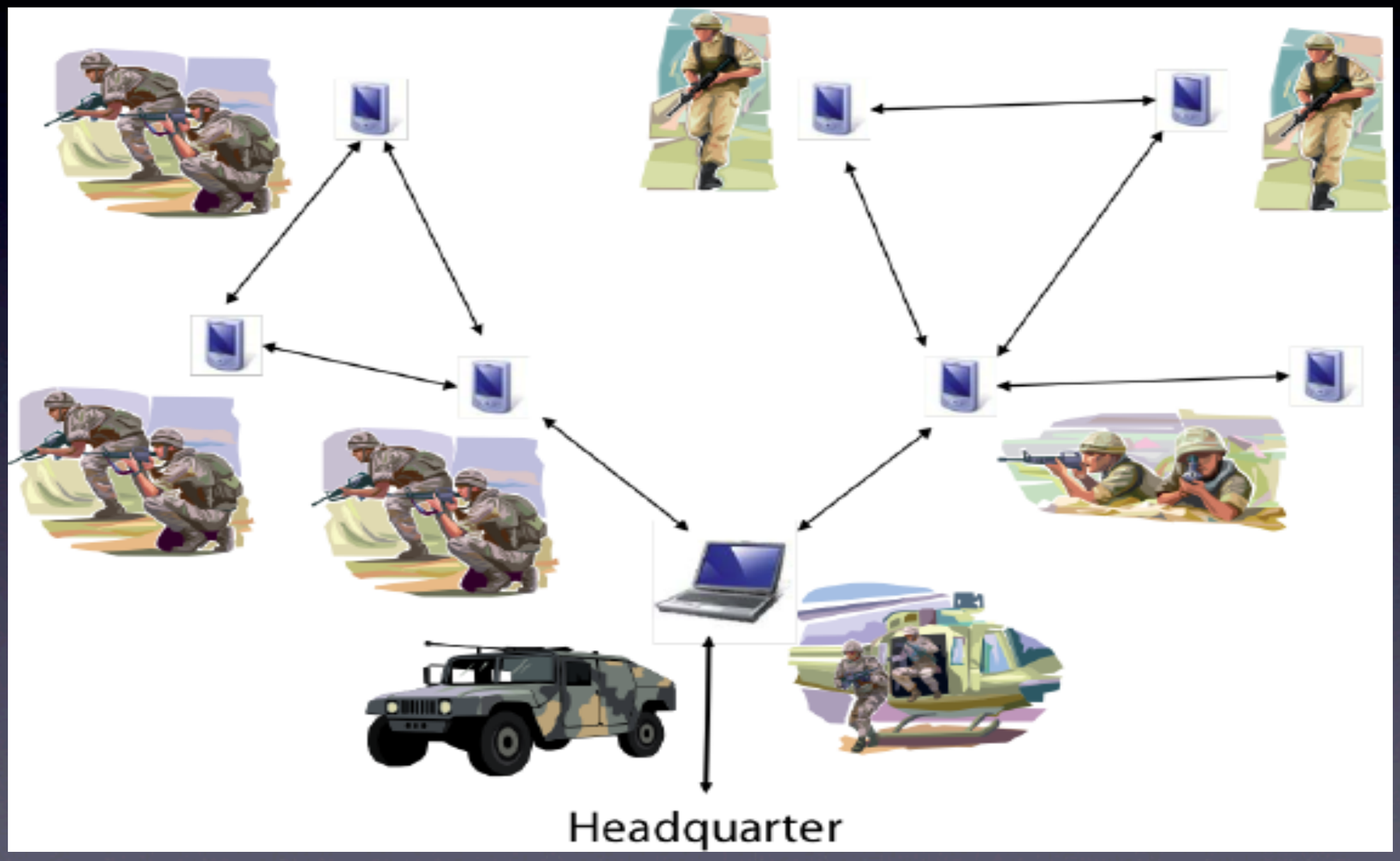
- Base station central point of trust
- Data aggregation
- Limited computing, memory and energy
- Large scale, redundancy



Uses of MANETs

- Where infrastructure cannot be deployed, must be deployed rapidly, or is at risk
  - military/tactical networks
  - disaster response
  - certain rural environments

MANETs



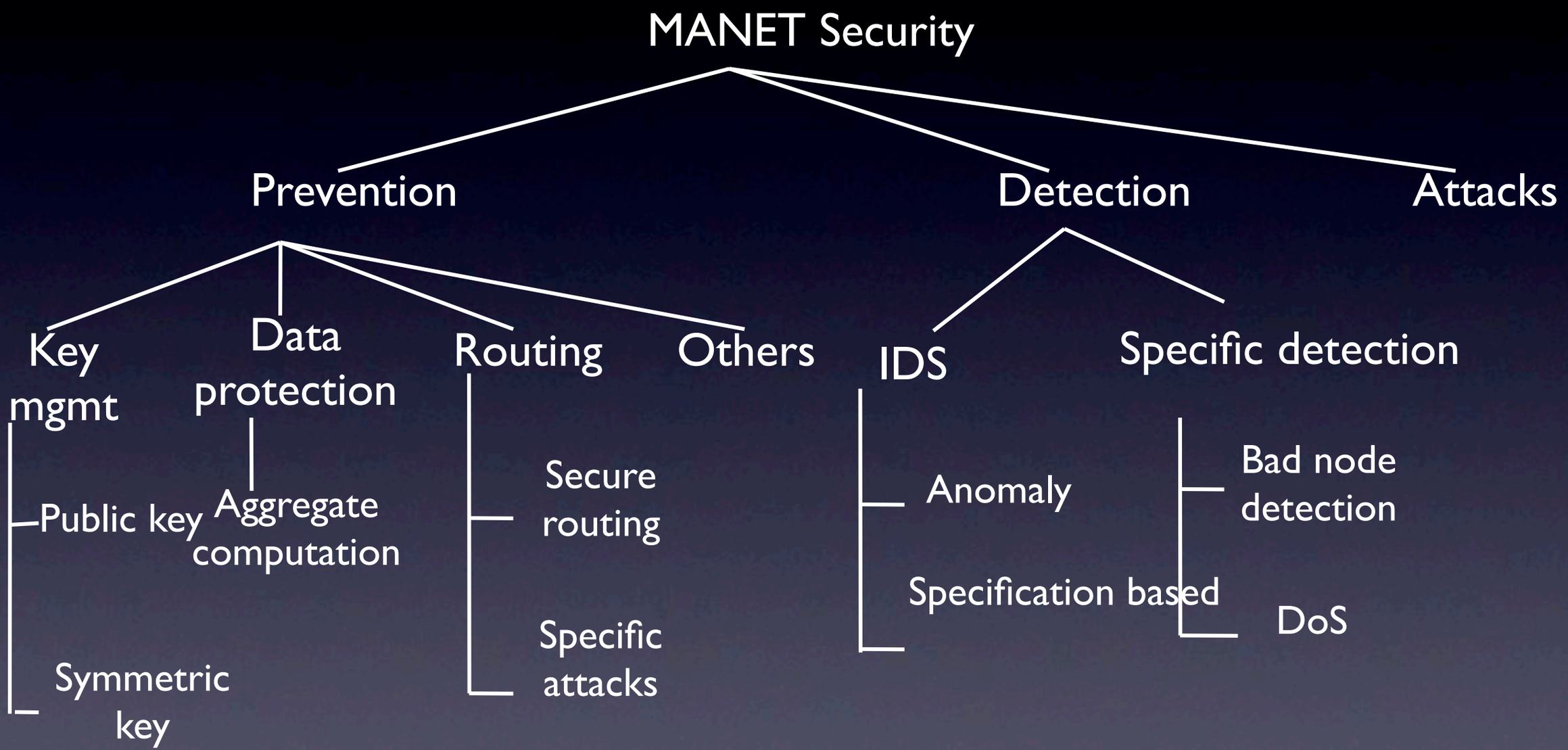
Security in MANETs

- Lack of clear line of defense
  - Mobile nodes function as routers
  - Wireless channel accessible to both legitimate nodes and attackers
  - Many MANET protocols assume trusted and co-operative environment
    - Routing: AODV, DSR
    - MAC: 802.11
- Compromises and physical capture
- Resource constraints
- Node mobility

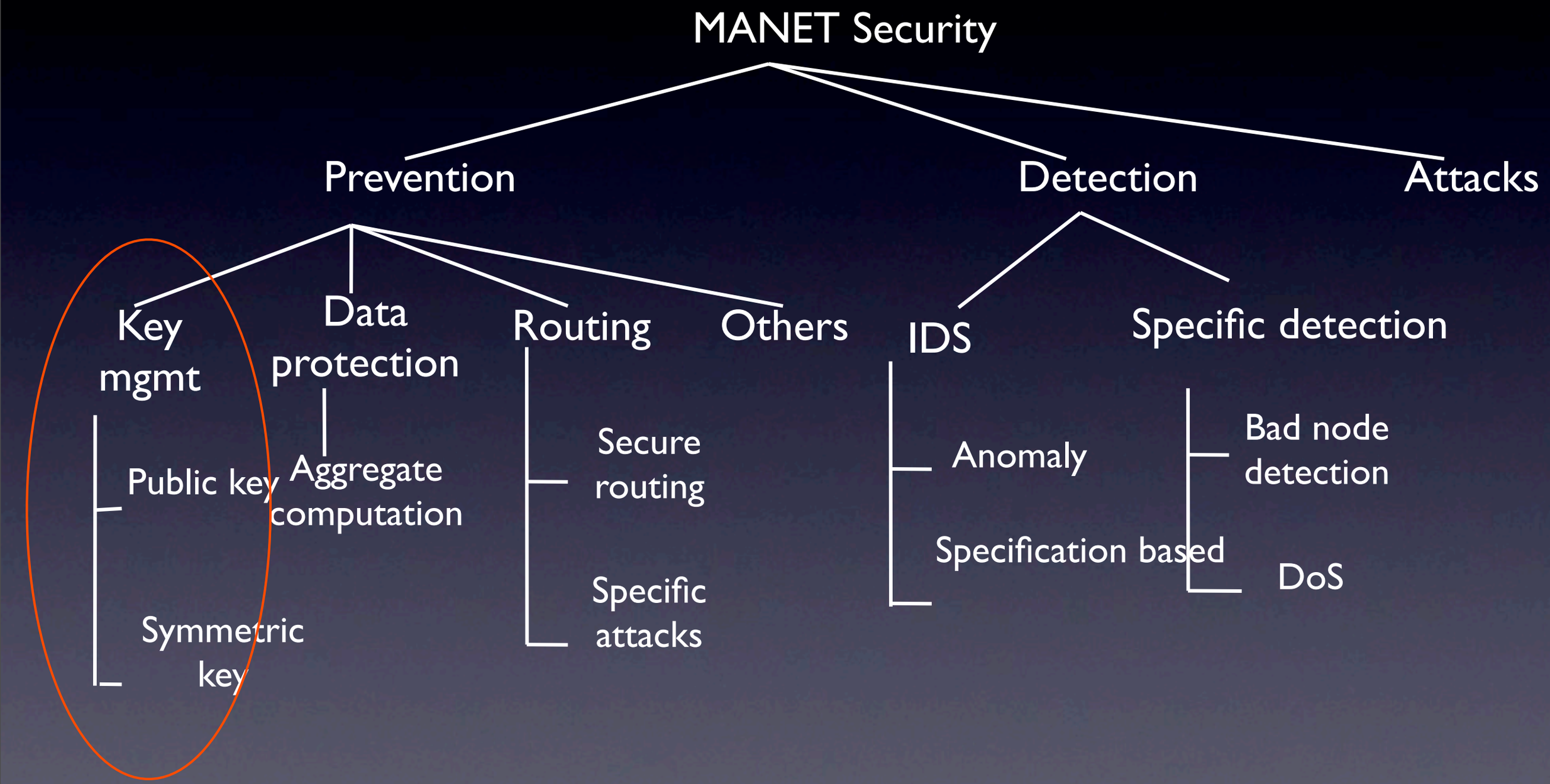
Security in MANETs

- Routing attacks
  - misbehaving nodes may attract traffic to see, modify or drop it
- Denial of service attacks
  - radio interference
  - network congestion
  - packet dropping
- All other network attacks apply

Securing MANETs



Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Public key
Symmetric key
Data protection
Aggregate computation
Routing
Secure routing
Specific attacks
Others
IDS
Anomaly
Specification based
Specific detection
Bad node detection
DoS

Key management

- Many attacks prevented using cryptographic means
- Require scalable key management solution
  - Public key
    - Problem: Availability of CA
  - Symmetric keys
    - Requirement for sensor networks

Public key distribution

- Problem: Availability of CA
- Solutions
  - Threshold cryptography [Zhou, Haas, Network 1999]
    - Divides the private key into n shares (s1,s2,…,sn)
    - (t+1) parties can perform operation, t parties cannot; n ≥ 3t+1
  - Distributed [Hubaux, Buttyan, Capkun, MobiHOC, 2001]
    - Users issue their own certificates; trusts limited number of other certificates
    - When two users want to communicate, merge the certificate repositories and find a certificate chain

Key management in sensor networks

- Challenges
  - Public key system impractical
  - Vulnerability of physical capture
  - Lack of a-priory knowledge of deployment configuration
  - Limited resources

- Key types [Zhu, Setia, Jajodia, CCS 2003]
  - Individual key shared with base station
  - pairwise key shared with another sensor node
  - cluster key shared with multiple neighboring nodes
  - group key shared by all the nodes

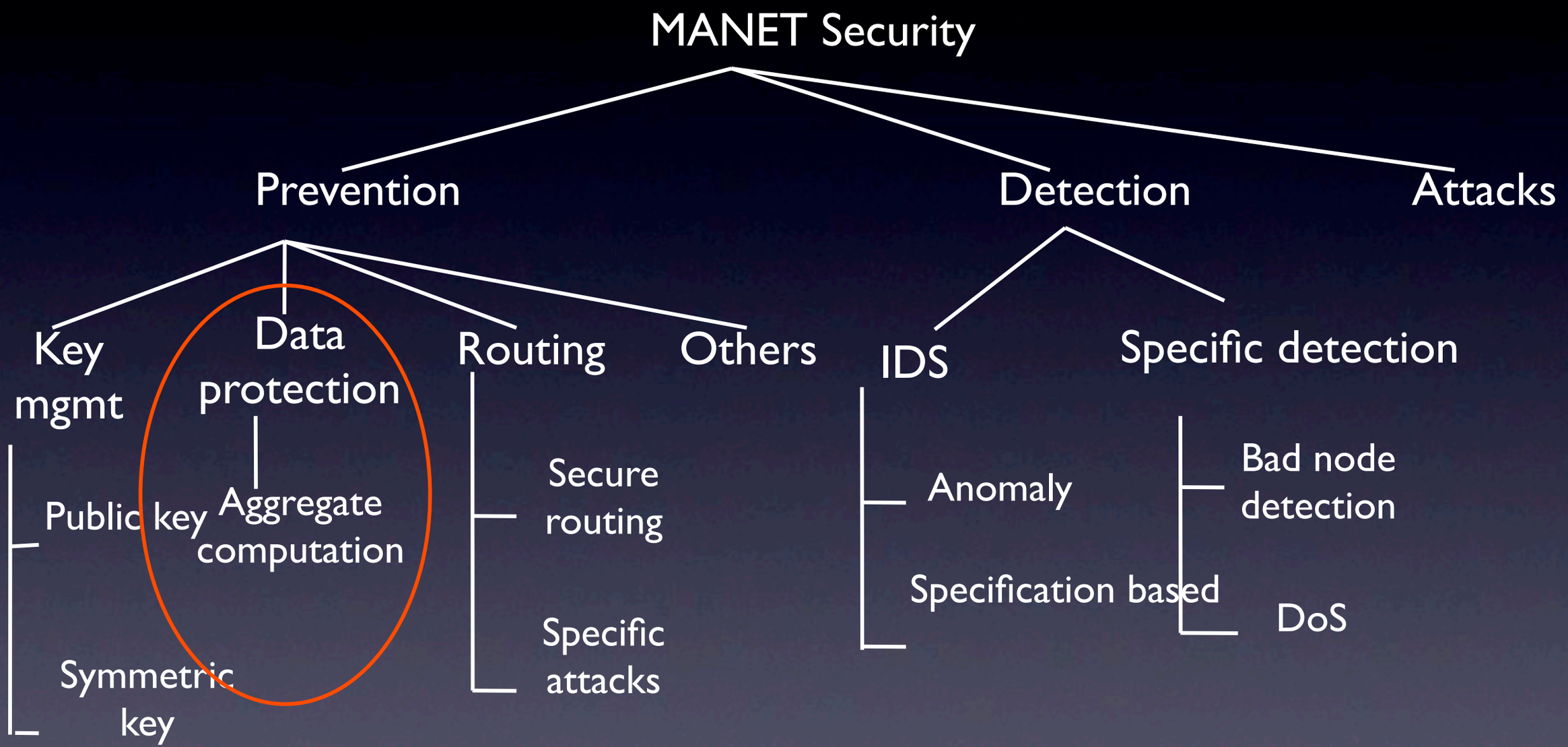
Key pre-distribution

- Problem: Not enough space to store pairwise keys for all possible neighbors
- Solution
  - Pre-distribute random subset of keys [Eschenauer, Gligor, CCS 2002]
  - Pairwise key between the nodes if they share any of those keys
  - Multi-path key establishment for neighbors not sharing keys
  - Q-composite random key pre-distribution [Chan, Perrig, Song, S&P 2003]
    - Require q common keys from the key ring for a pair of nodes
  - Polynomial pool-based key pre-distribution [Liu, Ning, CCS 2003]
    - Uses pool of randomly generated bivariate polynomials
    - Each node gets a subset of key share

Key pre-distribution scheme (cont.)

- Blom's key pre-distribution scheme
  - G:[λ+1,N] matrix, D:[λ+1,λ+1], $A=(D.G)^T$
  - k^{th} row of A and k^{th} column of G stored in node k
  - K = A.G, key matrix; λ- secure
- Multiple-space key pre-distribution scheme [Du, Deng, Han, Varshney CCS 2003]
  - Generate w key space (D1,G), (D2,G)…(Dw,G)
  - A node gets T subset
  - Better resilient than previous schemes
- Integrity (I)-codes based on physical layer [Cagalj et. al., S&P 2006]
  - Assumption: Cannot change 1 to 0 by the attacker
  - Can detect 0 to 1 change by coding

Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Data protection
Routing
Others
IDS
Specific detection
Public key
Symmetric key
Aggregate computation
Secure routing
Specific attacks
Anomaly
Specification based
Bad node detection
DoS

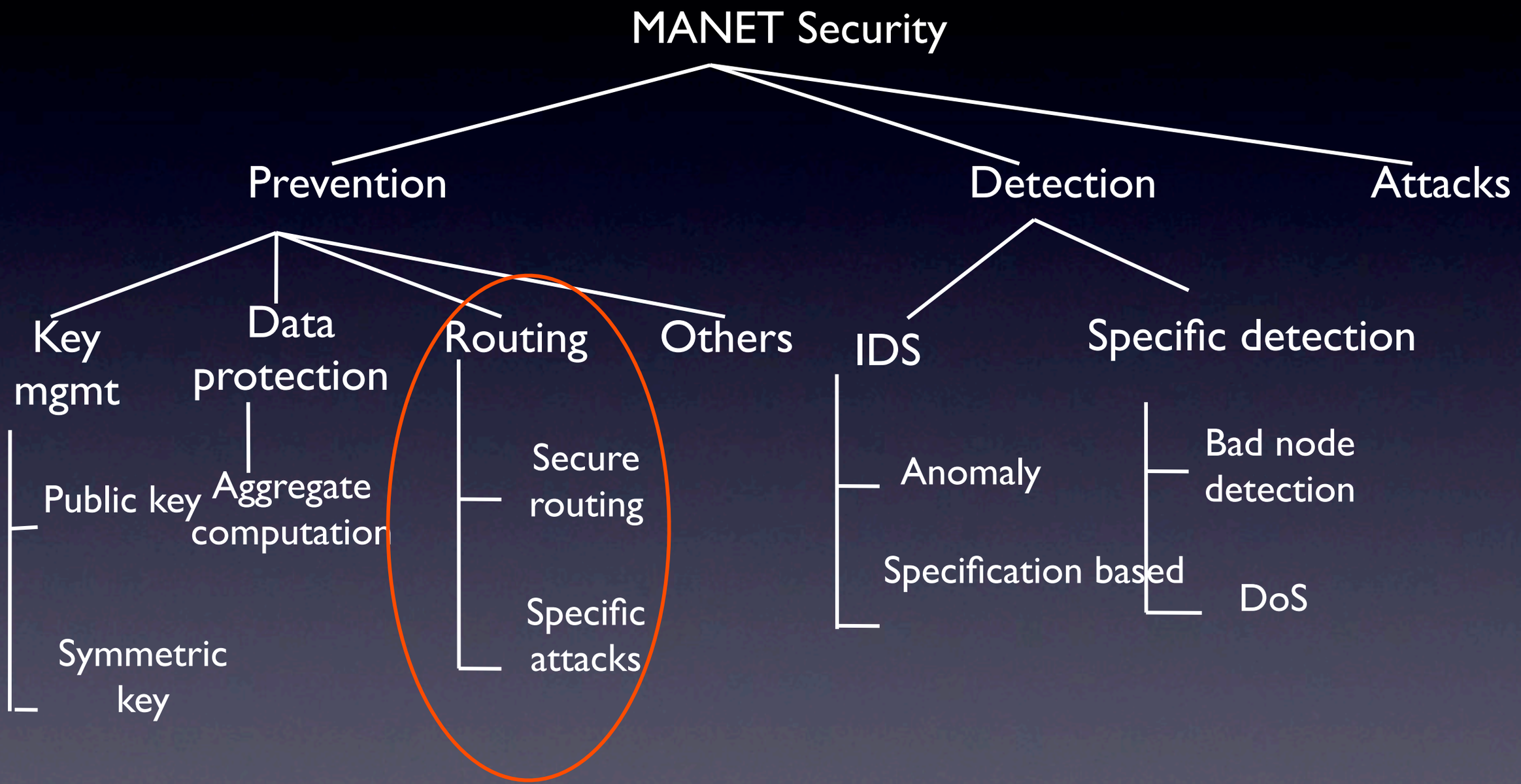
Securing Data

- μTESLA: Authenticated broadcast [Perrig, Szewczyk, Wen, Culler, Tygar, Mobicom 2001]
  - Delayed disclosure of symmetric keys
  - Requires loose time synchronization and authenticated key-chain commitment
  - Each key is a key in hash chain
- Time synchronization [Sun, Ning, Wang, Liu, Zhou, CCS 2006]
  - Pairwise time synchronization
    - Shared nature of wireless medium calls for recording the time only when the packet is guaranteed to leave
    - MAC computation at line rate
  - Global time synchronization
    - Based on pairwise synchronization
    - Need to be resiliant against compromised nodes
    - Authenticated local broadcast using μTESLA

Securing Data (cont.)

- Problem: Compromised sensor nodes may introduce false data
- Solution
  - Hierarchical aggregate computation [Chan, Perrig, Song CCS 2006]
    - Aggregation commit phase: Each node commits to the results obtained from its children
    - Result checking phase: Each node can verify that their result was taken by the parent
  - False data injection [Zhu, Setia, Jajodia, Ning, S&P 2004]
    - Compromised node can inject false data; detect upto t compromised nodes
    - At least t+1 nodes need to agree on a reading

Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Public key
Symmetric key
Data protection
Aggregate computation
Routing
Secure routing
Specific attacks
Others
IDS
Anomaly
Specification based
Specific detection
Bad node detection
DoS

MANET routing protocols

[Milanovic, Malek, Davidson, Milutinovic, Computer 2004]

- On-demand routing algorithms
  - Dynamic source routing (DSR)
  - Ad hoc on demand distance vector routing (AODV)
- Link state algorithms
  - Optimized link-state routing (OLSR)
  - Topology broadcast based on reverse-path forwarding (TBRPF)
- Hybrid approach
  - Discovers route only when needed, but use multipoint relays
  - Master, gateway and plain nodes

Routing Attacks

- Forge initiated routing packets
  - Cannot be detected using cryptographic techniques
  - IDS (e.g., DMEM) can detect it
- Forge forwarded routing packets and node identity
  - Cryptographic techniques can detect it
- Drop forwarded packets
  - Can be detected by sender based on acknowledgements
  - Reputation-based mechanisms

Routing Attacks (cont.)

- Rushing attacks
  - The attacker forwards the ROUTE REQUEST more quickly than legitimate nodes
    - The route is discovered through the attacker
- Worm hole
- Black hole
- Ad Hoc Flooding Attack (AHFA)
  - Attacker broadcasts mass route request packets

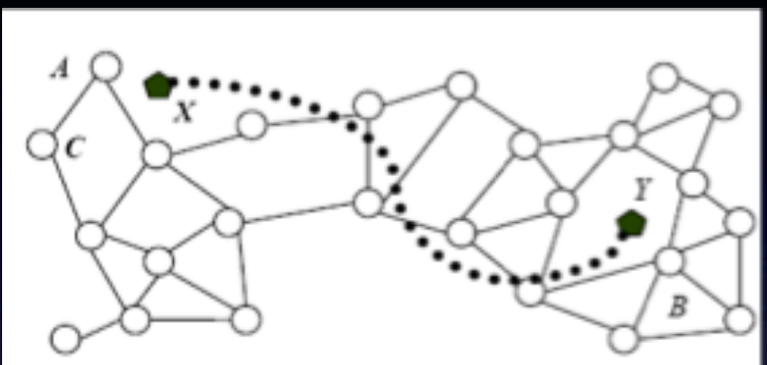


Figure 1. Wormhole attack. The adversary controls nodes *X* and *Y* and connects them through a low-latency link.

- JellyFish [Aad, Hubaux, Knightly, MOBICOM 2004]
  - Targeted against closed-loop flows such as TCP
  - Conforms to all routing and forwarding specifications
  - Reorder attacks
    - Delivers all the packets, but after placing them in reorder buffer
  - Periodic dropping attacks
    - Drop all packets for a short duration once per RTO
  - Delay variance attacks

Routing Security

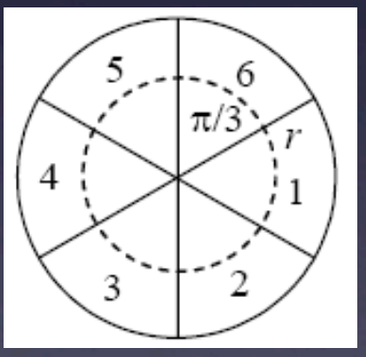
- Ariadne [Hu, Perrig, Johnson, MOBICOM 2002]
  - Based on DSR (dynamic source routing)
  - Uses TESLA, digital signature or pairwise keys for authentication
  - Route discovery
    - Target authenticates Route Requests using MAC
    - Initiator node verifies the reply using MAC
  - Route maintenance
    - Route error messages are authenticated

Preventing Routing Attacks

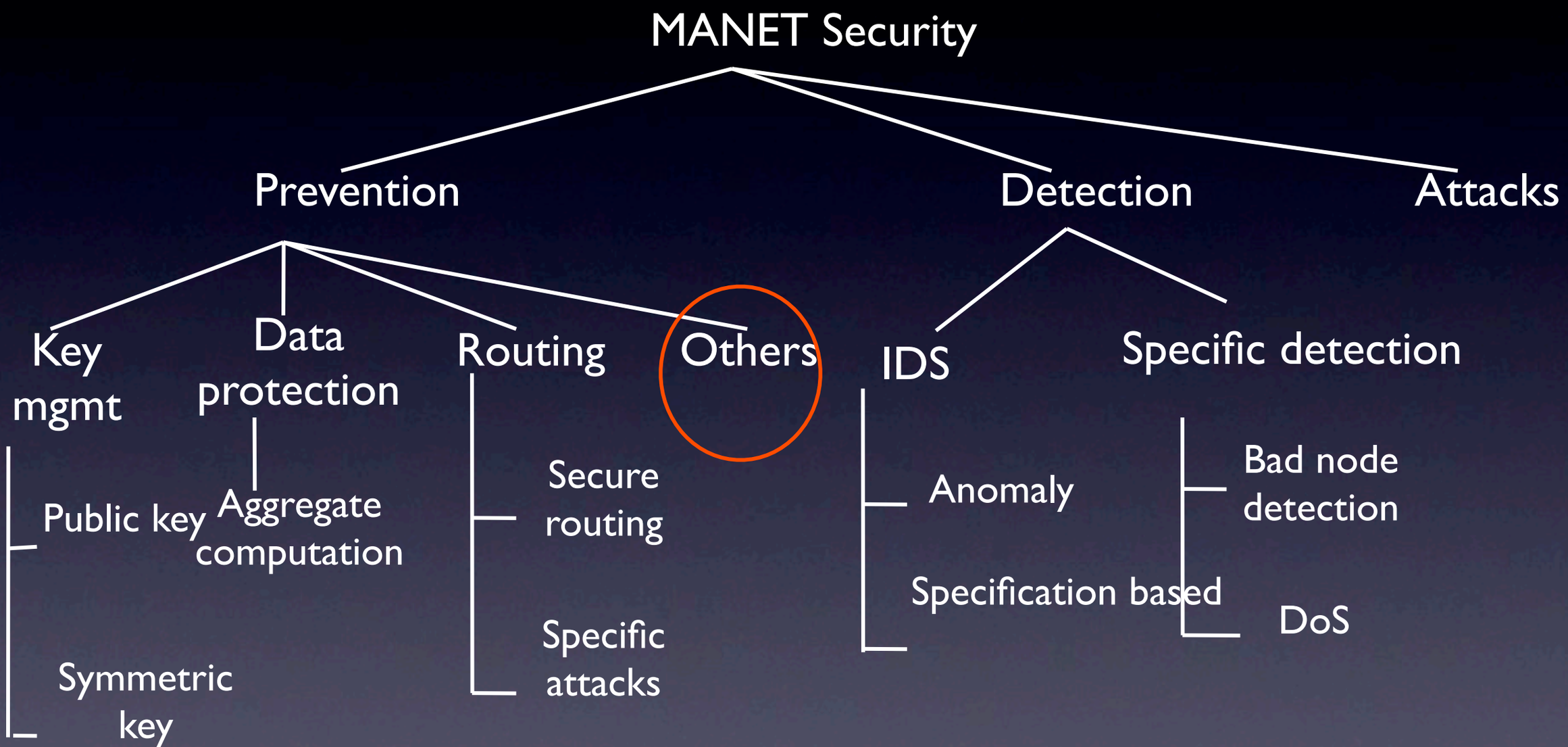
- Rushing attacks prevention [Hu, Perig, Johnson, WiSe, 2003]
  - Secure neighbor detection
  - Each node collects a number of REQUESTs and forwards one
- Flooding Attack Prevention (FAP) [Yi, Dai, Zhang, Zhong, Int. J. of Info. Technology, 2005]
  - Neighbors of attacker records the rate of route request
  - Denies the requests after threshold is reached
  - Easy to break the scheme, if the attacker pretends the request is a forwarded request!

Preventing Routing Attacks (cont.)

- Wormhole attack prevention [Hu, Evans, NDSS 2003]
  - Directional antennas: Divides the region into 6 zones
  - Directional neighbor discovery
    - A hears B from the opposite zone of B hears A
    - Cannot detect wormhole if nodes are in opposite zones relative to worm hole end points
  - Verified neighbor discovery protocol
    - A verifier V can verify the link A←→ link
      - zone(B,A) != zone(B,V); zone(B,A) != zone(V,A)
  - Strict neighbor discovery
    - Above scheme fails if A & B are unable to communicate, but close enough to have a verifier that can communicate with both A & B
      - Zone(B,V) cannot be both adjacent to zone(B,A) and zone(V,A)



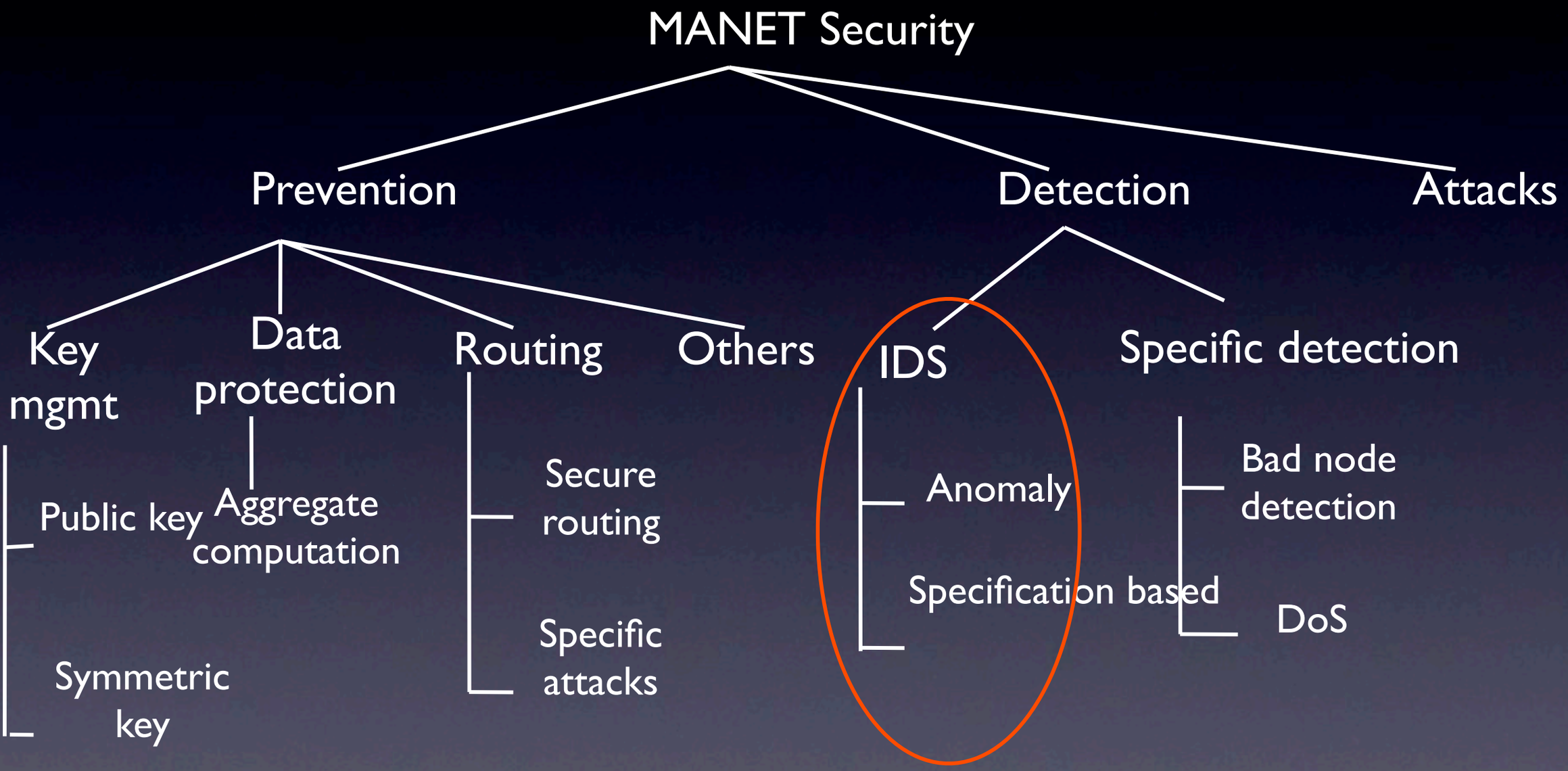
Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Data protection
Routing
Others
IDS
Specific detection
Public key
Symmetric key
Aggregate computation
Secure routing
Specific attacks
Anomaly
Specification based
Bad node detection
DoS

Transport for Mobility

- Network and transport layer solution for multi-homing and mobility [Nikander, Ylitalo, Wall, NDSS 2003]
  - IP address has dual role host identity and topological location
- Security problems with multi-homing and mobility
  - Address stealing
  - Address flooding
- Proposed solution
  - Host Identity Protocol (HIP): cryptographic namespace and protocol layer between network and transport layer
  - Packet forwarding agents: Forwards packets sent to a given IP address to another IP address

Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Public key
Symmetric key
Data protection
Aggregate computation
Routing
Secure routing
Specific attacks
Others
IDS
Anomaly
Specification based
Specific detection
Bad node detection
DoS

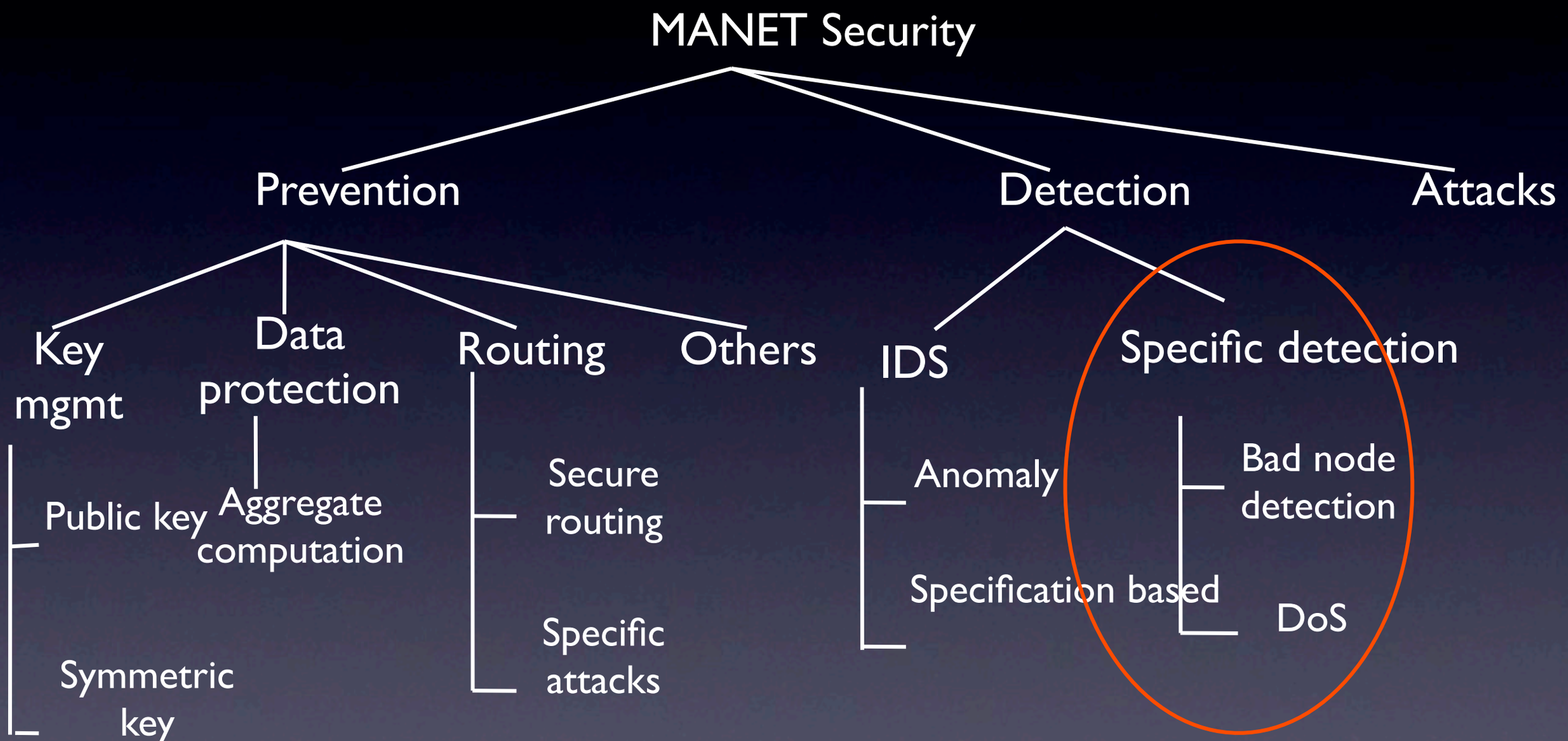
IDS Architecture

- IDS Requirement
  - Distributed, without centralized point
    - Needs practical and scalable approach to gather evidence from other nodes
  - Links are much more unreliable
  - Limited bandwidth and computing power
- Solutions
  - Local intrusion detection architecture (LIDS) [Albers et. al., WIS, 2002]
    - Different LIDS exchange security data and intrusion alerts
    - Audit data: SNMP MIBs
    - Use of mobile agents to do specific mission in autonomous and asynchronous manner
  - Distributed IDS Architecture [Zhang, Lee, Mobicom 2000]
    - Local detection engine: input from local data collection
    - Cooperative detection engine: input from neighboring nodes

Routing attack detection

- Routing Attack detection based on specification
  - Based on extended finite state automation (EFSA) of AODV [Huang, Lee, RAID 2004]
    - Detects invalid state, transition and action violation
  - DMEM for OLSR [Tseng, Wang, Ko, Levitt, RAID 2006]
    - Detection by validating the consistency among related routing messages
    - Example: Neighbors in Hello messages must be reciprocal
- Intrusion response [Wang, Tseng, Levitt, Bishop, RAID 2007]
  - Topology dependency index (TDI)
    - Number of nodes that cannot be reached without the attacker
  - Attack damage index (ADI)
    - Number of nodes to which the routing has changed after attacks
  - If TDI = 0 or ADI > 2 TDI → Isolate attacker
- Model the attacks on AODV protocol using attack tree [Ebinger, Bucher, LNCS, 2006]
  - Greatest damage from black hole or wormhole; Easy to perform rushing and Sybil

Taxonomy


MANET Security
Prevention
Detection
Attacks
Key mgmt
Public key
Symmetric key
Data protection
Aggregate computation
Routing
Secure routing
Specific attacks
Others
IDS
Anomaly
Specification based
Specific detection
Bad node detection
DoS

Compromised/Selfish node detection

- Tamper resistant hardware
- Node replication attacks [Parno, Perrig, Gligor, IEEE S&P 2005]
  - Replicas of a compromised node planted in the network
  - Neighbors forward the location claim of a node to randomly selected witnesses
  - High probability of collision (birthday paradox)
  - Lower overhead if the intermediate routers also acts as witnesses
- Reputation mechanism [Jaramillo, Srikant, Mobicom 2007]
  - Co-operation induced by threatening partial or total disconnection
  - DARWIN: Avoid retaliation after a node has falsely perceived as selfish; cooperation restored
    - Modeled after game theory
    - Player that has better standing should proportionately punish its opponents with the difference in the two standing instead of absolute standing of its opponent.
    - Collusion resistance

Other attack detection

- Secure implicit sampling (SIS) [McCune, Shi, Perrig, Reiter S&P 05]
  - Detection against denial of broadcast messages
  - Elicits authenticated acknowledgements from subset of nodes unpredictable to attacker
  - If number of ACKs received is less than a threshold of expected, there is attack
    - ACK not received either due to packet loss or due to attack

Related work: network capabilities

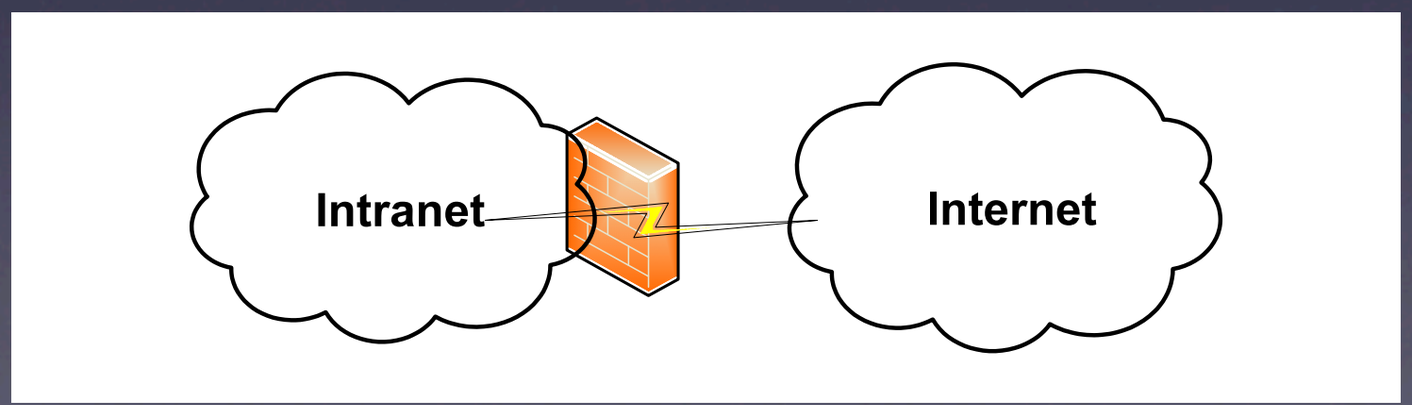
- Capability implemented in early computer systems (1984)
- "visas" for packets (1989)
- Network capabilities to prevent DoS in wired networks (2003)
  - Capability assigned by receivers
  - Links in the path between a sender and receiver cannot be snooped

What can we do?

- For open environments: tomorrow
- For closed (e.g., military) environments:
  - redesign network from scratch
  - Policy enforcement framework
  - Distributed Enforcement: all intermediate nodes enforce the capability policy

Securing MANETs

- Firewalls keep away malicious traffic from set of nodes
- Placed on the perimeter, enforcing policy
  - Nodes inside trusted; outside potential enemies
- MANETs have no well-defined perimeter



Distributed Firewalls

Distributed Firewalls

- Traditional Firewalls: broken assumptions
  - Inside trusted, outside untrusted
  - Machines require uniform external access

Distributed Firewalls

- Traditional Firewalls: broken assumptions
  - Inside trusted, outside untrusted
  - Machines require uniform external access
- Policy centrally defined; Enforcement at end hosts
- Distributed firewalls sufficient for MANETs?
  - No protection of network bandwidth
  - No limit on amount of service access
  - No protection of routing protocols

Distributed Enforcement

- Capability: access rules and bandwidth constraints represented using capabilities
- Deny-by-default: every packet in the network need to have an associated capability
- Unauthorized traffic dropped closer to the source
- Protects end-host resources and network bandwidth

DIPLOMA

- DIstributed PoLicy enfOrceMent Architecture for MANETs
  - Enforcement done at all nodes
  - Access and bandwidth control
    - Capability based access control
      - Useful for highly dynamic environments
        - Nodes participating not known in advance
        - Same IP may be assigned to multiple nodes
      - Rule update does not require populating to all the nodes
      - Prevents source address spoofing

DIPLOMA Components

- Policy language for access control and bandwidth access
- Rules and algorithms for deriving new policy
- Protocol for communication of policy
- Enforcement of policies

Capability

- Access control and bandwidth limitation represented using capability (KeyNote [BFIK99])
  - Identity of the principal
  - Identity of the destination
  - Type of service and bandwidth
  - Expiration date
  - Issuer & Signature
- Policy tokens
  - Issued by the administrator
- Network capability
  - Issued by the receiving node

Policy Token Example

serial: 130745
owner: unit01.nj.army.mil (public key)
destination: *.nj.army.mil
service: https
bandwidth: 50kbps
expiration: 2010-12-31 23:59:59
issuer: captain.nj.army.mil
signature: sig-rsa 23455656767543566678

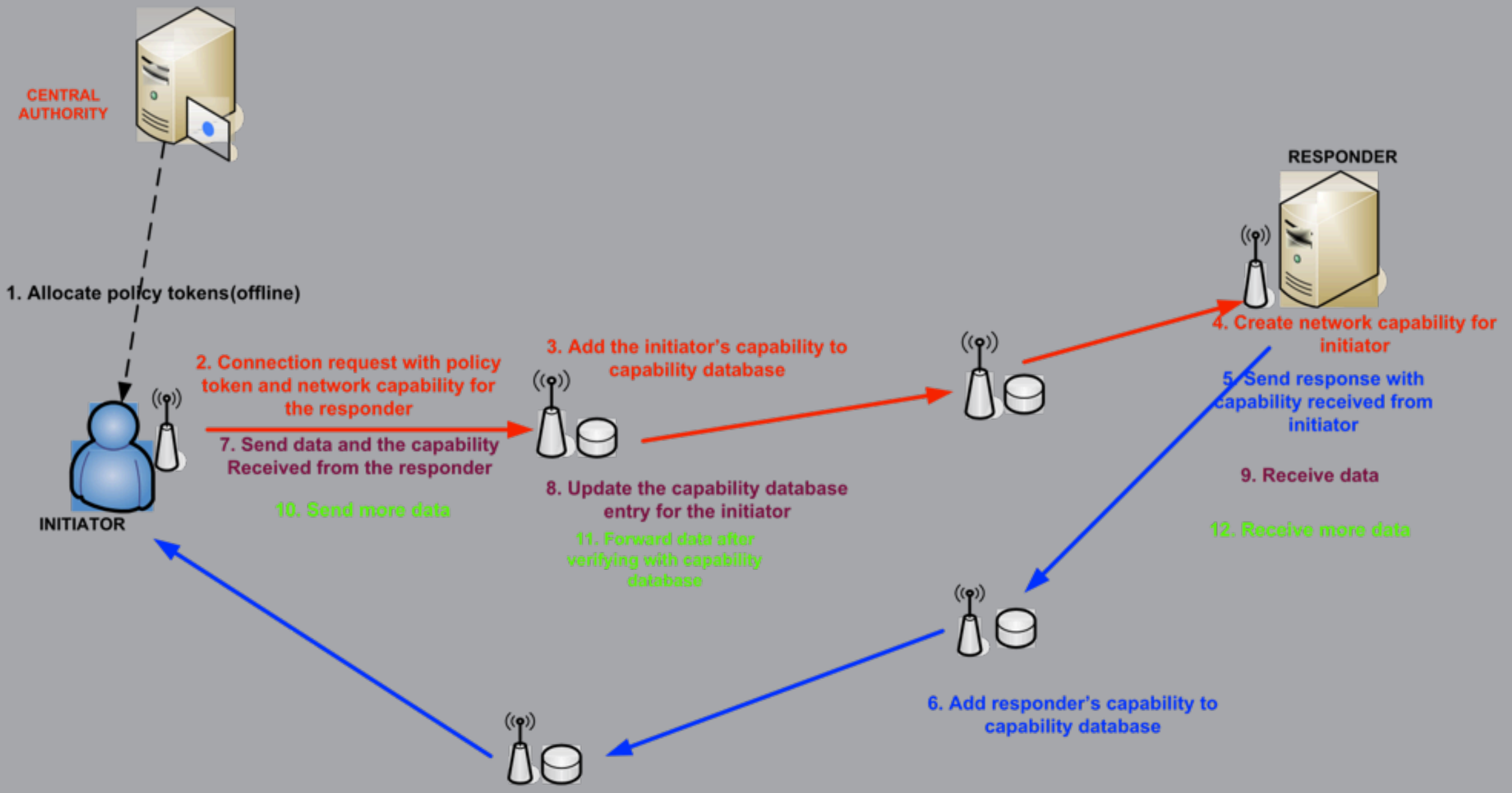
Network Capability Example

serial: 1567
owner: unit01.nj.army.mil (public key)
destination: unit02.nj.army.mil
bandwidth: 150kbps
expiration: 2009:10:21 13:05:35
issuer: unit02.nj.army.mil
comment: Policy allowing the receiver to issue this capability.
signature: sig-rsa 238769789789898

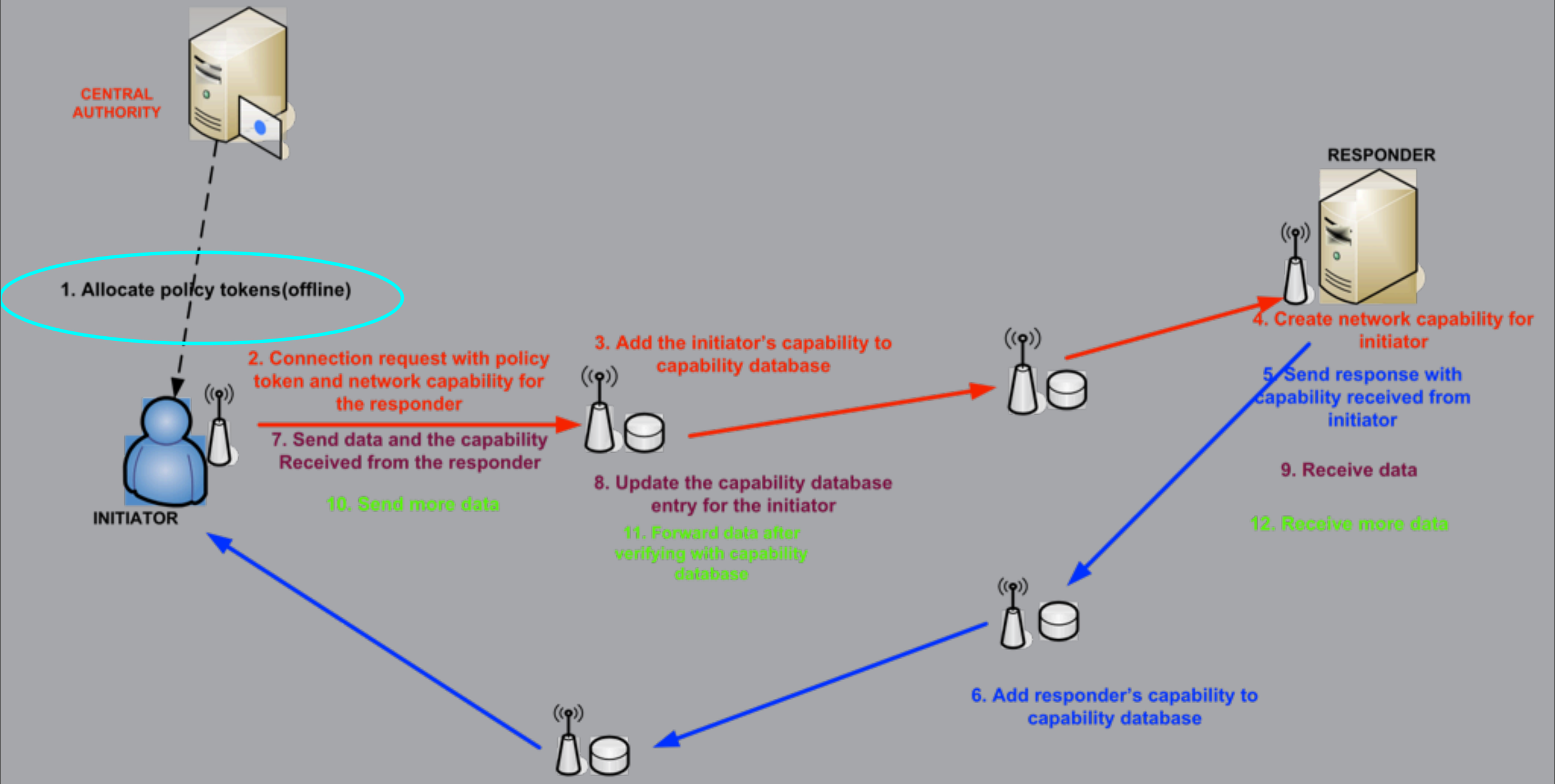
Protocol

- Capability associated with each communication session
  - Transaction identifier and signature
- Capability Establishment
  - Source node informs the intermediate nodes about transaction identifier, capability and key for signature
    - Smaller keys used for per packet signature
- Sender
  - Adds transaction id, sequence number and signature to the packet
- Intermediate nodes and Receiver
  - Verifies the packet (probabilistically) for signature and bandwidth

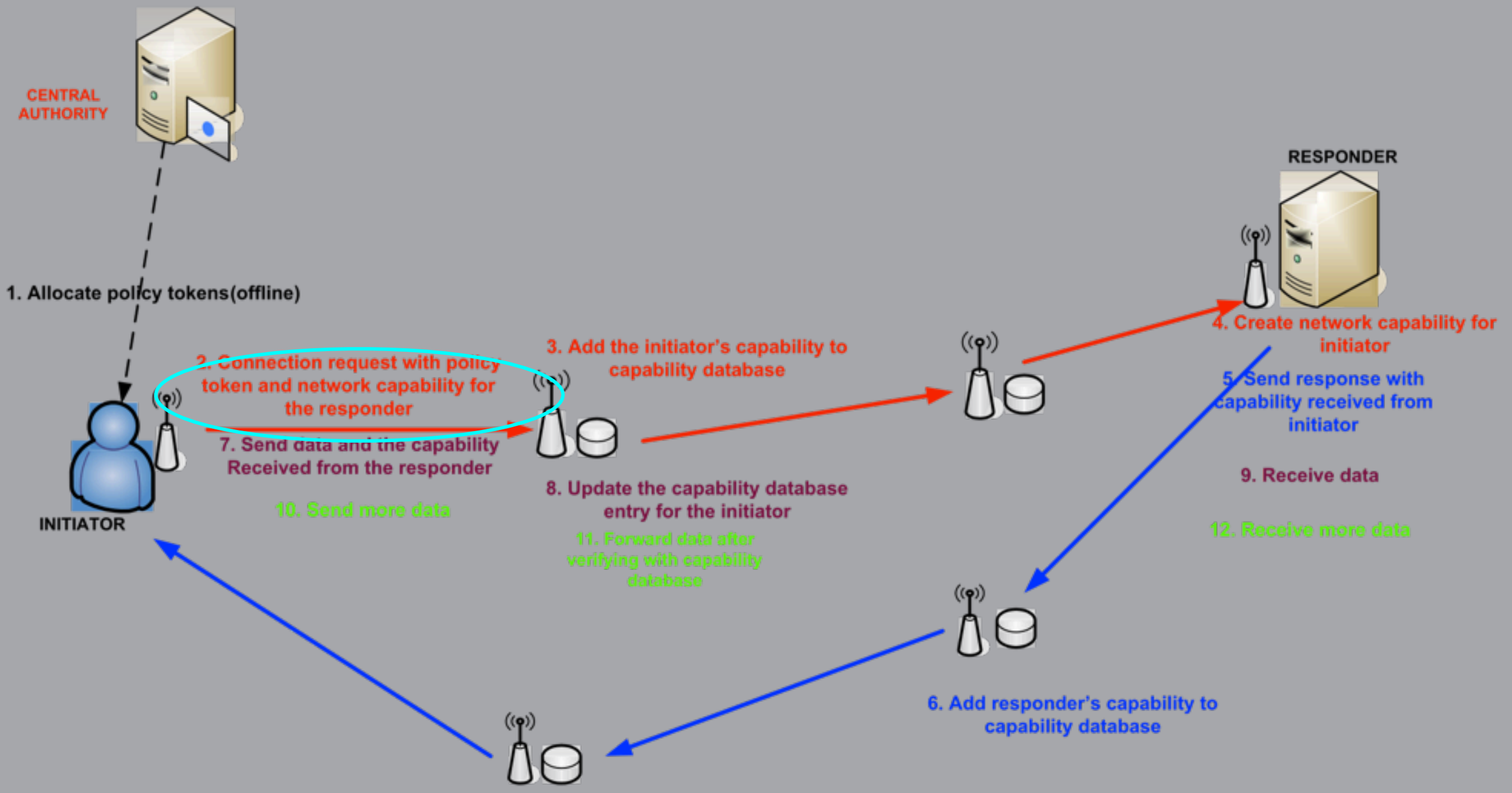
System Architecture



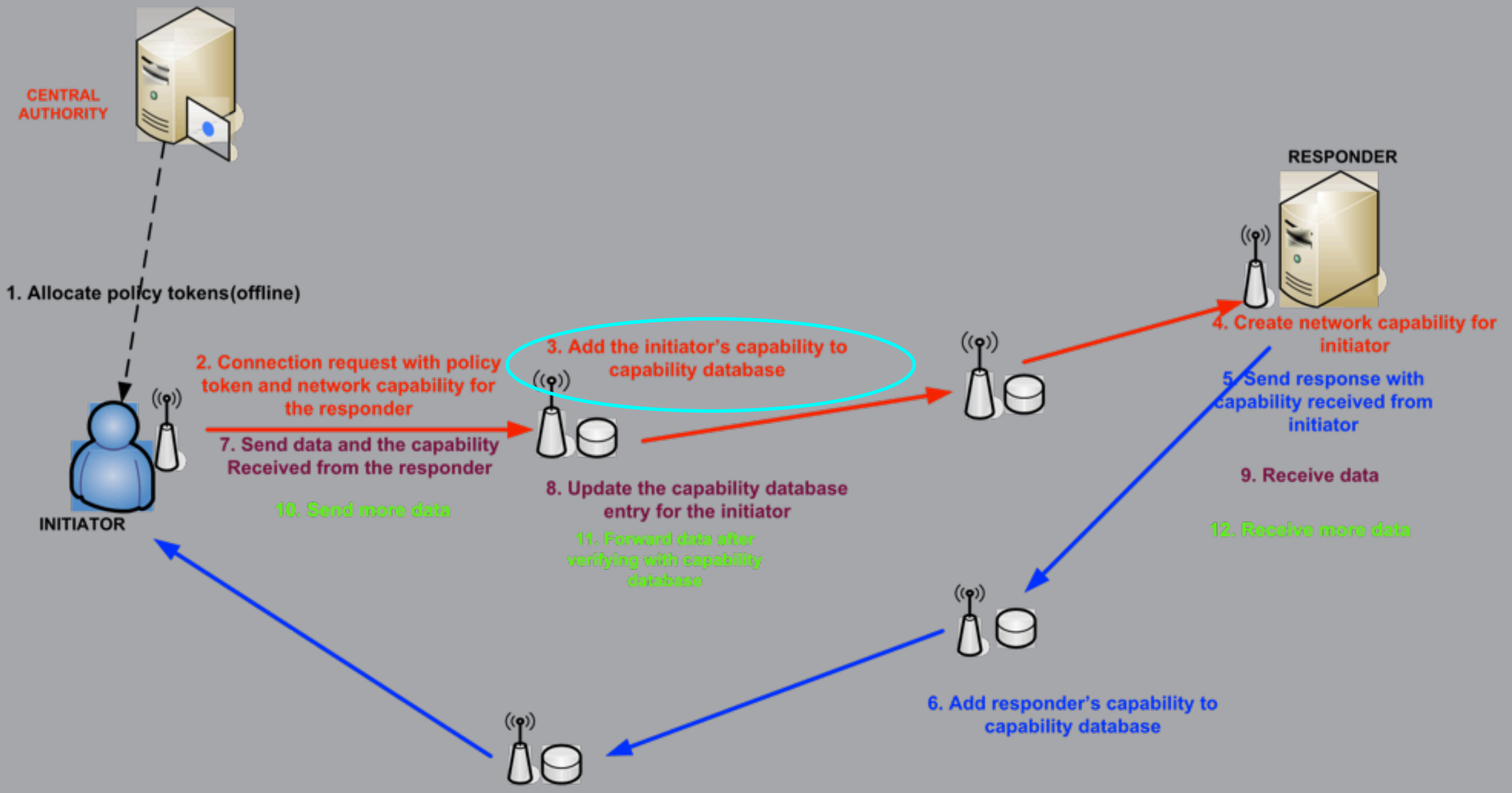
System Architecture



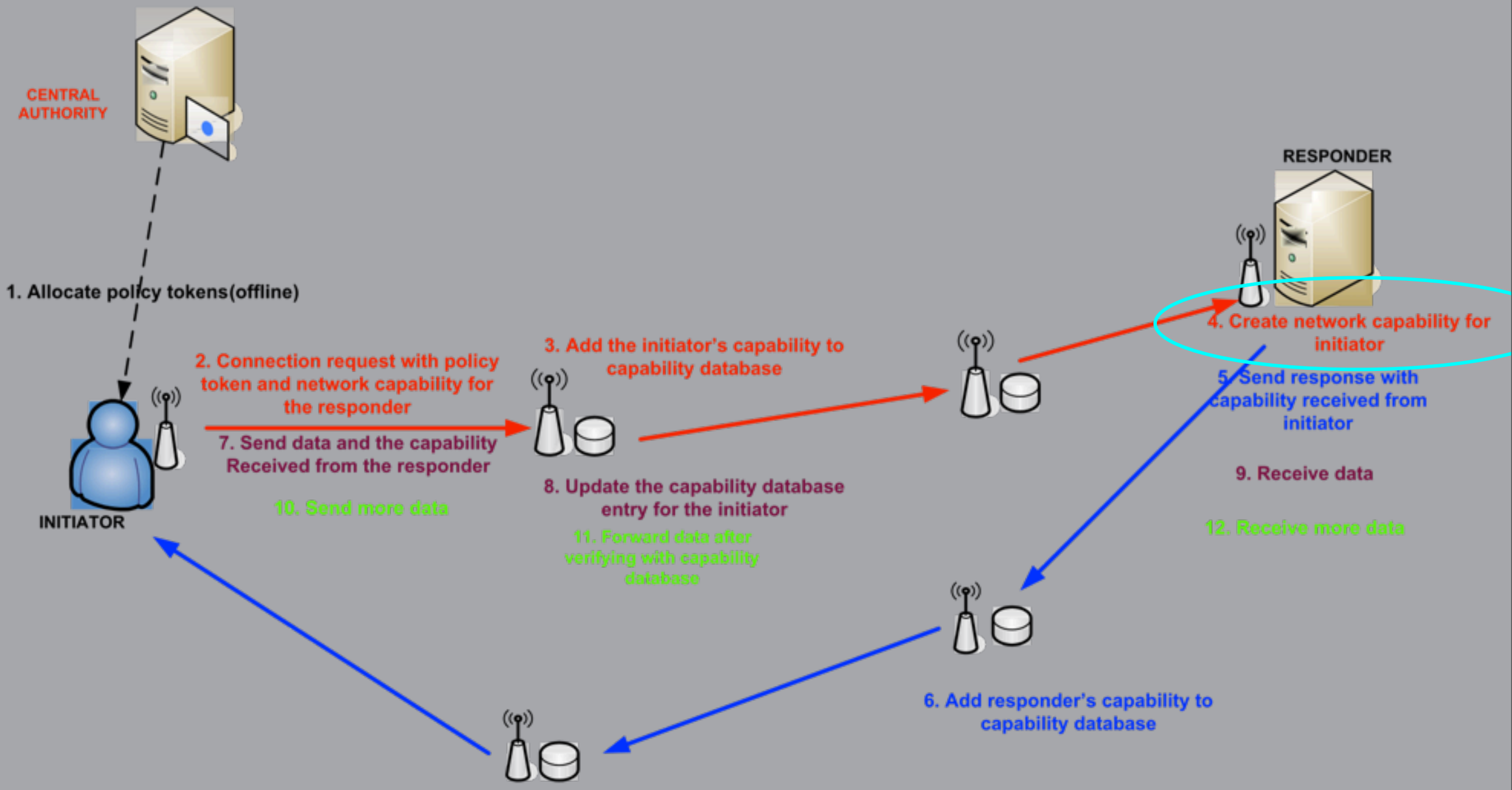
System Architecture



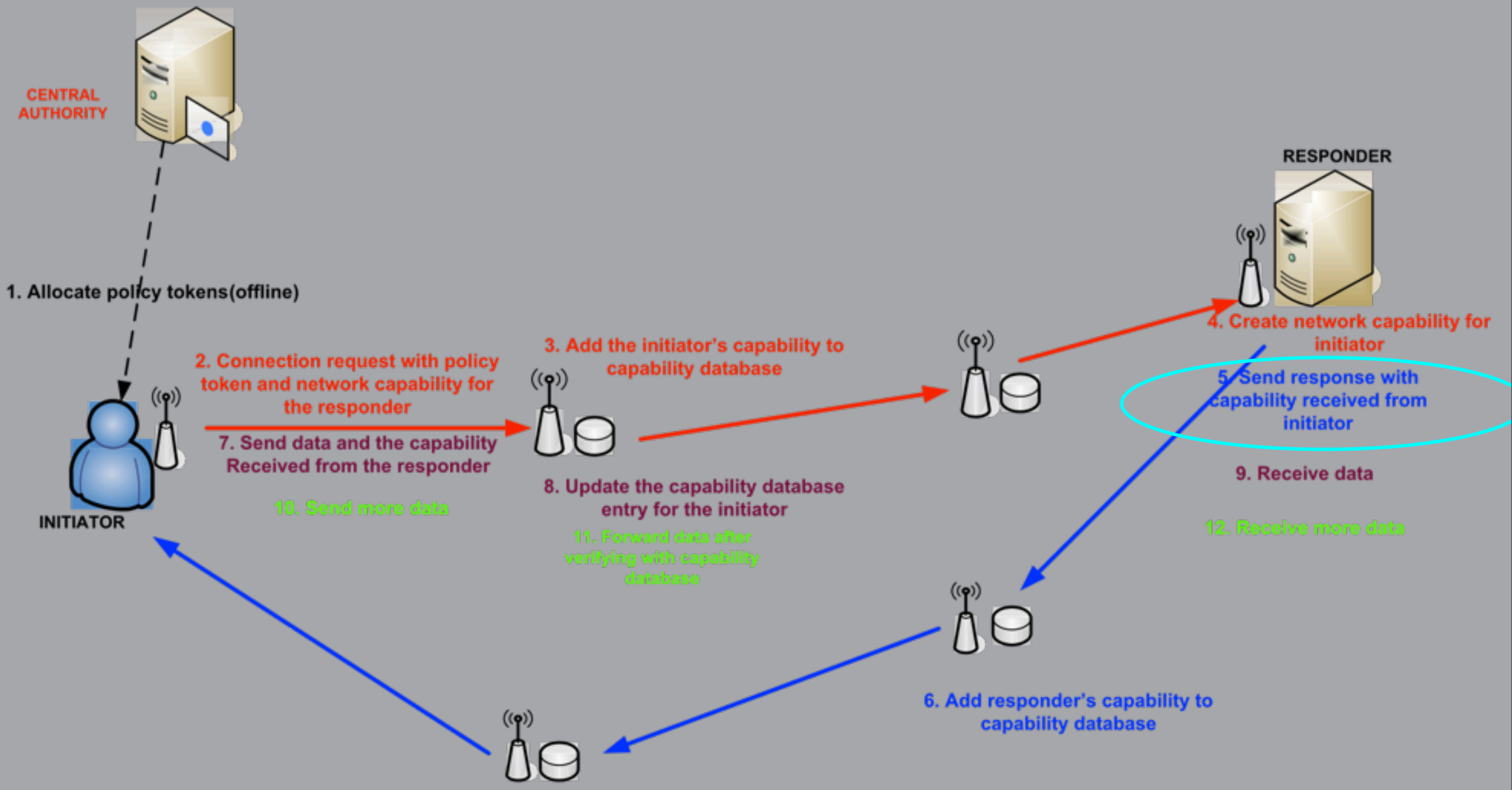
System Architecture



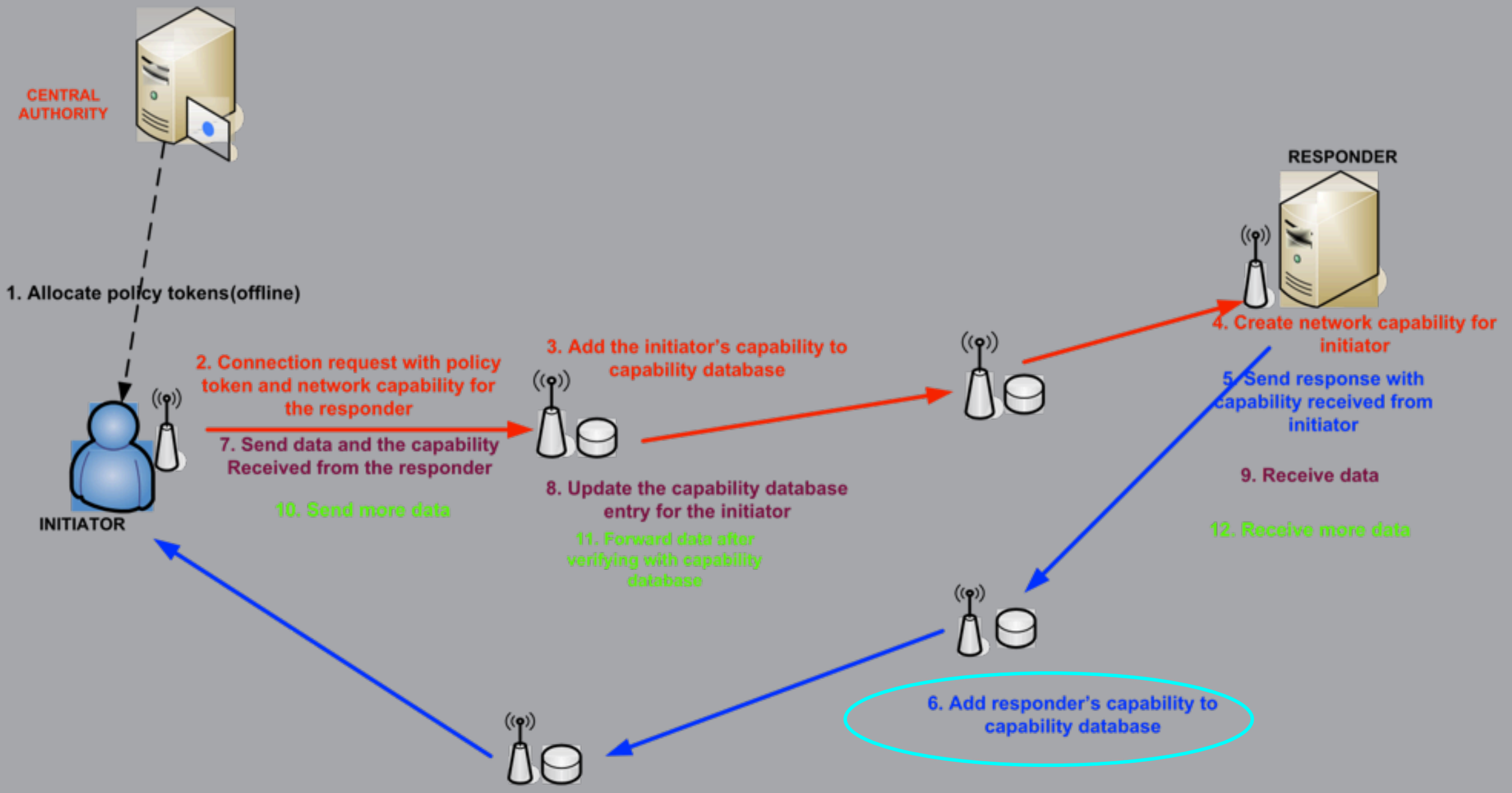
System Architecture



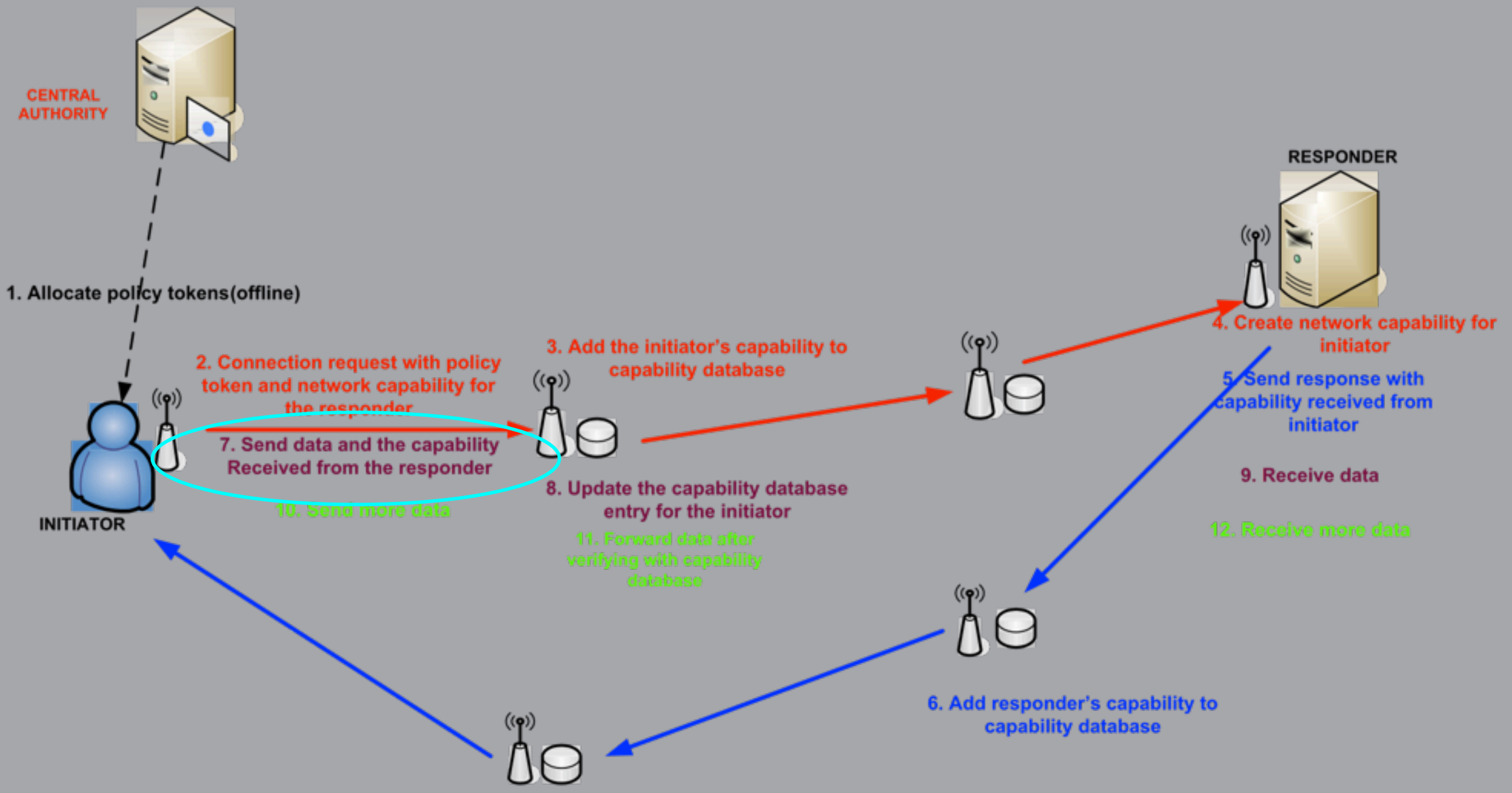
System Architecture



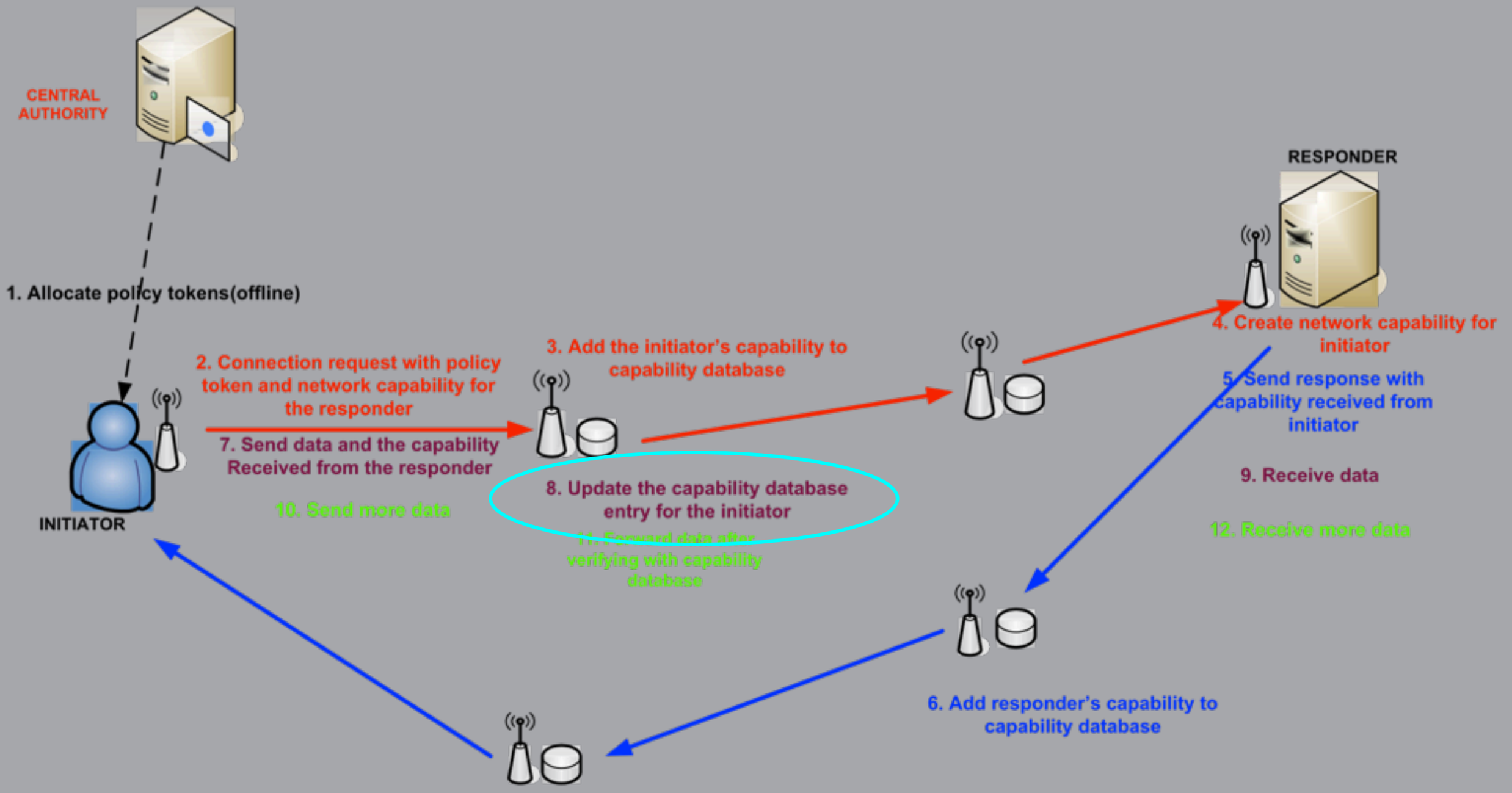
System Architecture



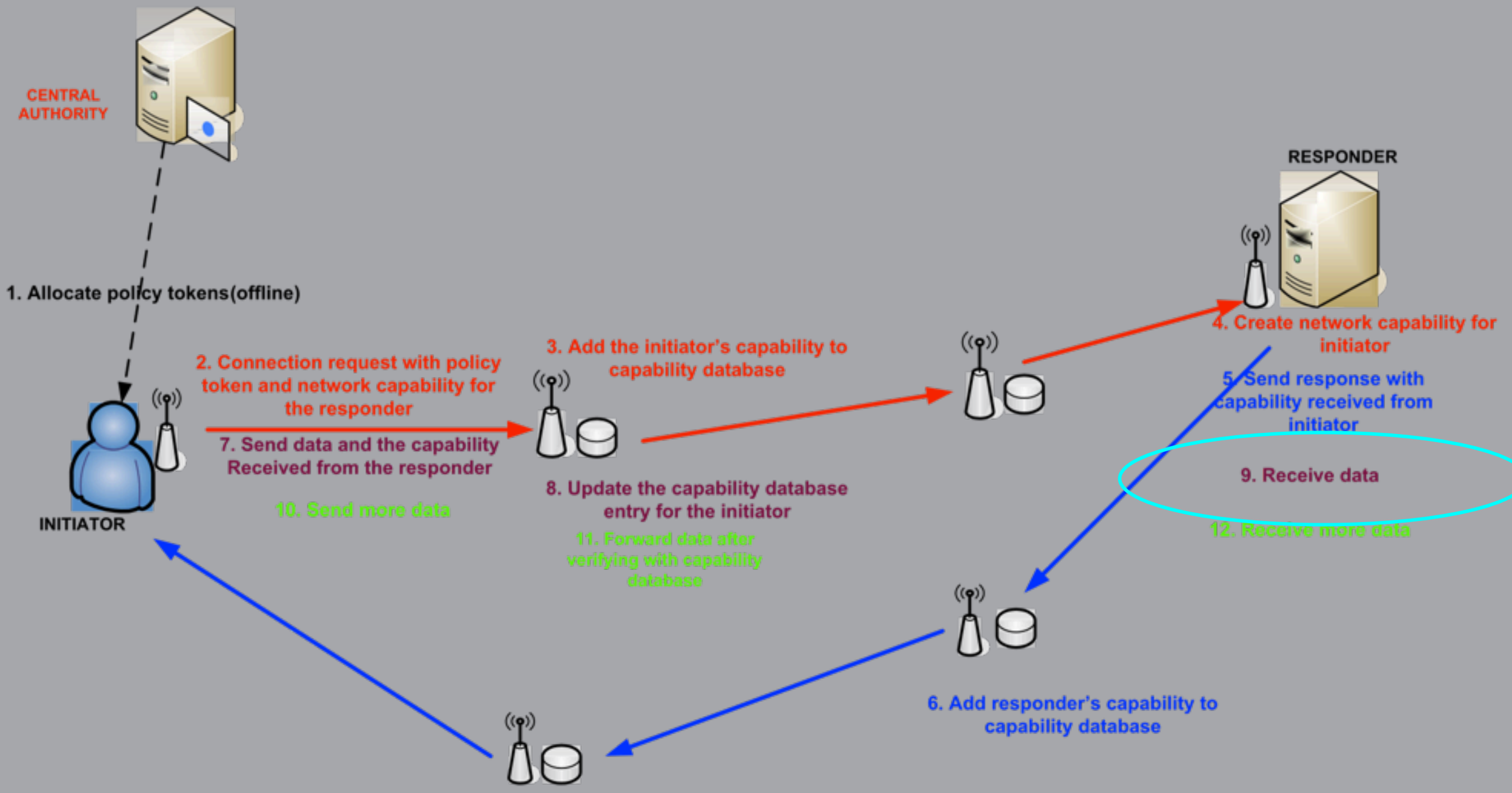
System Architecture



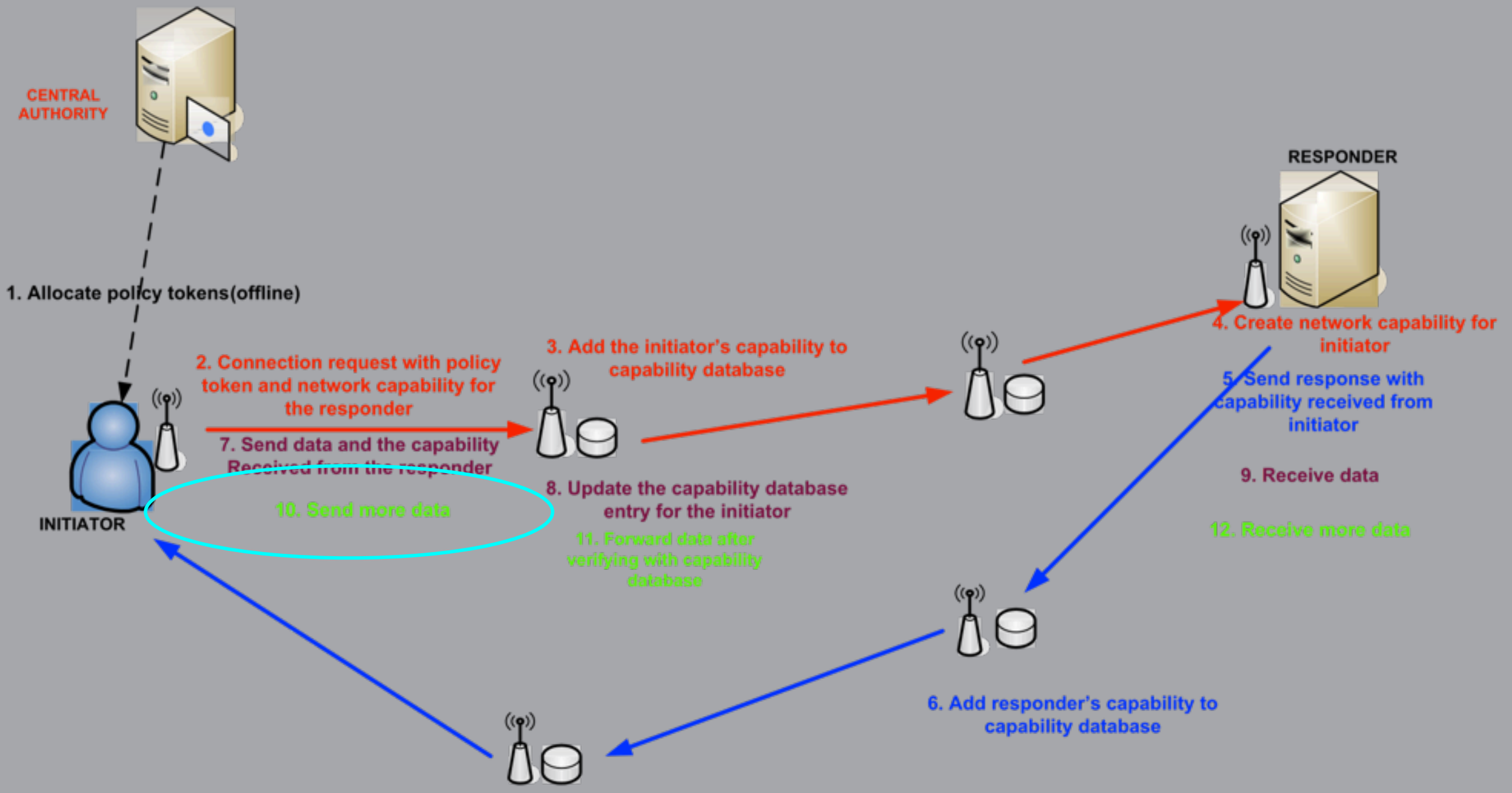
System Architecture



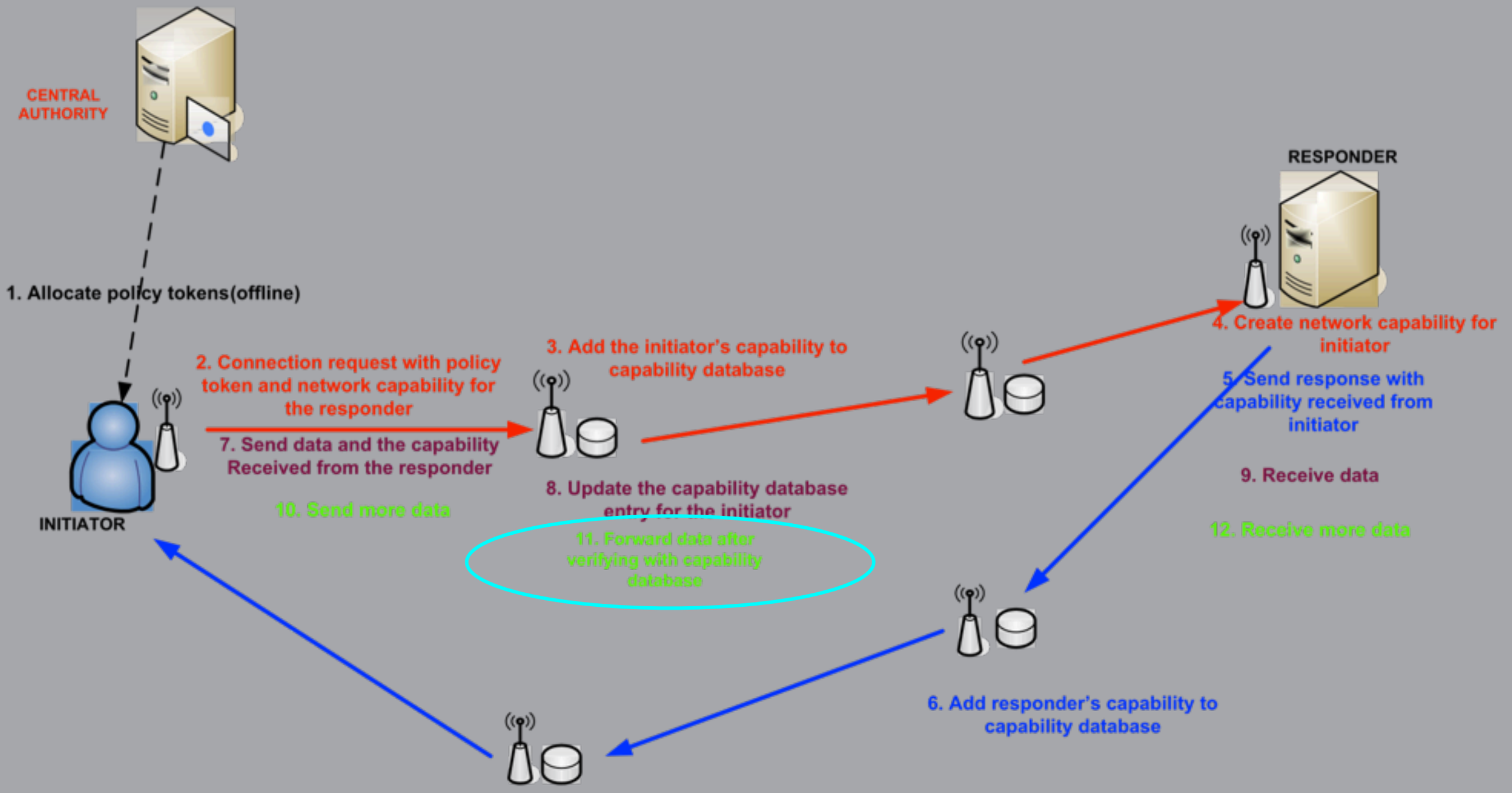
System Architecture



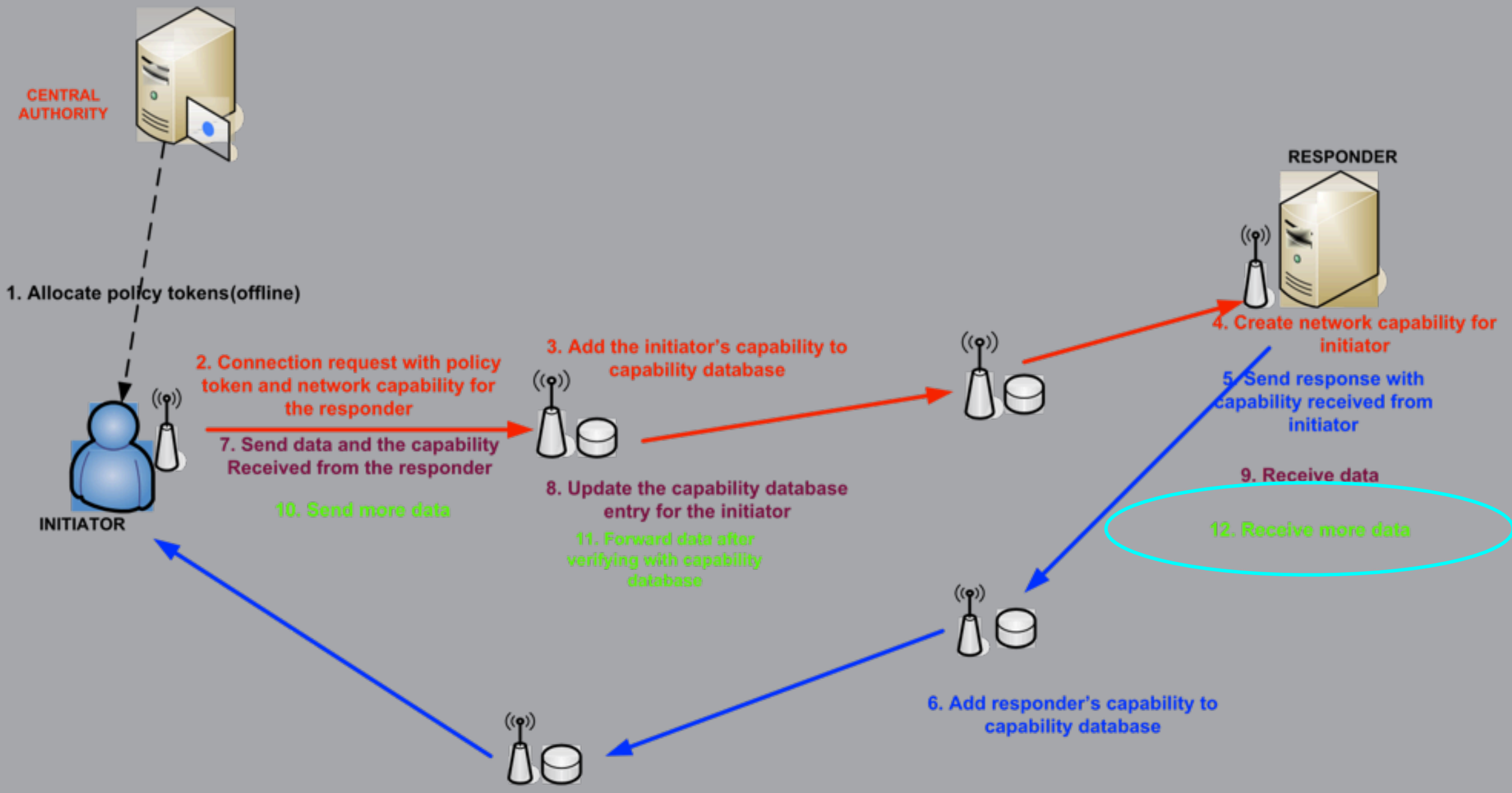
System Architecture



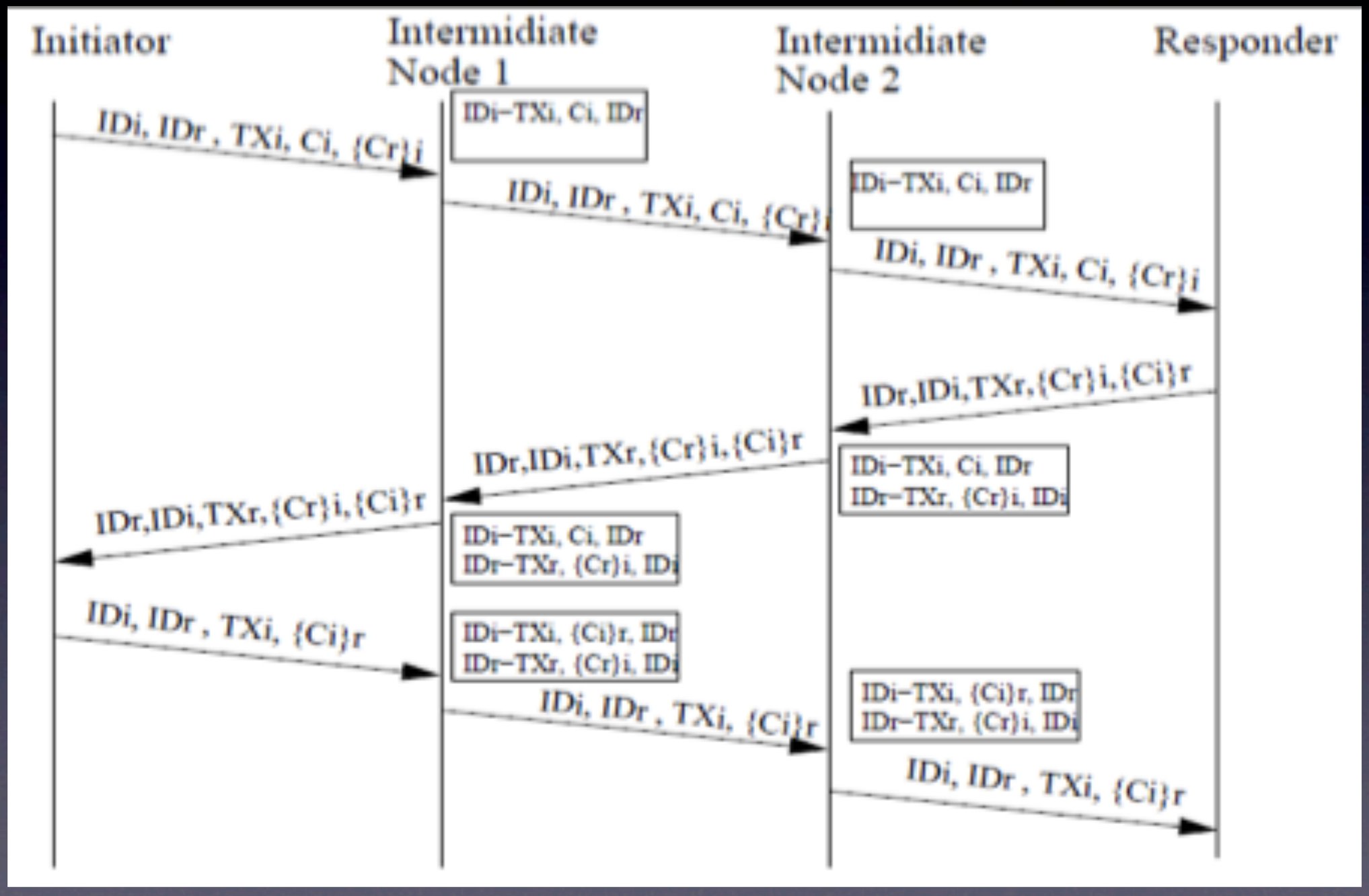
System Architecture



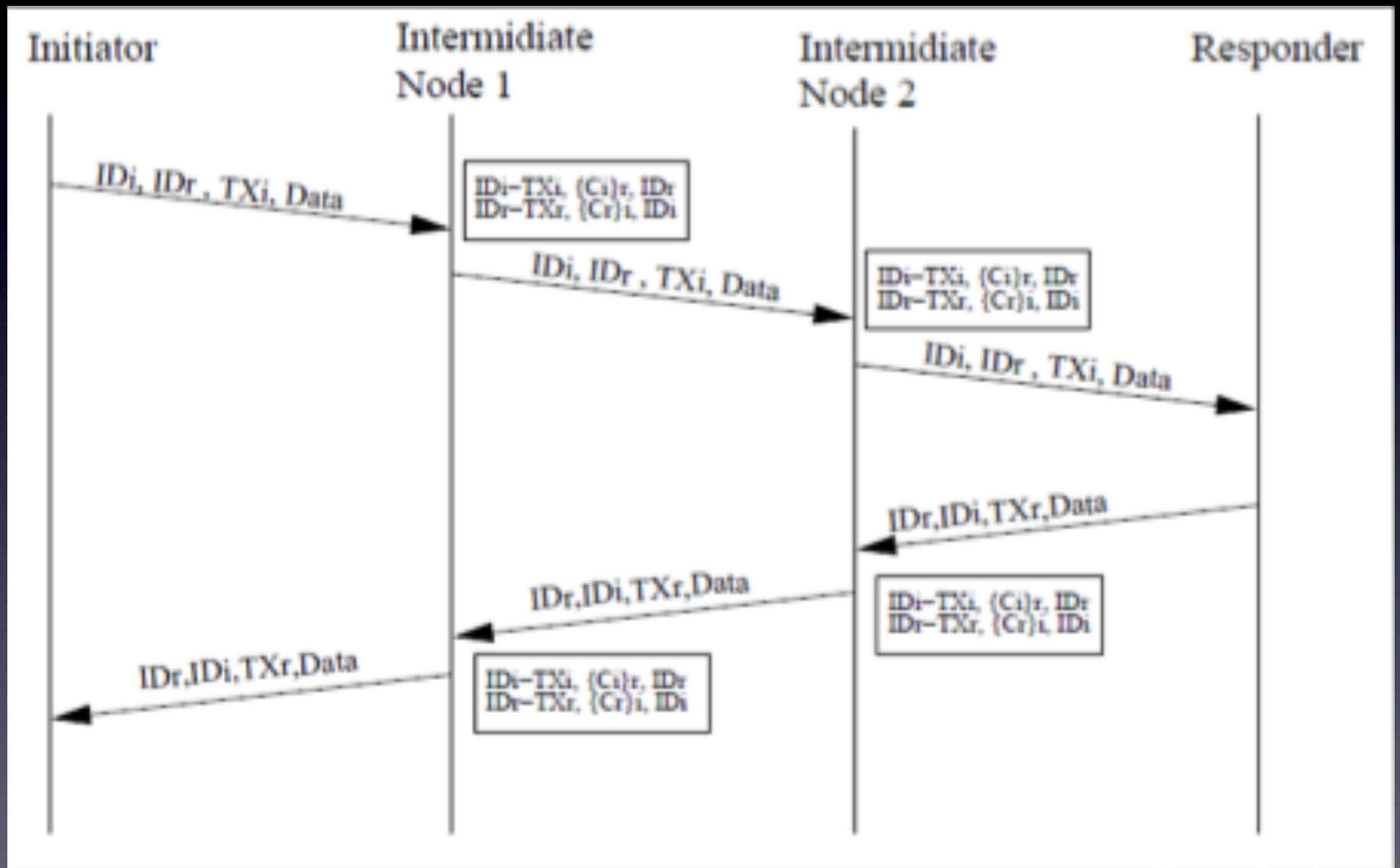
System Architecture



Capability Establishment



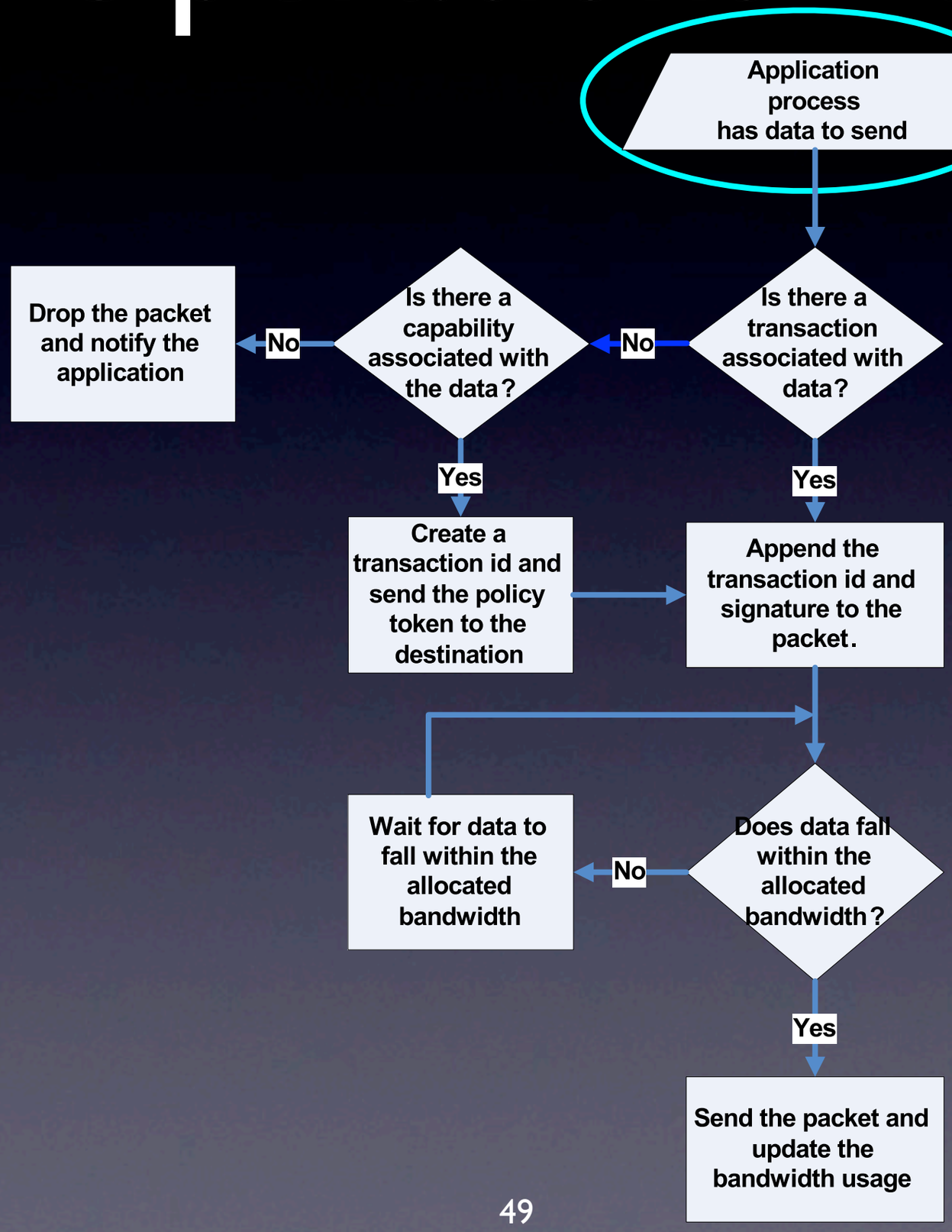
Data Transfer



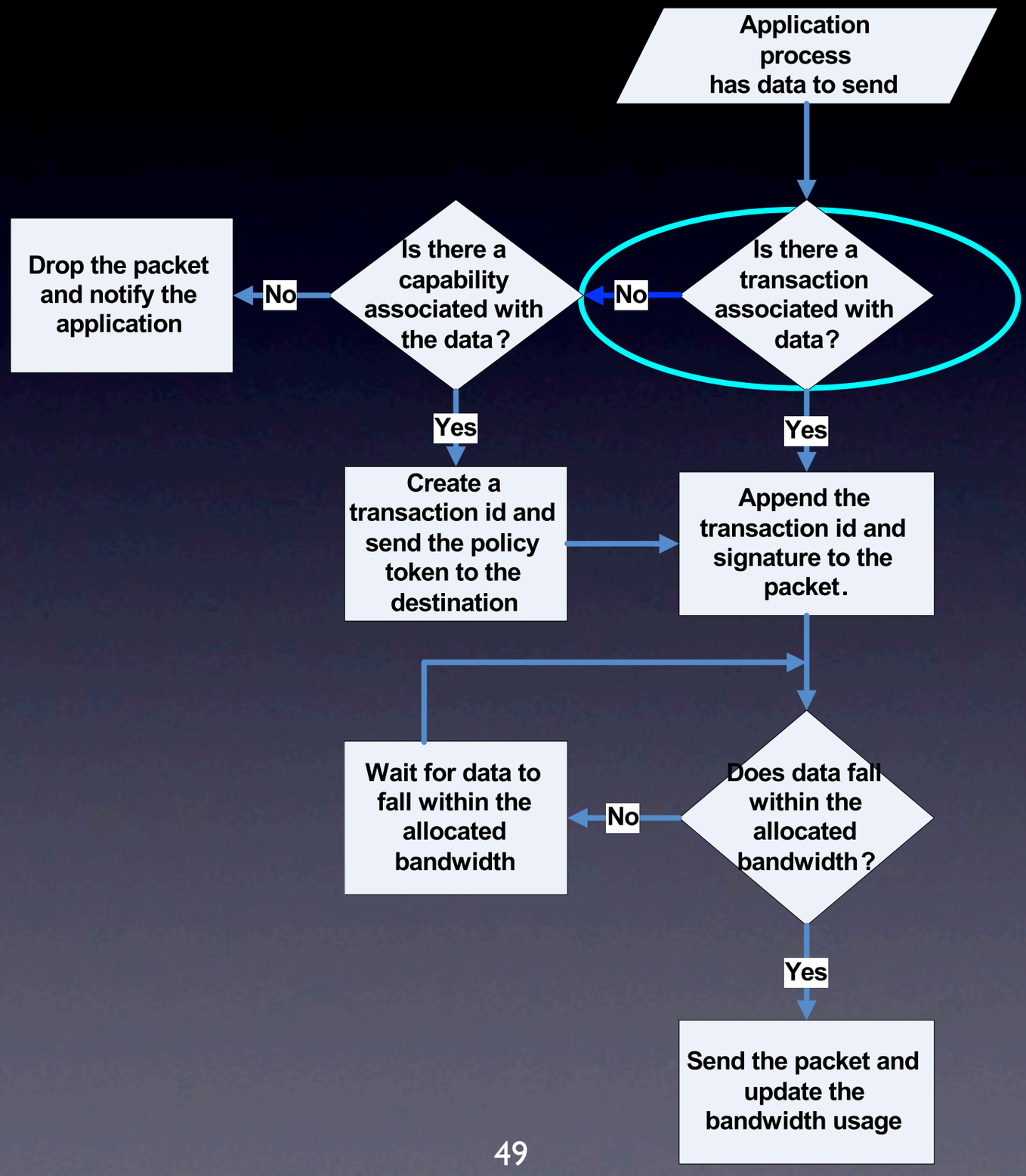
Node State

- Capability Table (intermediate nodes)
  - Sessions passing thru the node
- Transaction Table (sender)
  - Sessions initiated by the node
- Issue Table (receiver)
  - Network capabilities issued by the node
- Policy Table (sender)
  - All the capabilities available to the node

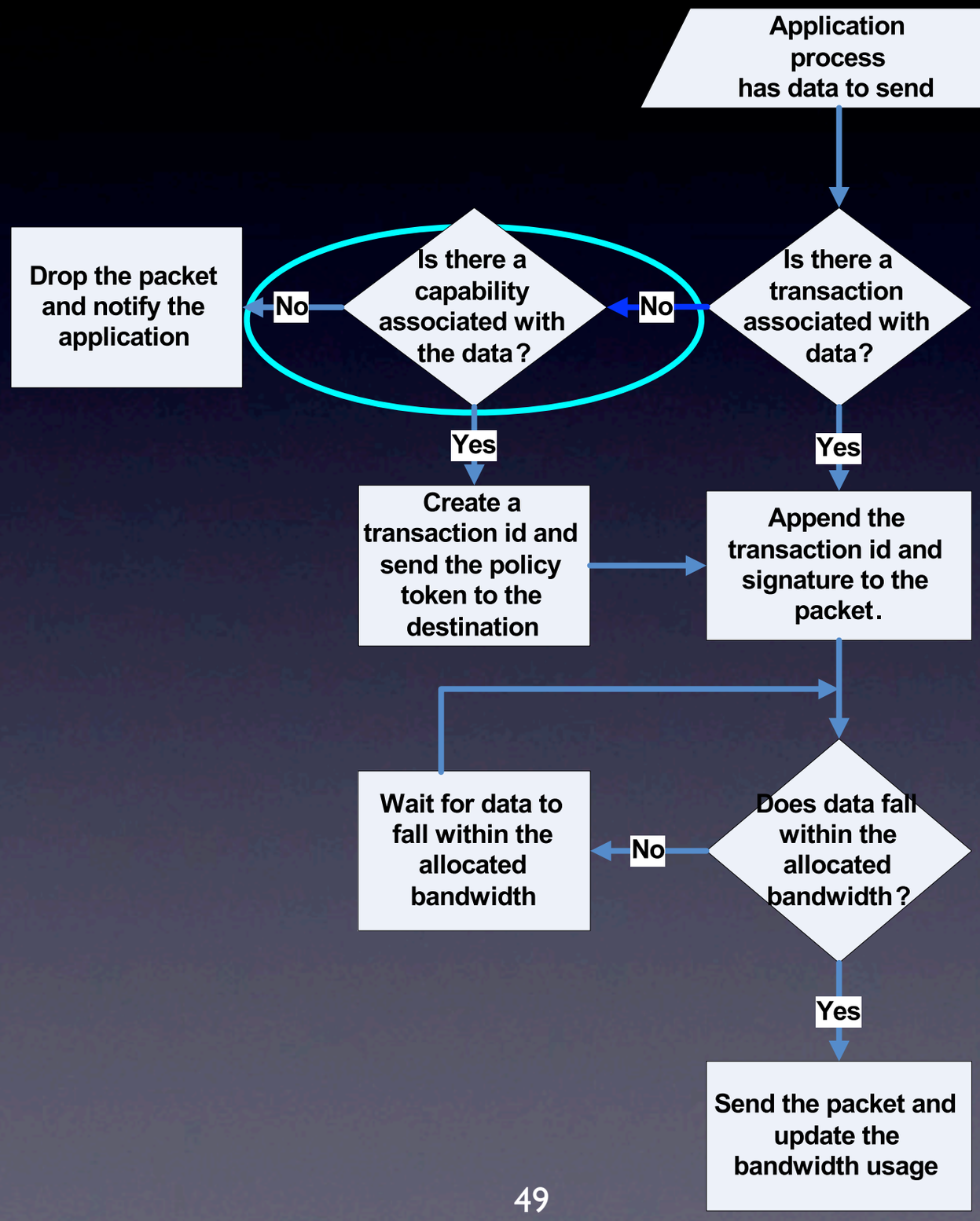
Node Operations - Sender



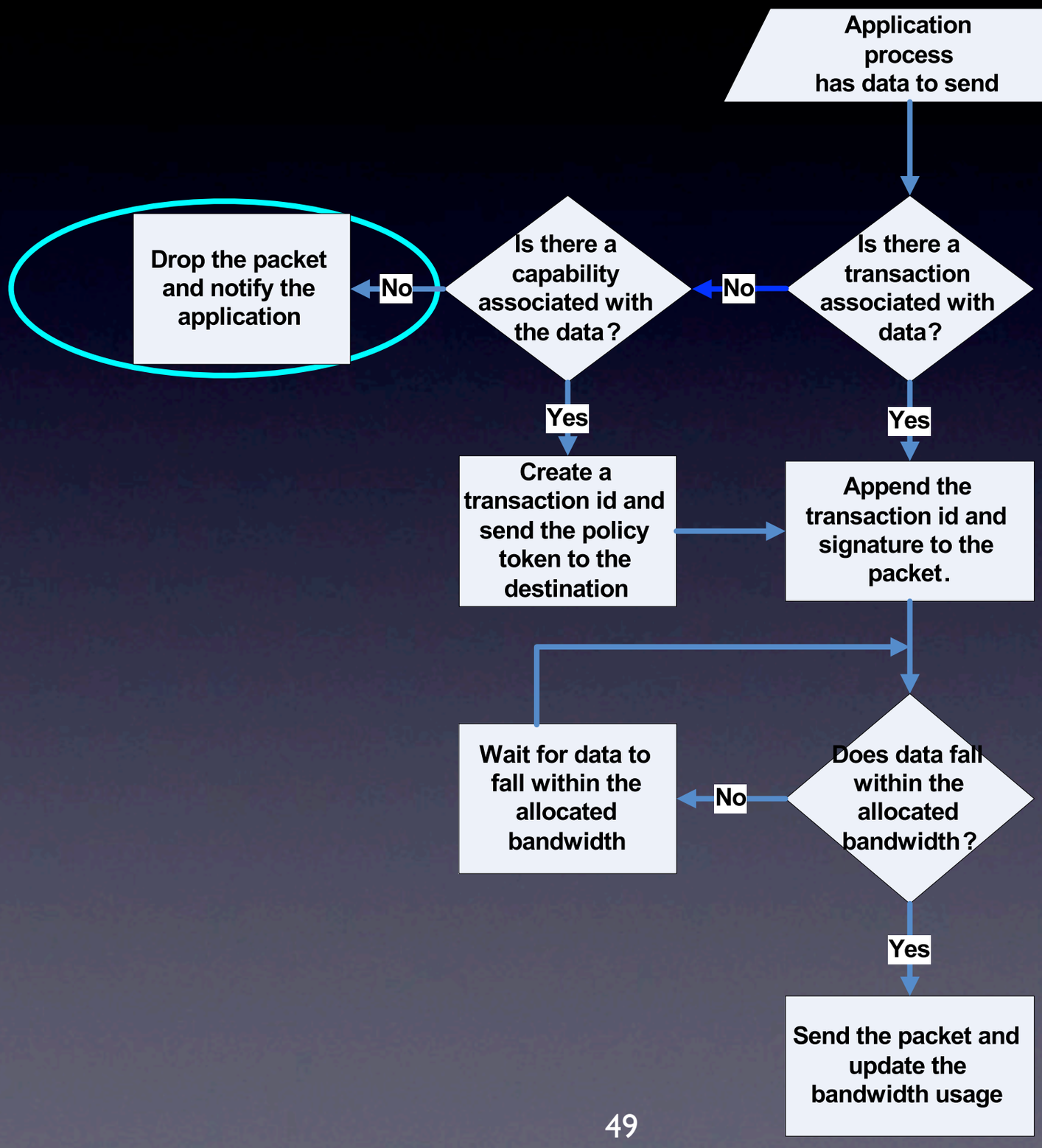
Node Operations - Sender



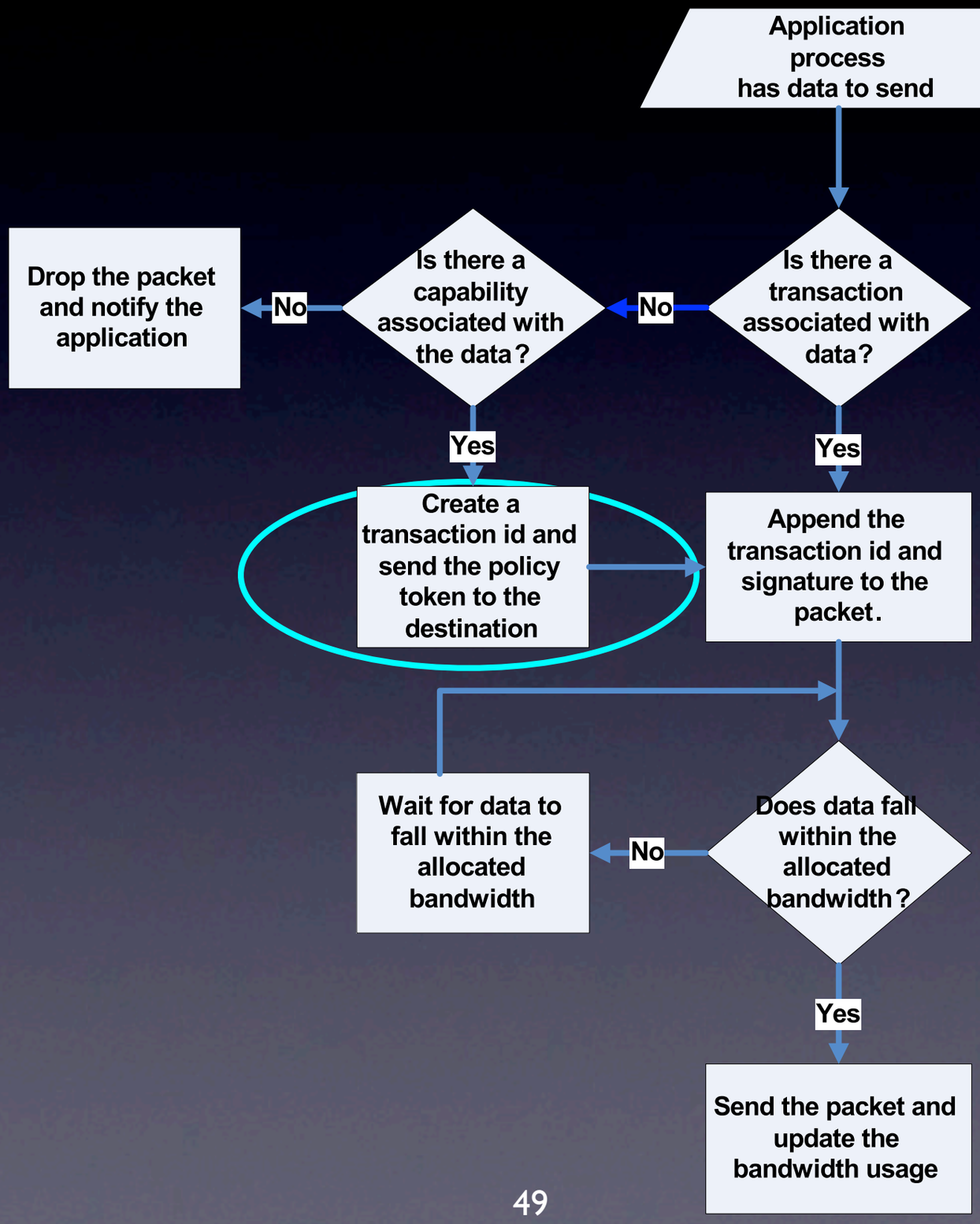
Node Operations - Sender



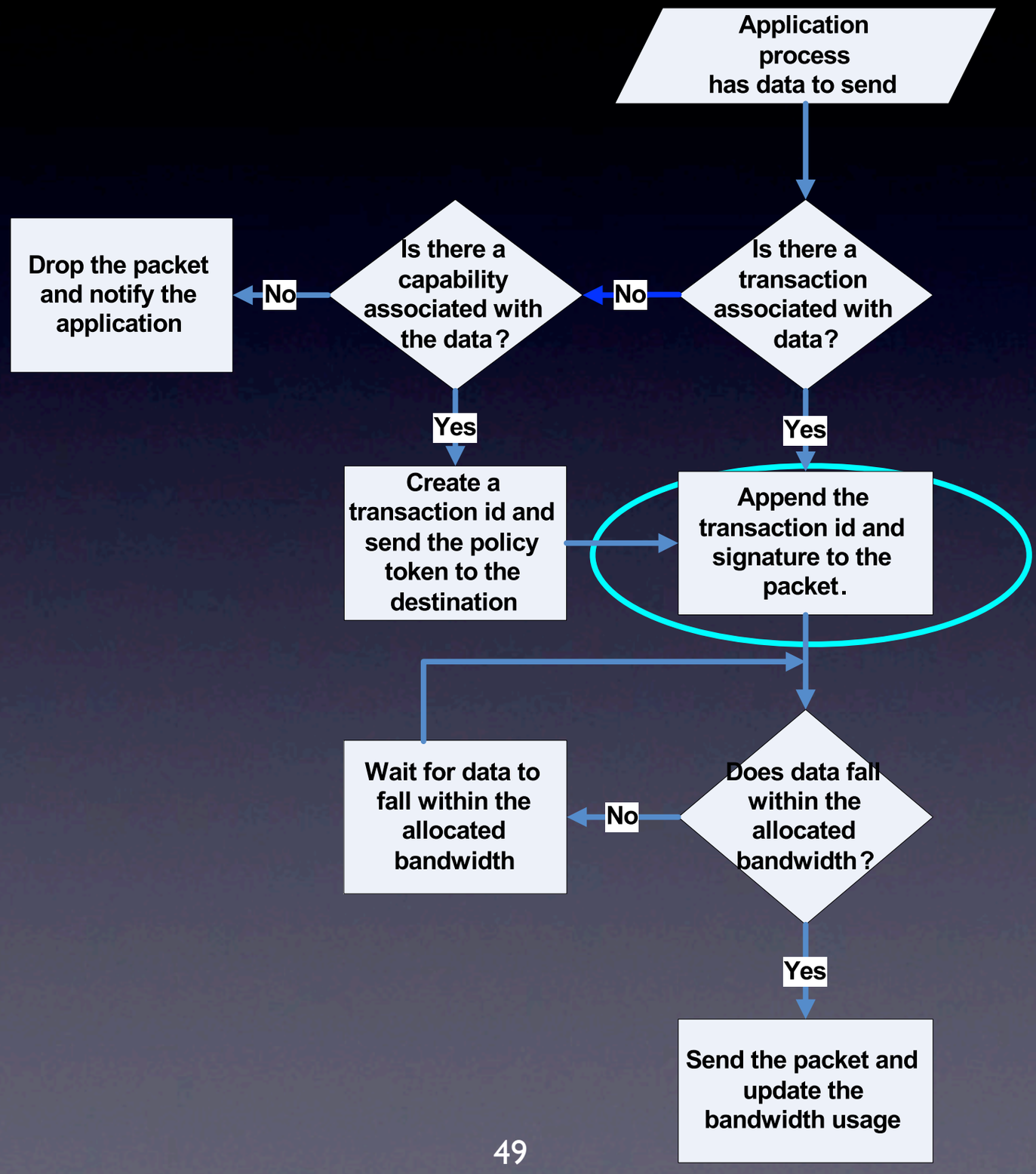
Node Operations - Sender



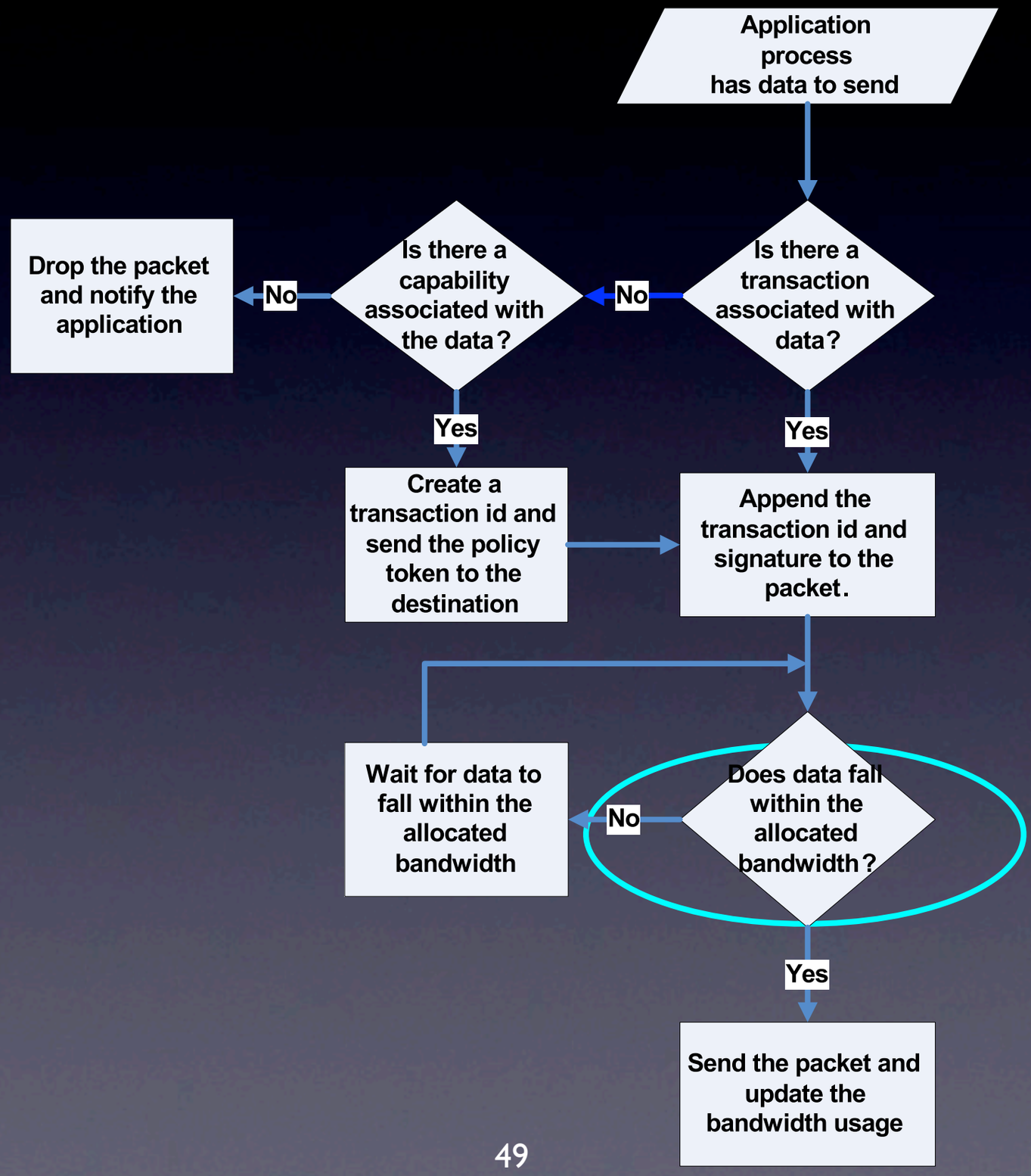
Node Operations - Sender



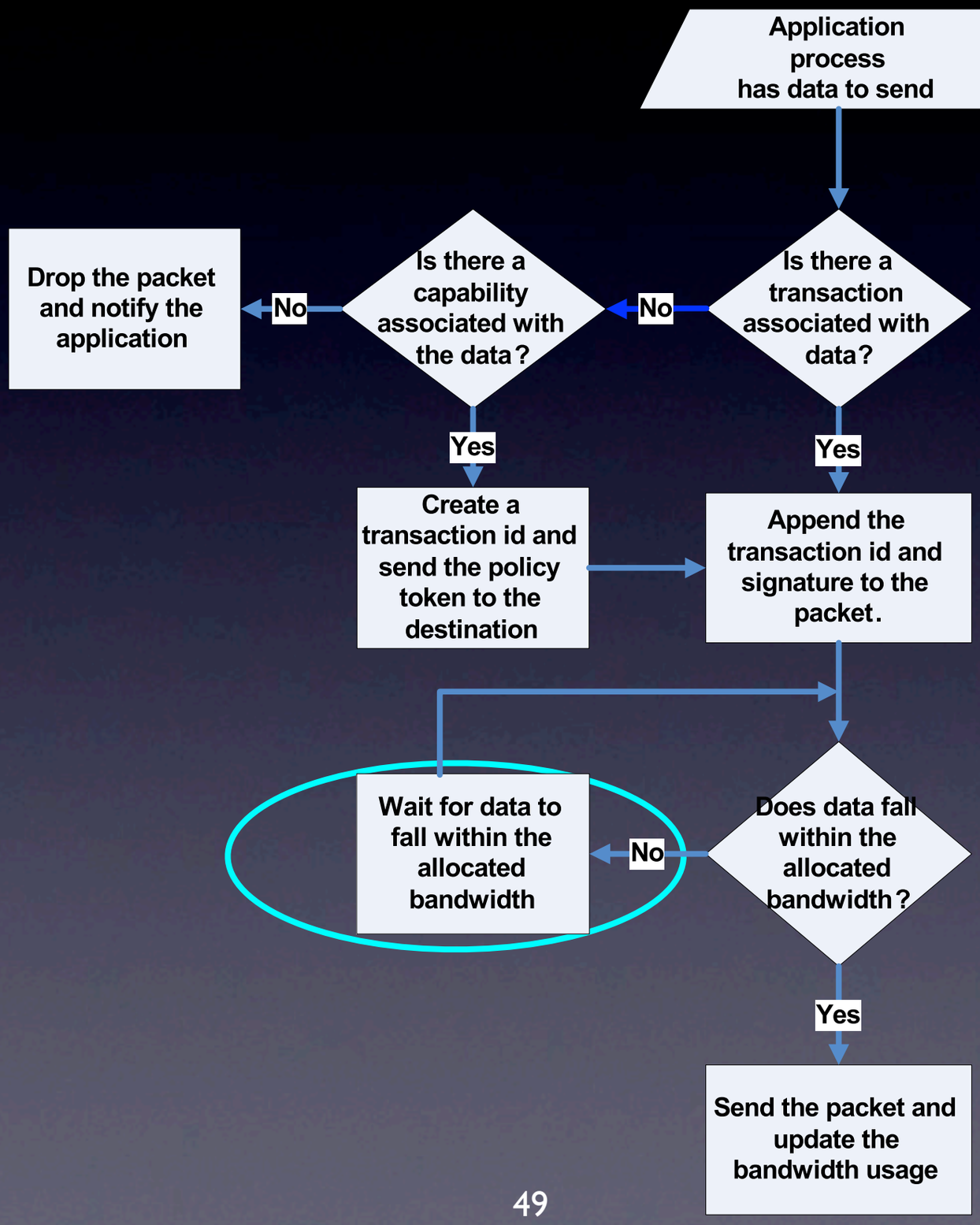
Node Operations - Sender



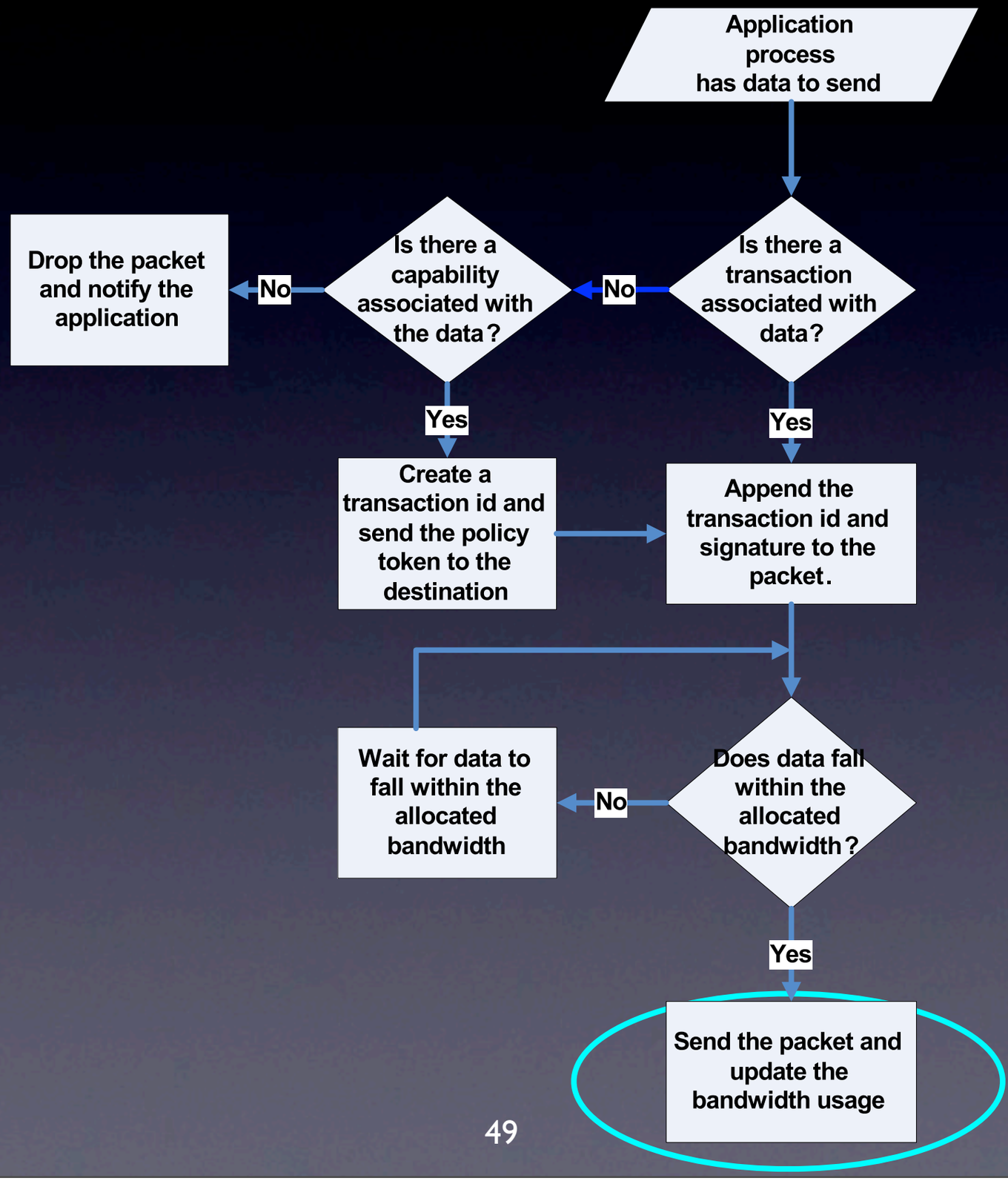
Node Operations - Sender



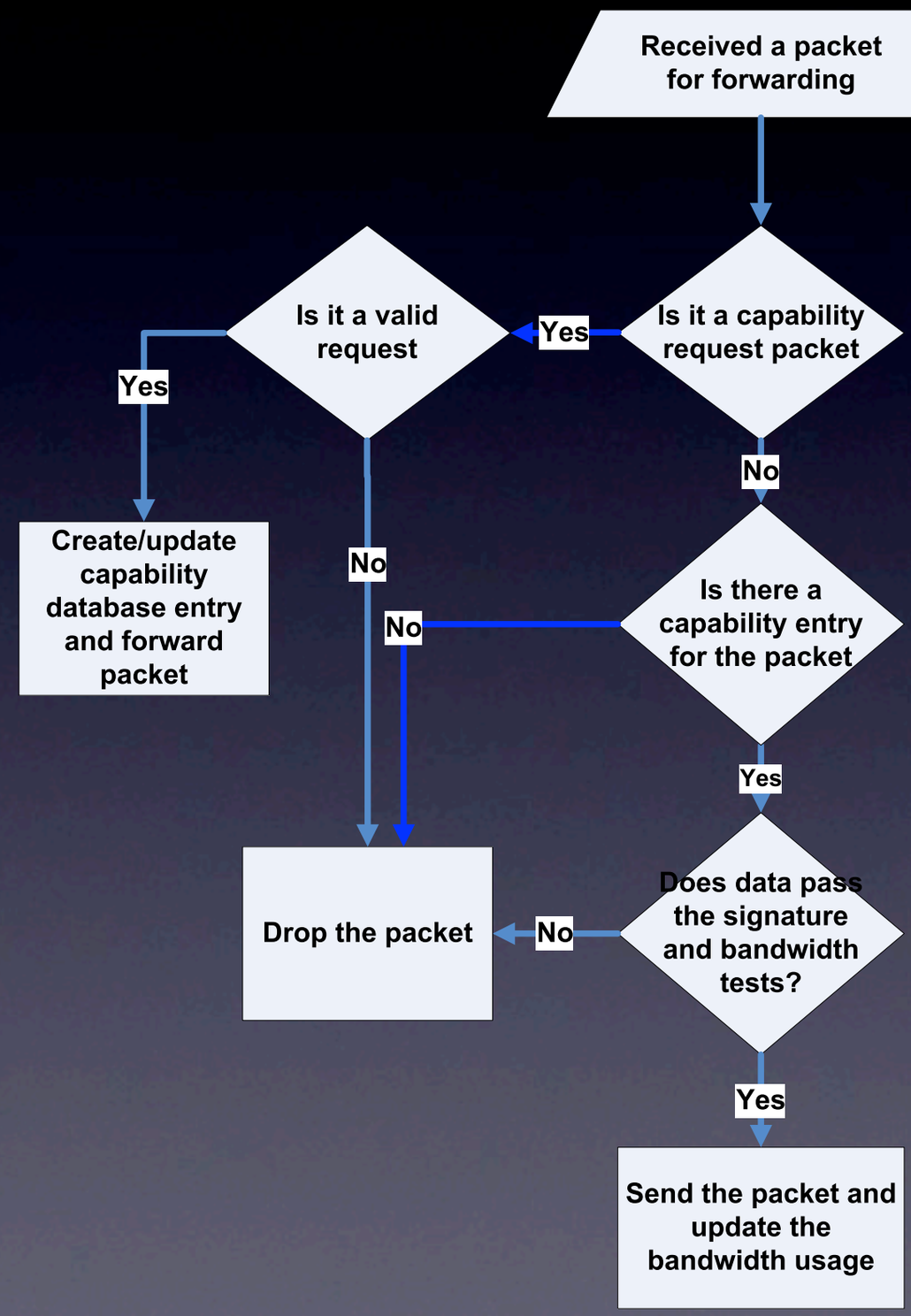
Node Operations - Sender



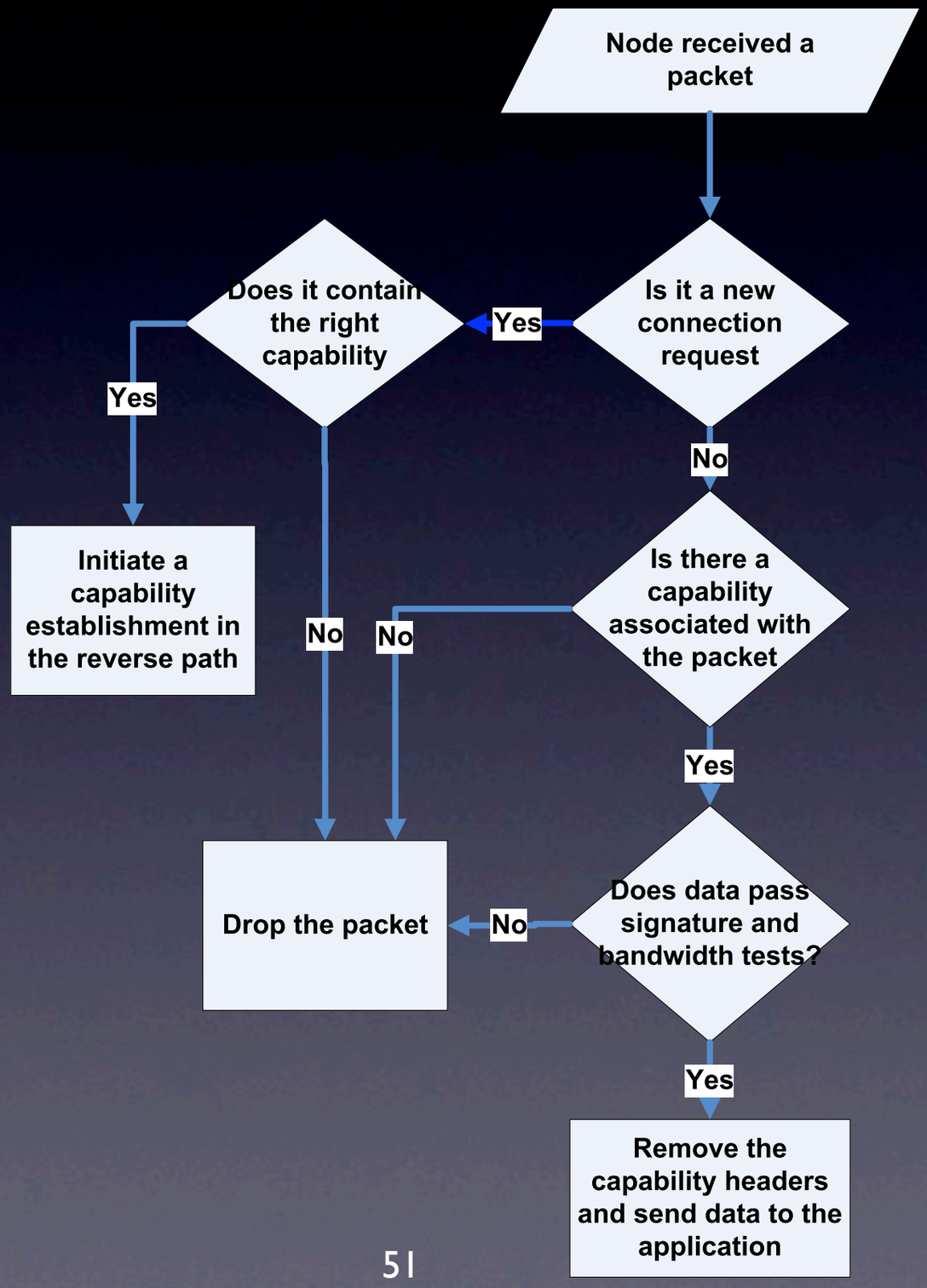
Node Operations - Sender



Node Operations – Intermediate Node



Node Operations - Receiver

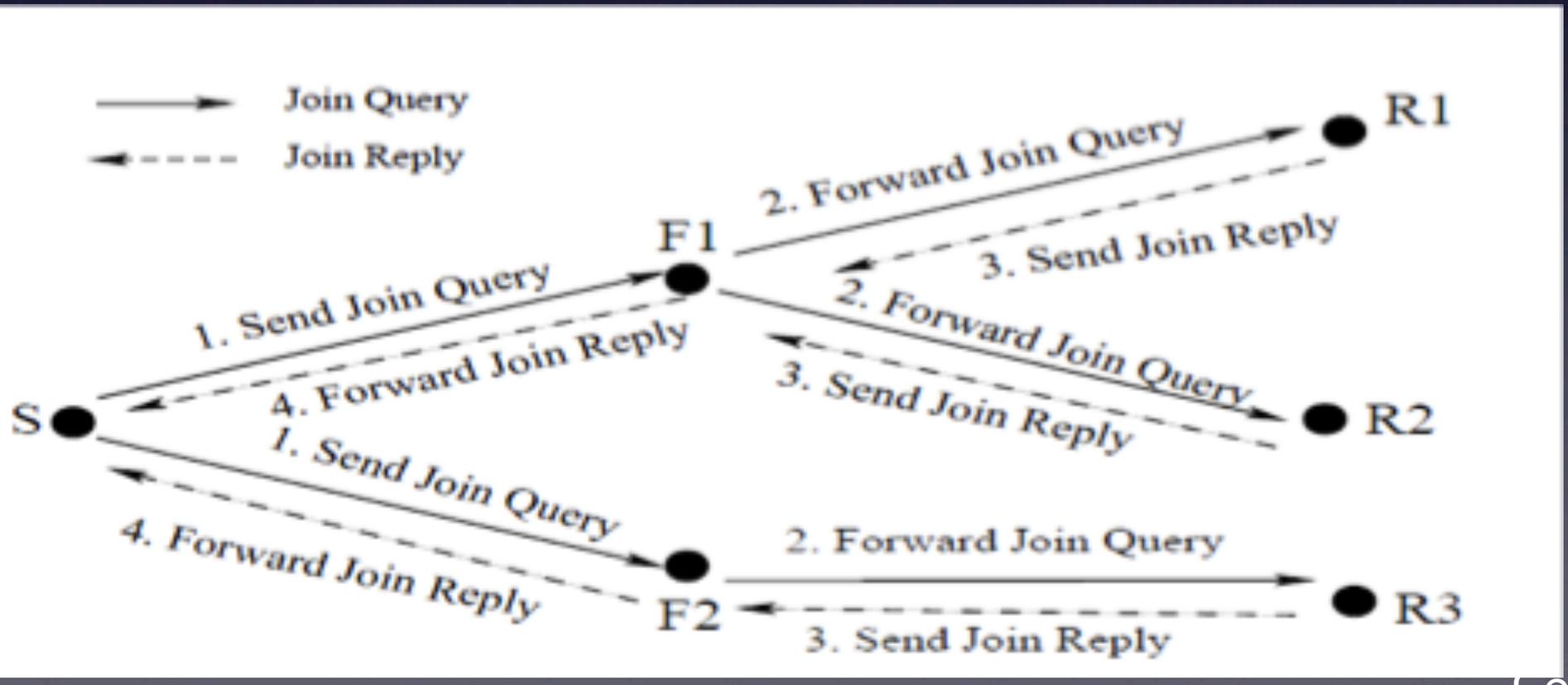


Routing Traffic

- Attacks can be launched using routing traffic alone
- DIPLOMA limit the number of route requests
  - Allow route request only the node has capability
  - Limit the number of route request per capability

Multicast Traffic

- Multicast Policy Tokens (MPT)
  - Contains multicast group and bandwidth allowed
- DIPLOMA enabled On Demand Multicast Routing Protocol [LSG00]
  - Join Query and Join Reply has MPT

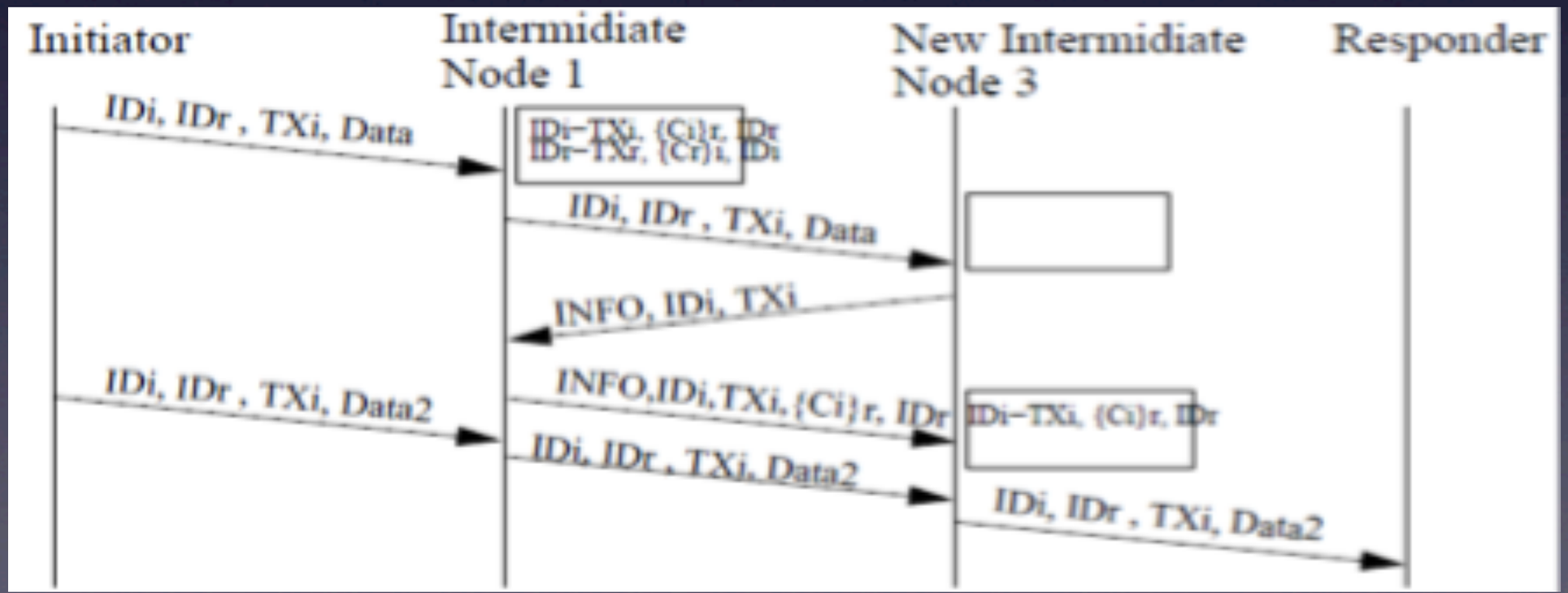


Challenges

- Route Change
- Selfish Nodes
- Capability Misuse
- Bandwidth Allocation

Route Change

- Frequent route change in MANET due to mobility
- New intermediate node get state update from upstream node
  - Changes localized



Selfish Nodes

- MANET requires co-operation of nodes
  - Routing protocols
  - Packet forwarding

- DIPLOMA requires
  - Signature verification
- Reward and punishment model to ensure co-operation [JS07]
  - Nodes forwarding too many packets with wrong signature is selfish

Capability Misuse

- Nodes may reuse the same capability for multiple sessions
  - Consolidated capability
  - Multiple disjoint paths
- Distributed IDS to detect it [ZL00]
  - Require minimum amount of data exchange
- Capability bandwidth divided into buckets
  - Bitmask intersection to detect the reuse

Resource Allocation

- Policy tokens at hosts → Access control
- Network capabilities → Bandwidth
  - Allocated by the receivers according to the policy tokens they have
- How to allocate the bandwidth in the policy?

Feasibility

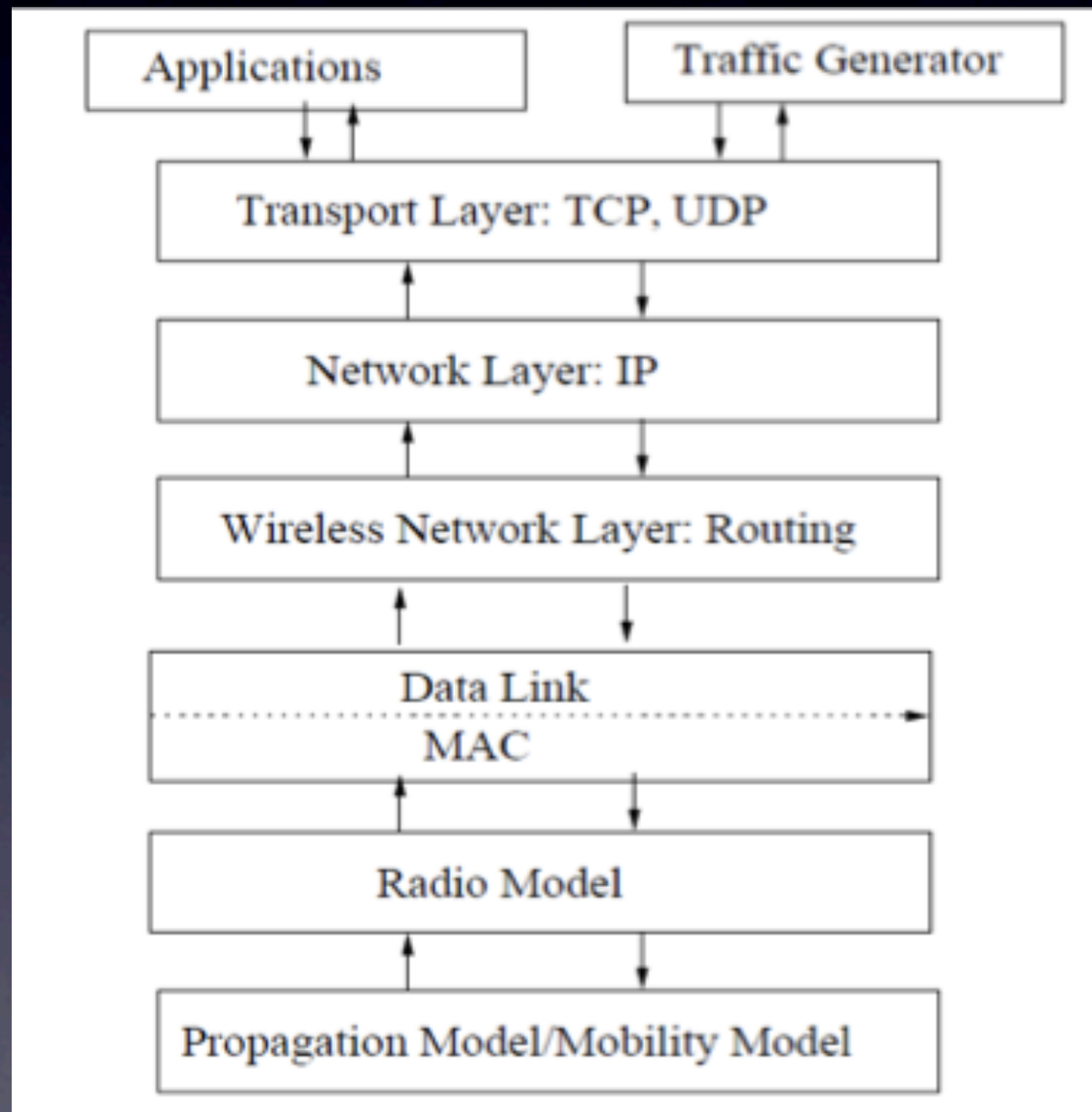
- Memory and CPU per packet high in MANETS
  - Technology trend: Faster and more power efficient processors
  - iPhone: 624 MHz Arm-11 processor, 128 MB RAM
- Threat Model and Security Analysis
- GloMoSim Simulator
- Orbit Lab Testbed

GloMoSim

- Global Mobile Information System Simulator
  - Discrete event simulator
  - A layered approach – communication using APIs
- Added DIPLOMA layer
  - Process protocol packets
  - Capability establishment and enforcement
  - Bandwidth enforcement
  - Supported packet processing delay

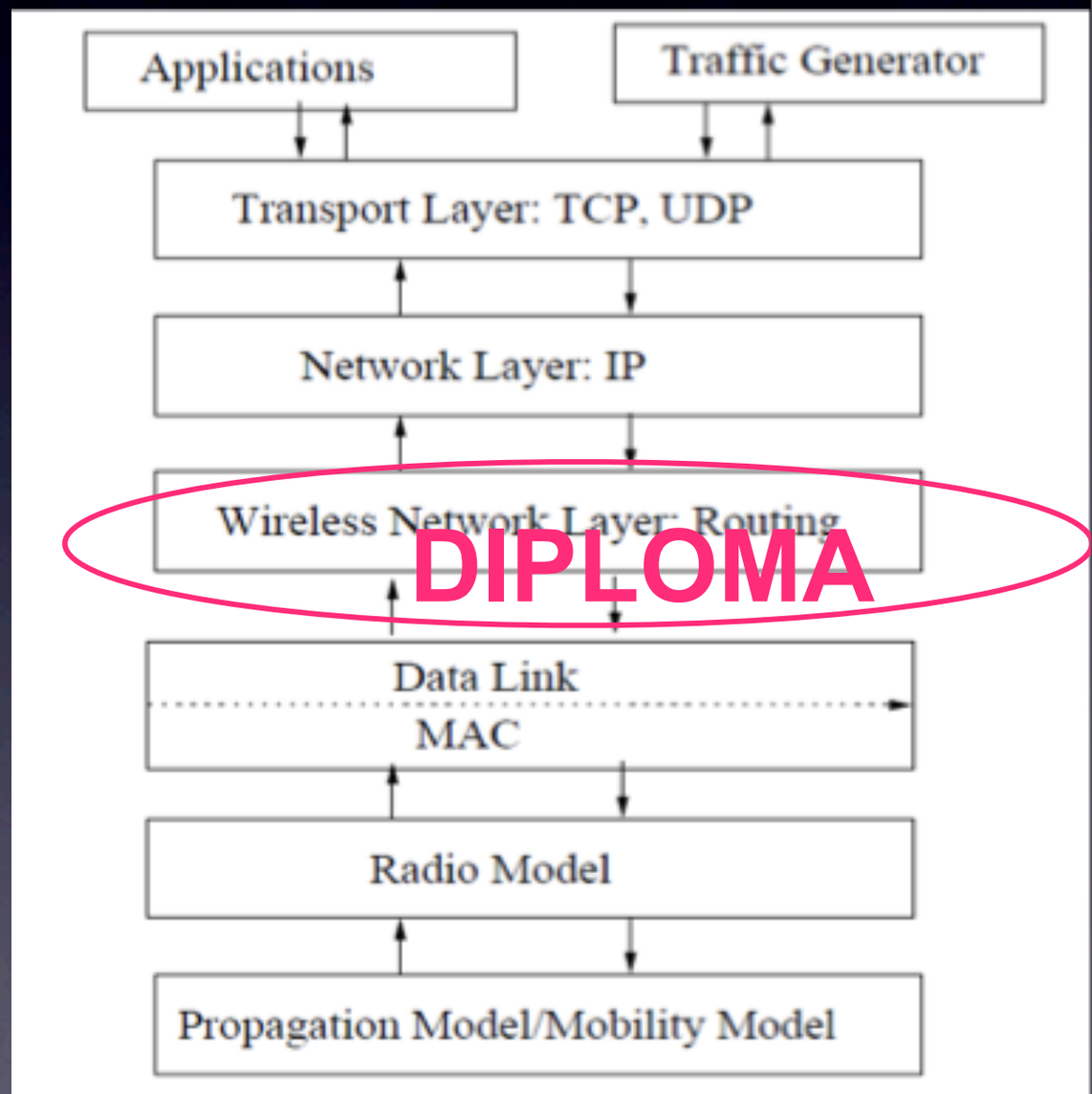
GloMoSim

- Global Mobile Information System Simulator
  - Discrete event simulator
  - A layered approach – communication using APIs
  - Added DIPLOMA layer
    - Process protocol packets
    - Capability establishment and enforcement
    - Bandwidth enforcement
    - Supported packet processing delay



GloMoSim

- Global Mobile Information System Simulator
  - Discrete event simulator
  - A layered approach – communication using APIs
  - Added DIPLOMA layer
    - Process protocol packets
    - Capability establishment and enforcement
    - Bandwidth enforcement
    - Supported packet processing delay



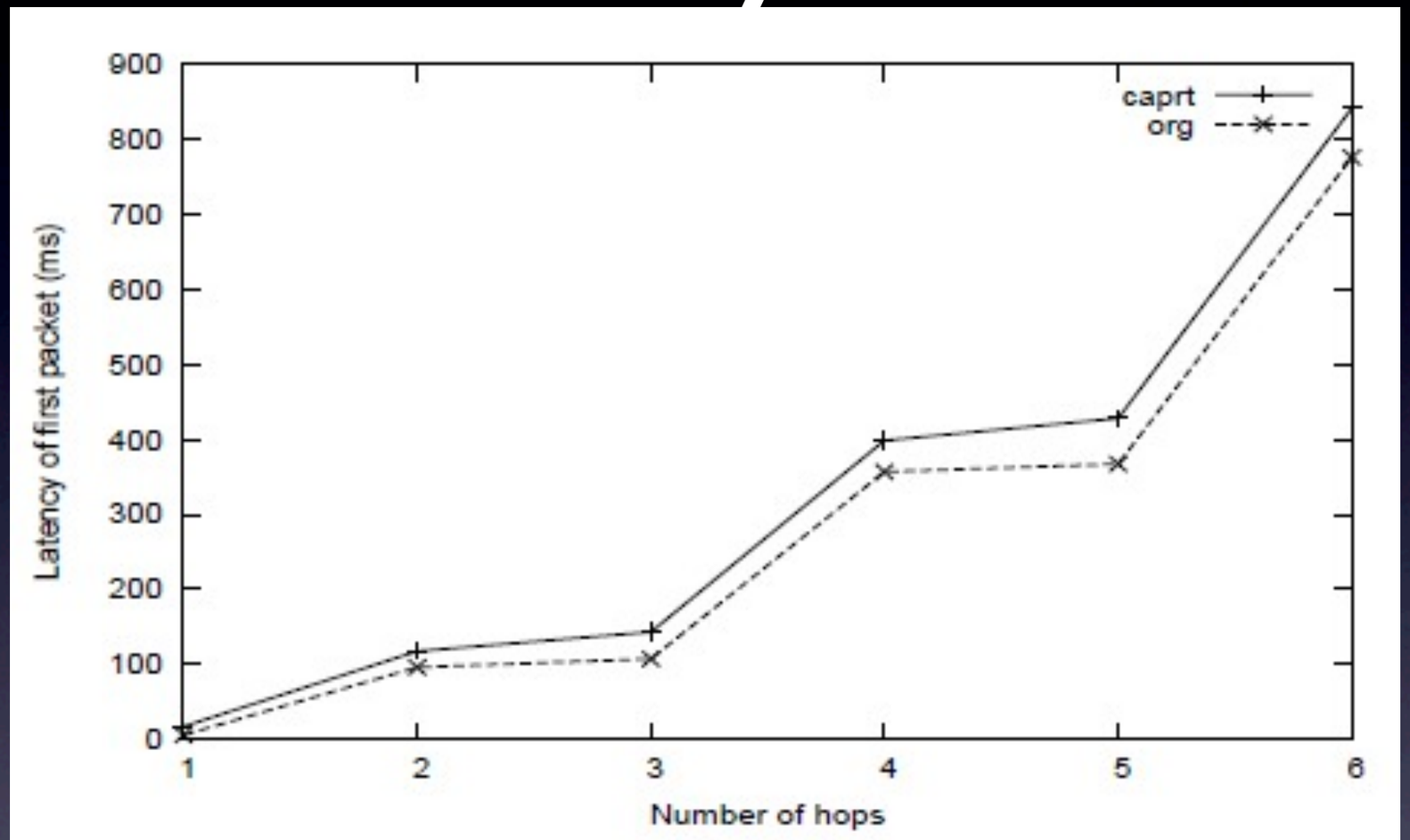
Parameters of Interest

- Latency of packets
  - Time taken for a packet to reach from a source to destination
  - First packet latency, Average latency
- Throughput
- Packet Delivery Ratio (PDR)

Input Parameters

- Radio range = 377m, link bandwidth = 2 Mbps, 802.11 MAC
- Packet processing time = 0.01 mS (equavalent to 100Mbps for 128 B packets)
- Database: insertion = 0.01 mS, lookup = 0.005 mS
- 1024 bit RSA for capability
  - Signature 3.159 mS, verification 0.140 mS
- 256 bit for packet signature
  - Signature 0.168 mS, Verification 0.0275 mS

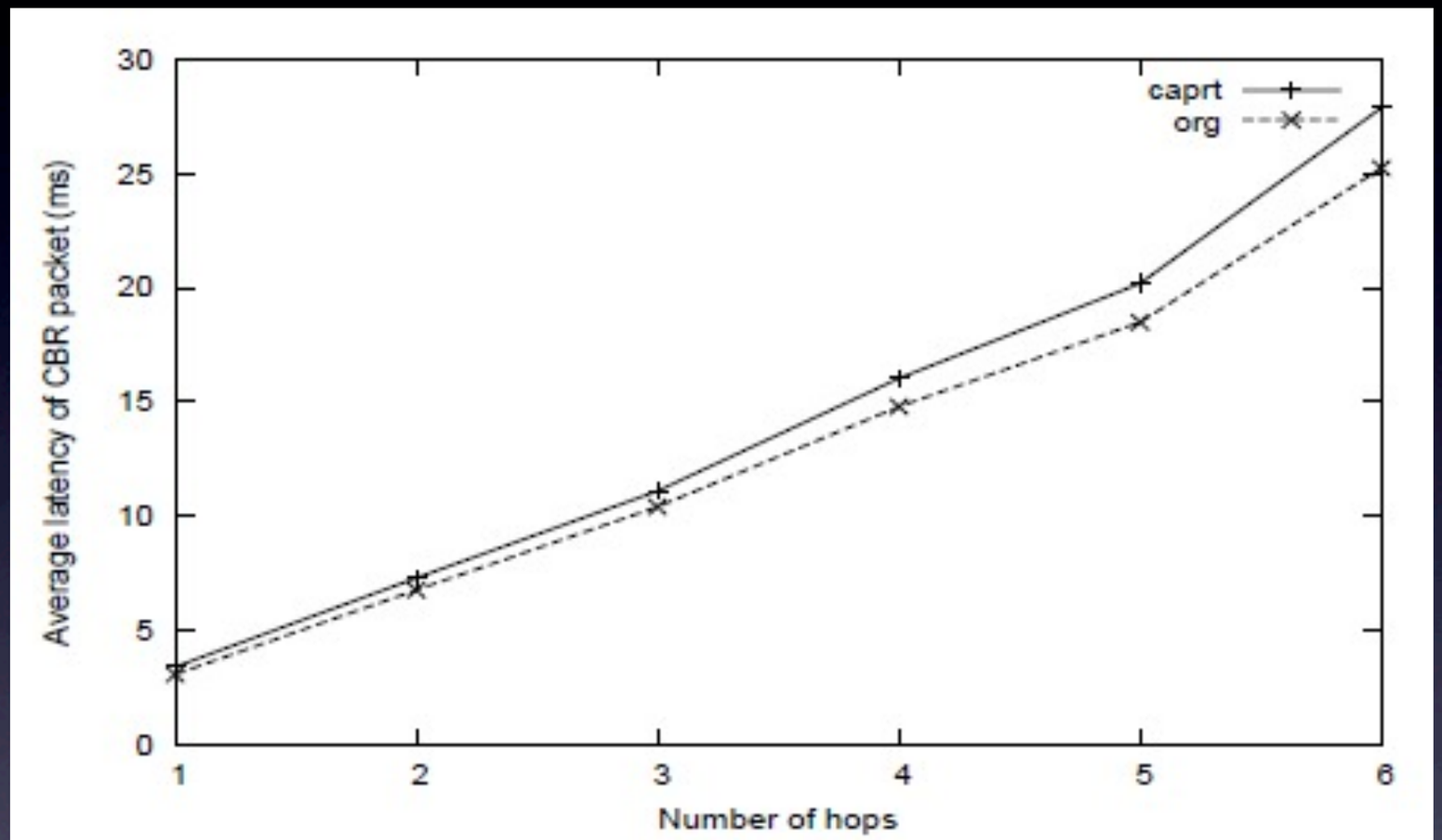
Latency of first packet



- Line topology (node distance = 200 m)
- CBR 512 B

- Capability establishment, database lookup, signature verification, larger header (36B)
- Overhead (35.8 mS, 41.6 mS, 60.9 mS) – About 20.5%

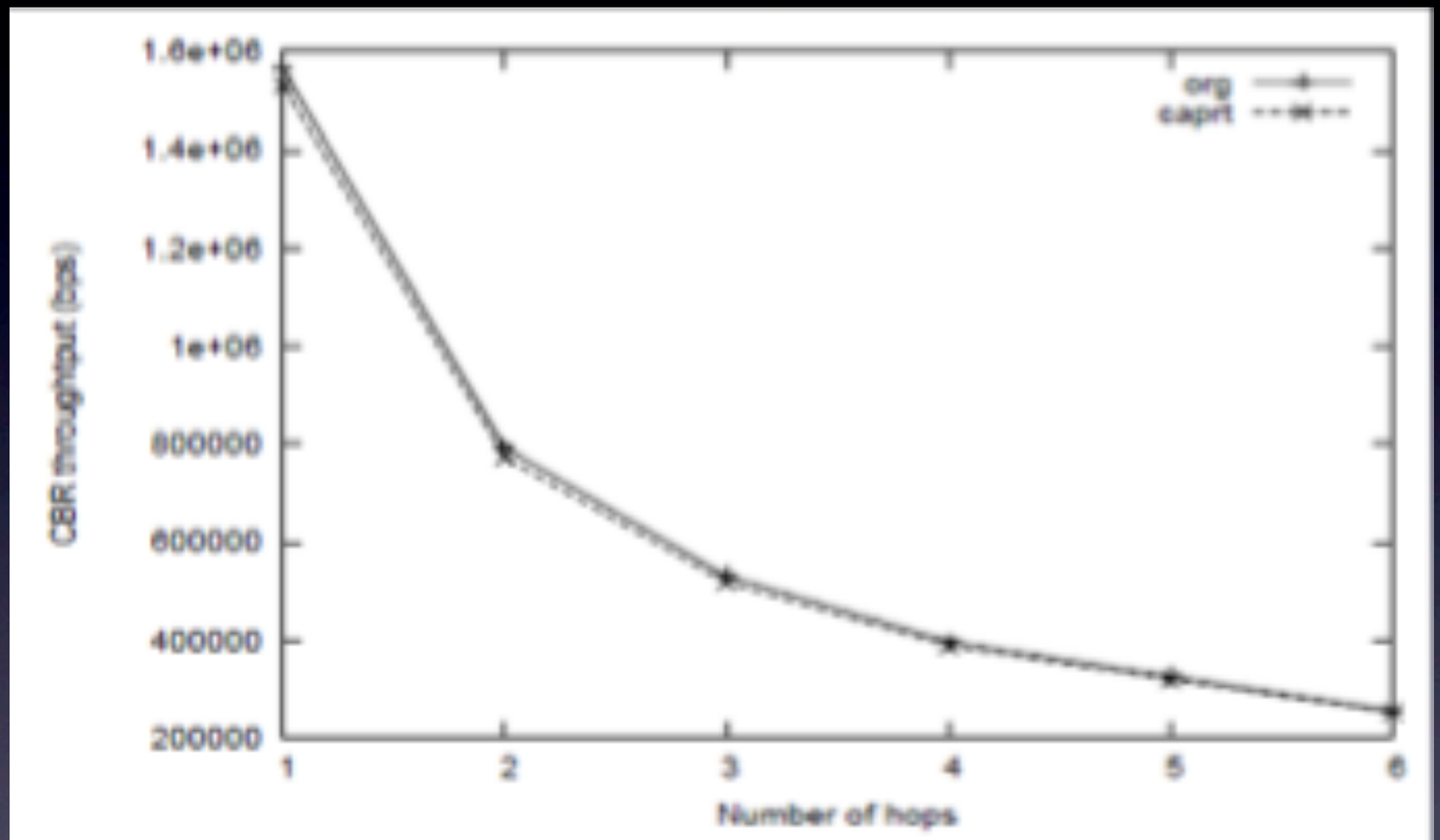
Average Latency



- Line topology
- CBR 512 B, 100 mS, 1000 pkts

- Database lookup, signature verification, larger header (36B)
- Overhead (0.6 mS, 1.2 mS, 1.6 mS) – About 8%

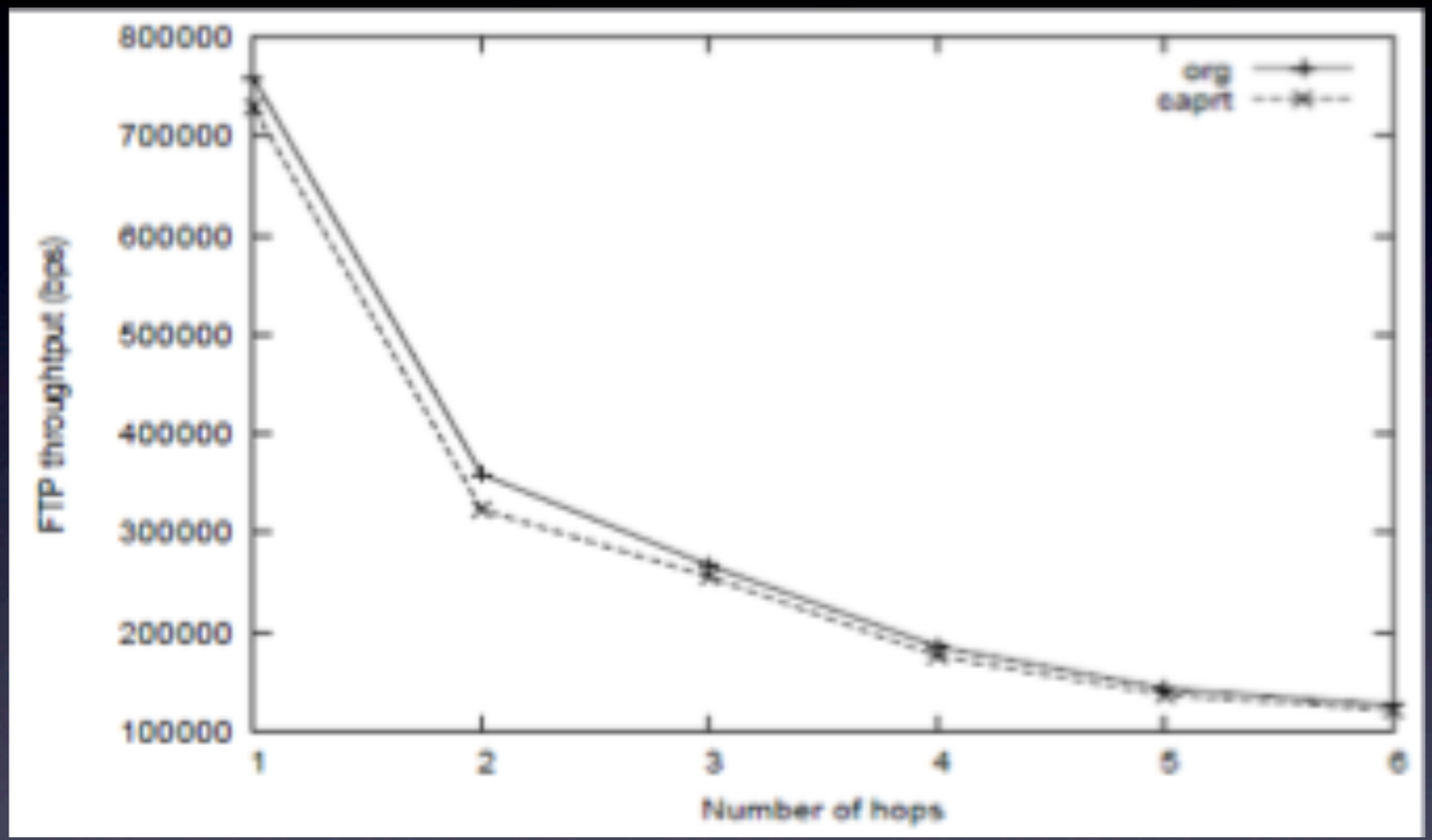
Throughput (CBR)



- Line topology
- CBR 1400 B, 1 mS

- Throughput overhead: 2% lower for our scheme

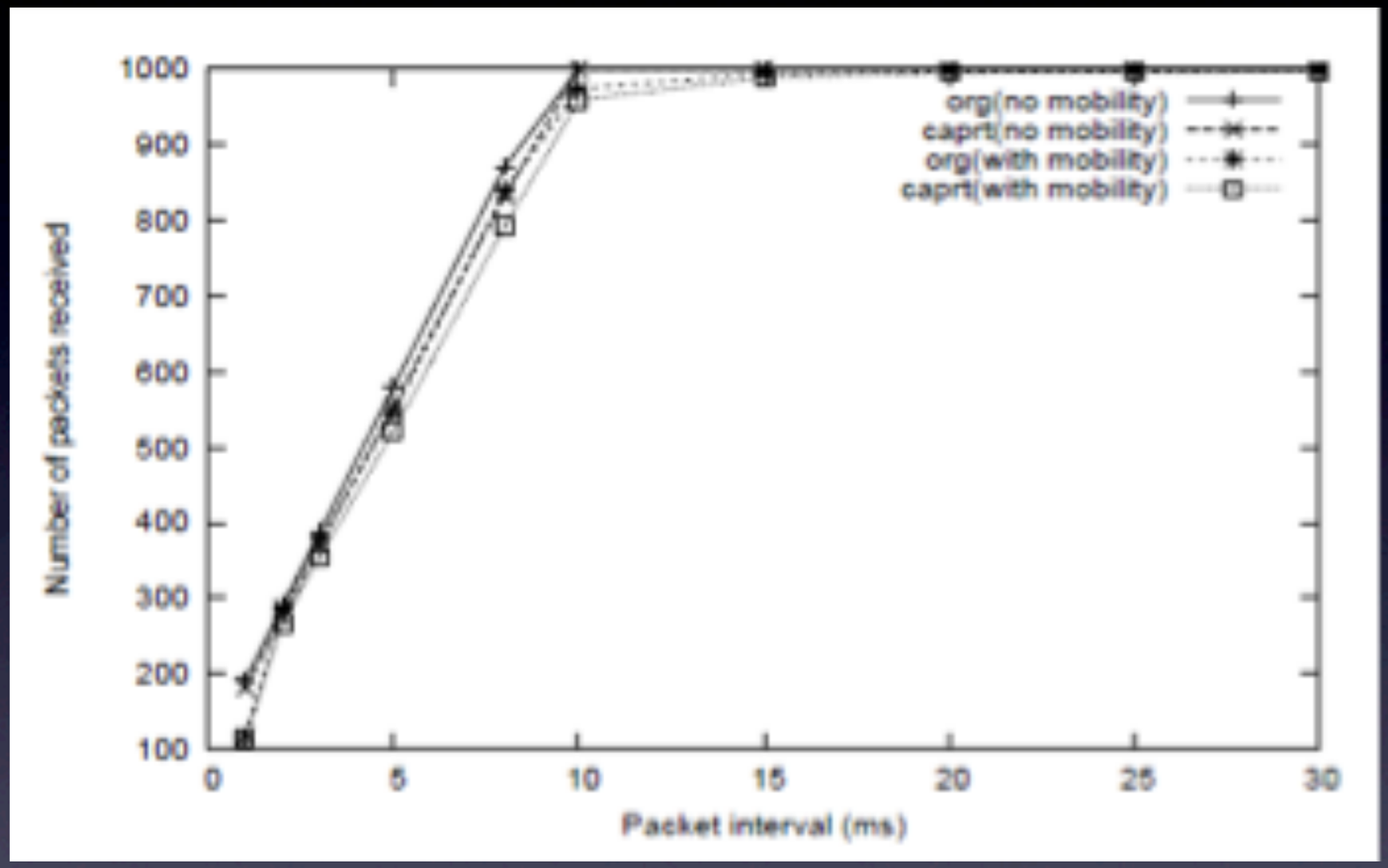
Throughput (FTP)



- Line topology
- 10 FTP files

- Throughput overhead: 5.3% lower for our scheme

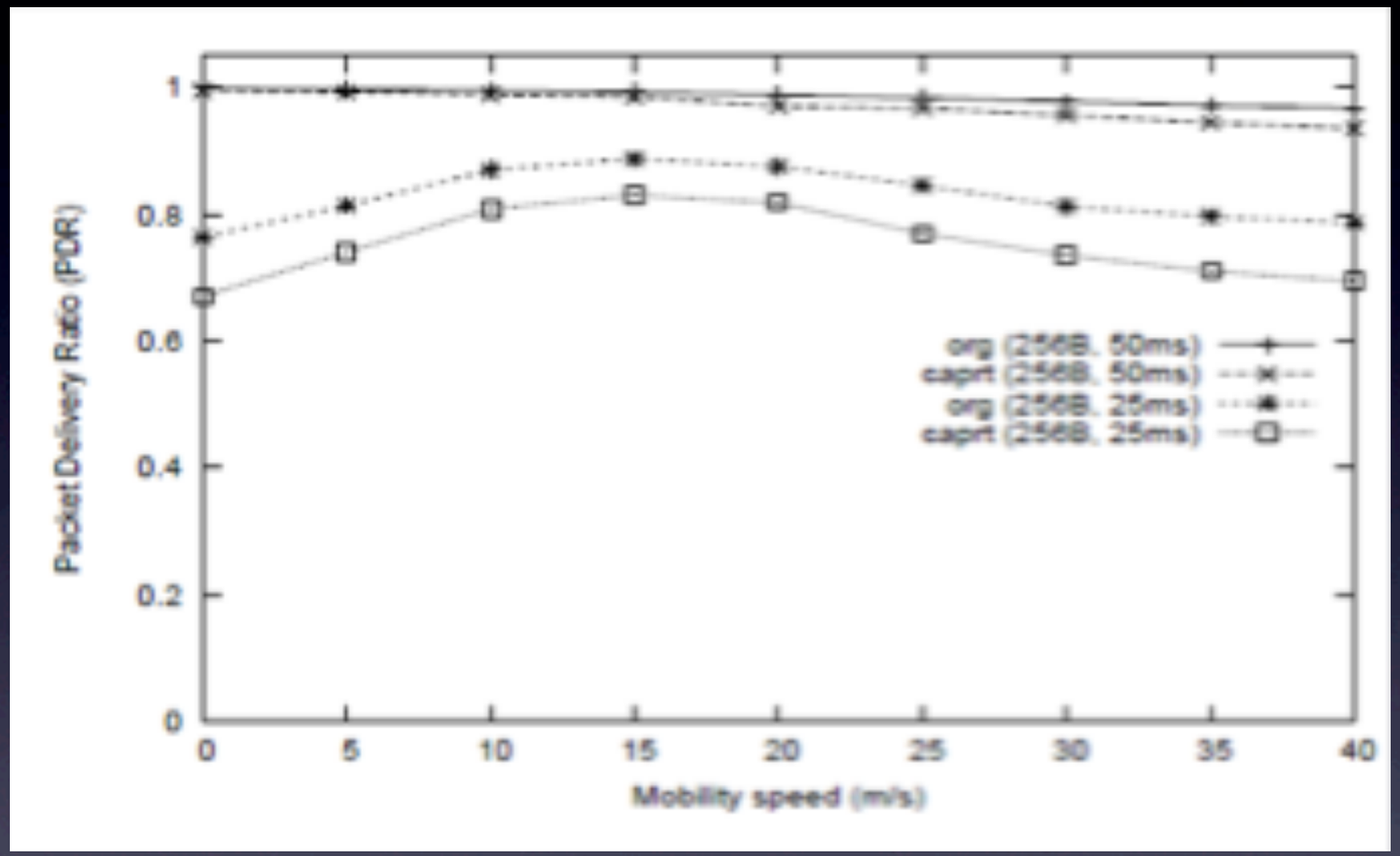
Route Change



- Line topology
- CBR 512 B, 1000 pkts
- Path length: 3
- Route change at 0.5 S

- Original Drops: 108mS worth of traffic
- Our scheme: 155mS

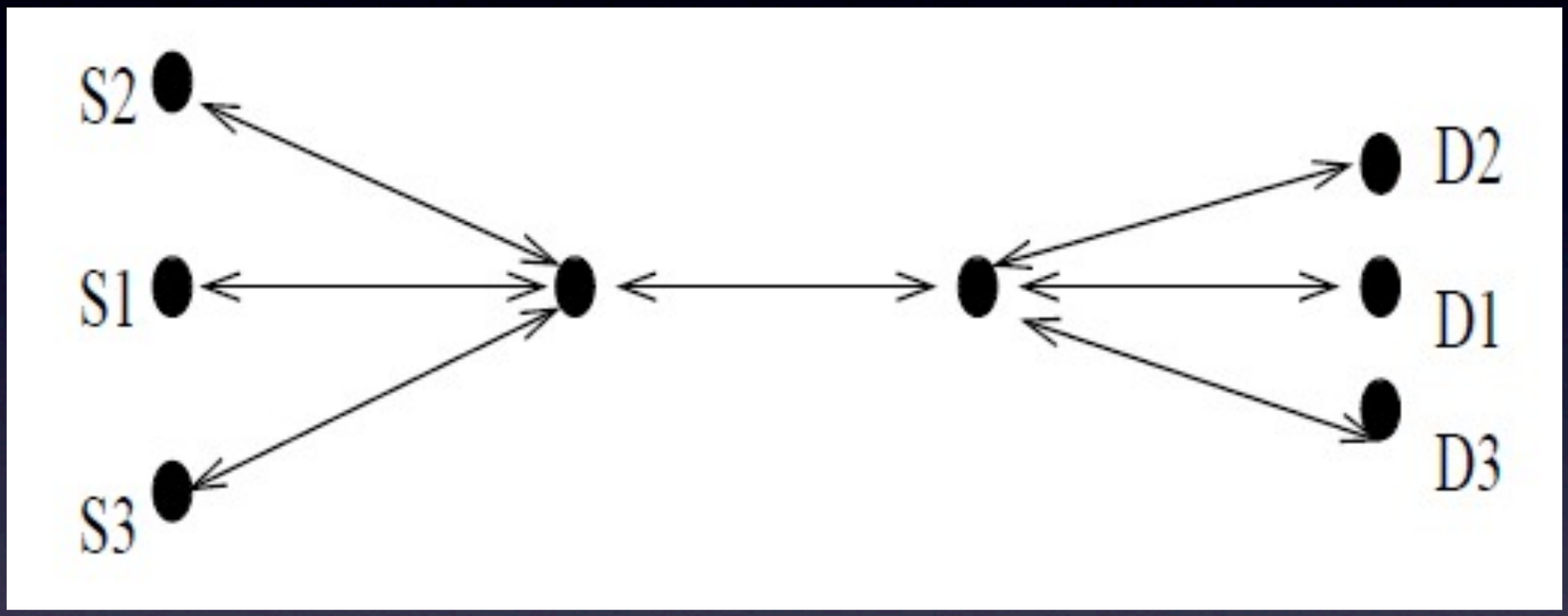
Mobility on Grid



- Random topology: 50 nodes, 1200x1200m grid
- CBR 256 B
- 5 pairs of traffic
- Random way point mobility

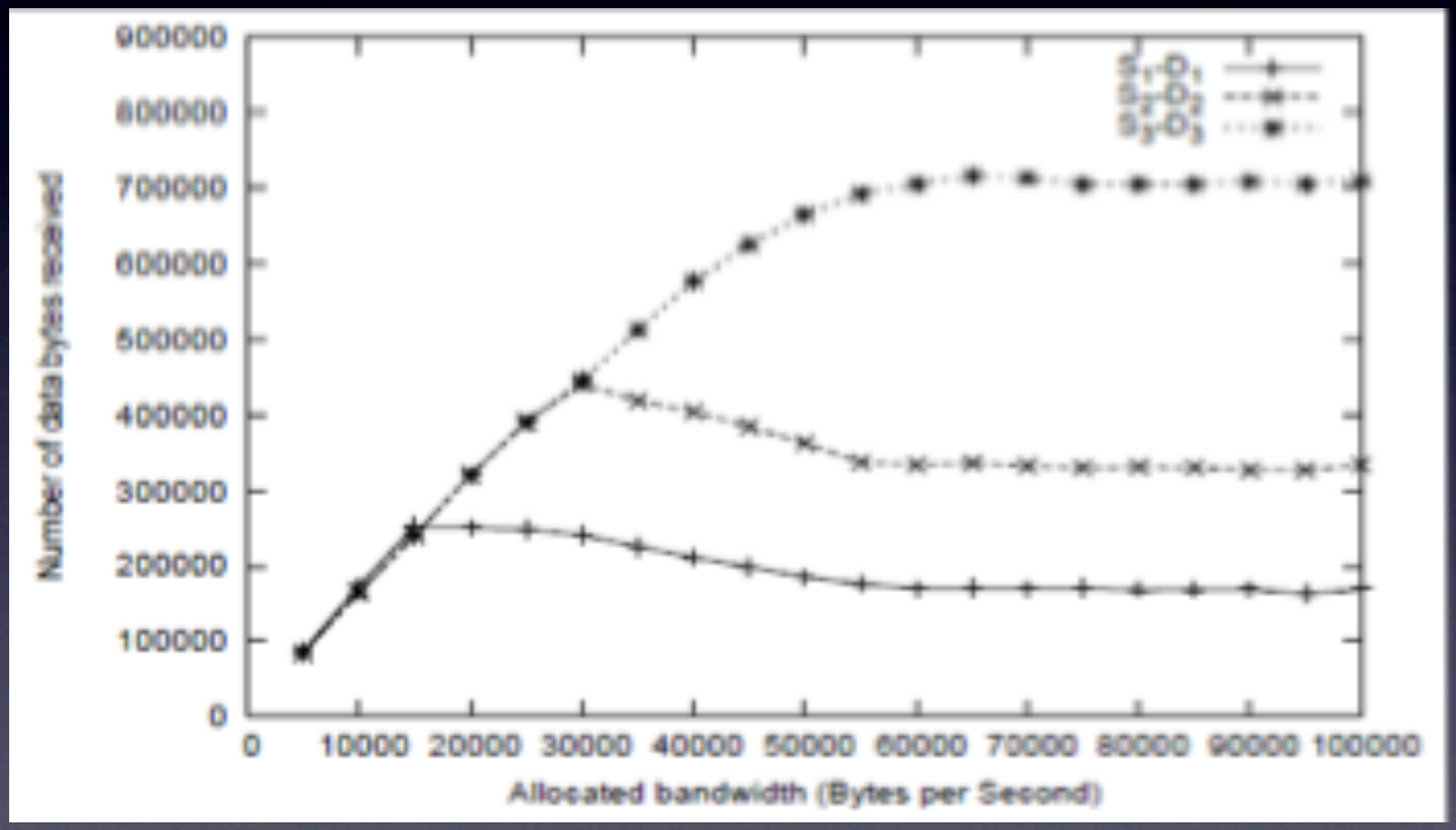
- PDR overhead: 1.6% (50mS), 9.14(25mS) lower for our scheme

Resilience against misbehaving nodes



- S1-D1: CBR 512B, 40mS
- S2-D2: CBR 512B, 20mS
- S3-D3: CBR 512B, 10mS

Resilience against misbehaving nodes



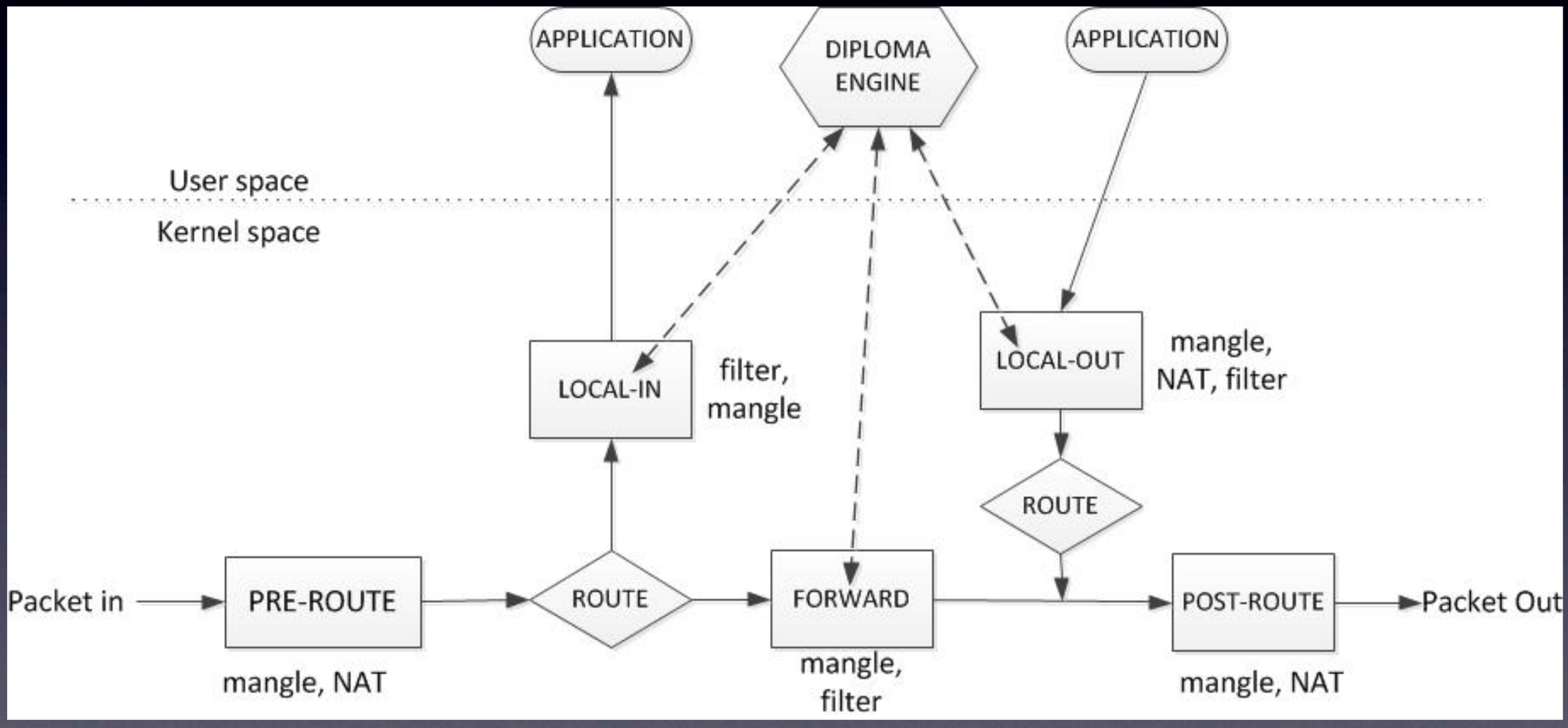
Orbit Lab

- 400 nodes with 802.11 radios
  - 20x20 grid, node 1 m apart
- 2 node sandboxes for testing
- Framework to install and save the images
- Ruby scripts to install, run experiments
- Multi-hop achieved through MAC filtering

Linux Implementation

- Without changes to any application
- Implementation using netfilter queue
  - iptables gives the packet to user level daemon
- Outgoing Packet
  - Establish capability if first packet
  - Add transaction id, seq. number, signature
- Transit Packet → Validate the packet
- Received Packet
  - Packet verification
  - Strip the capability headers
- Change MTU size to avoid fragmentation

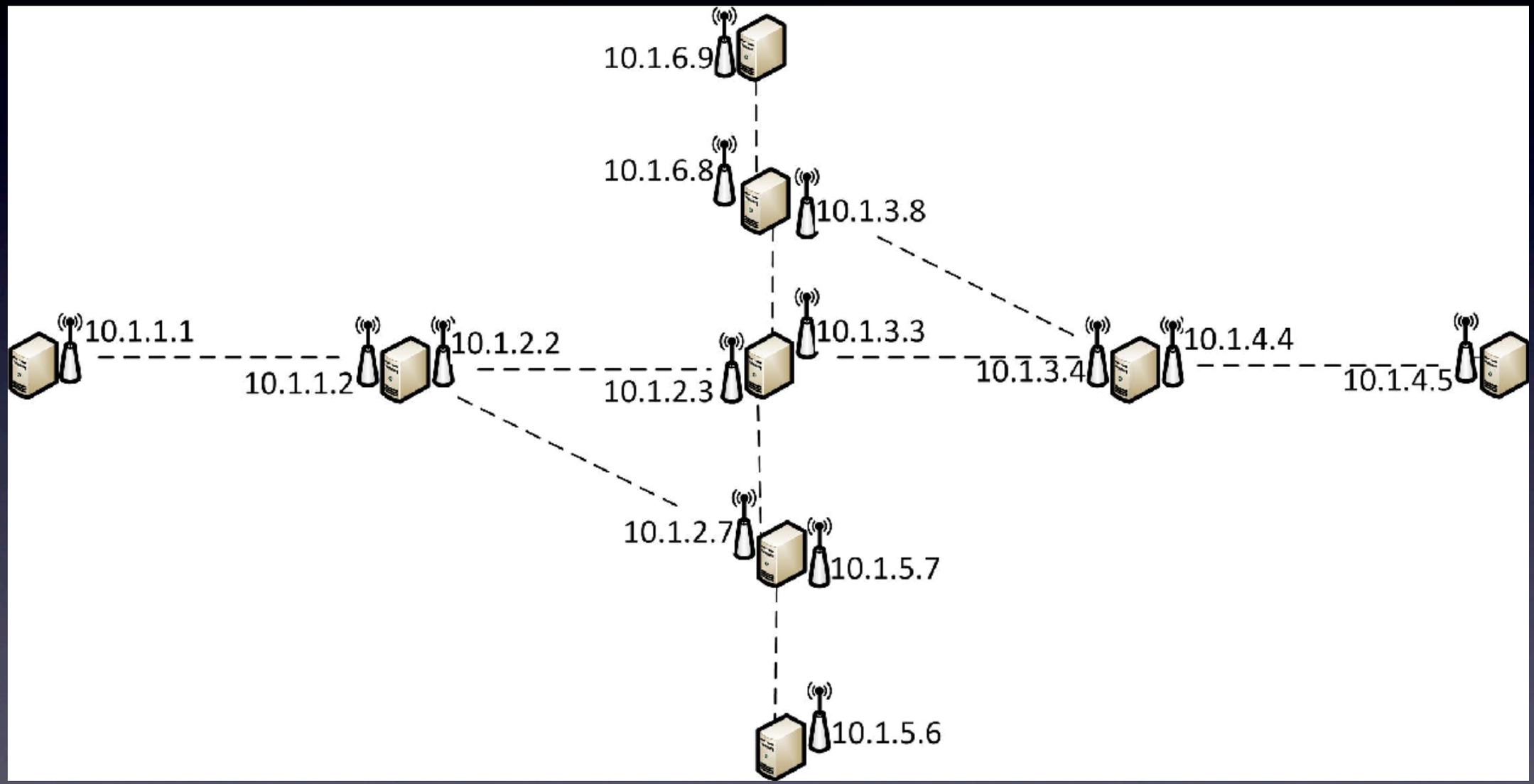
Implementation



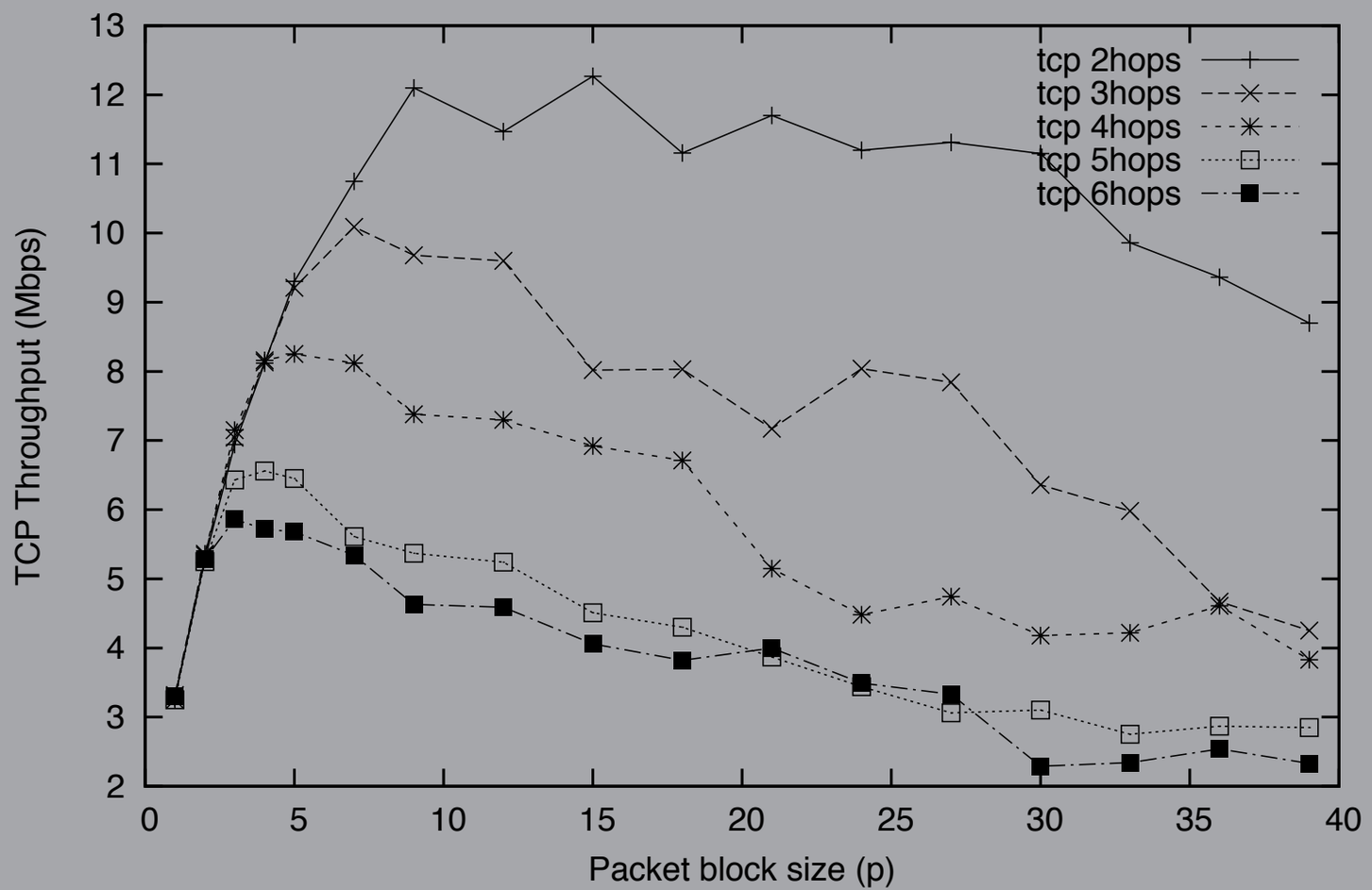
Orbit Lab

- 400 nodes with 802.11 radios
  - 20x20 grid, node 1 m apart
- 2 node sandboxes for testing
- Framework to install and save the images
- Ruby scripts to install, run experiments
- Multi-hop achieved through MAC filtering

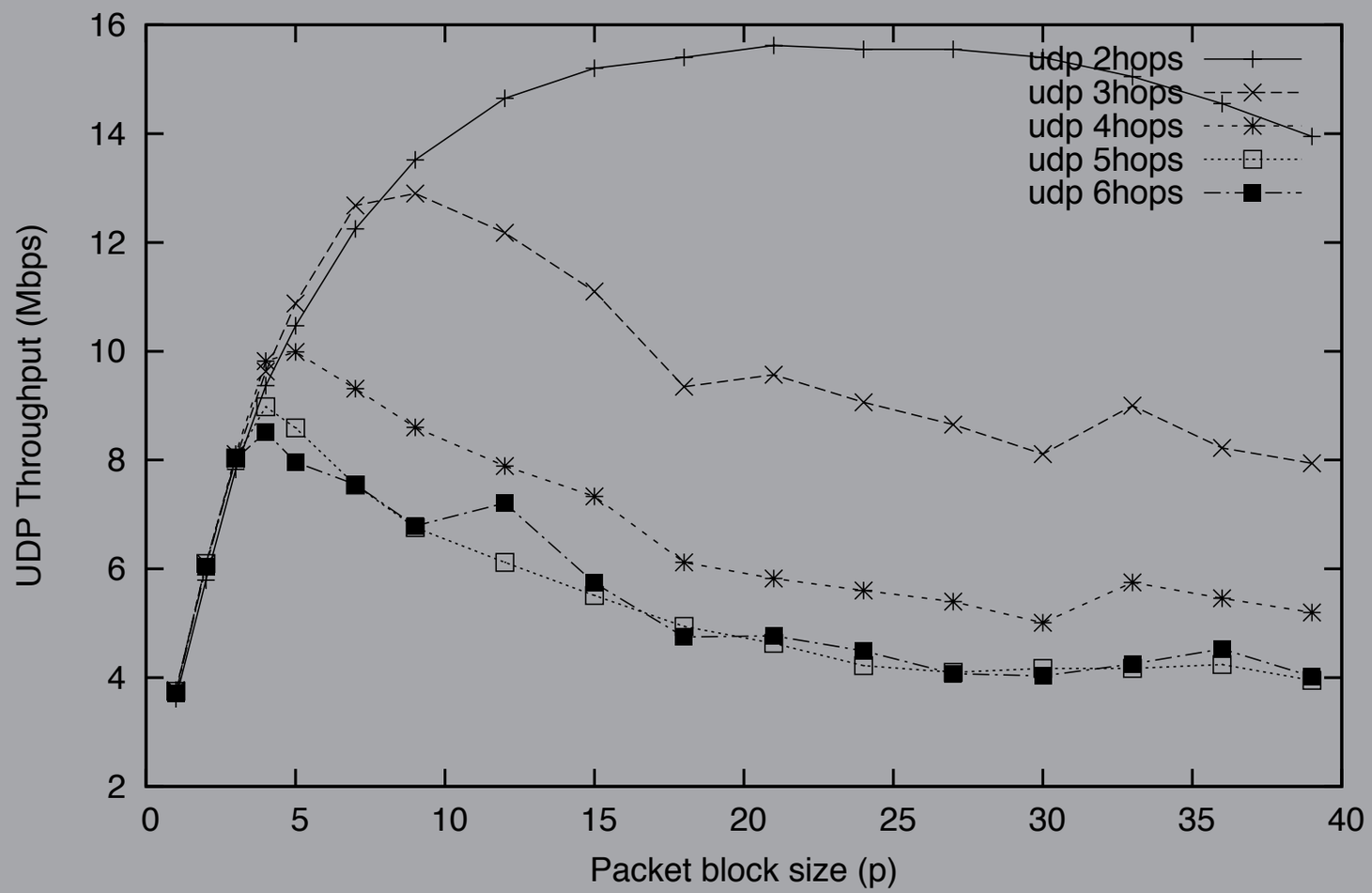
Topology


10.1.6.9
10.1.6.8
10.1.3.8
10.1.1.1
10.1.1.2
10.1.2.2
10.1.2.3
10.1.3.3
10.1.3.4
10.1.4.4
10.1.4.5
10.1.2.7
10.1.5.7
10.1.5.6

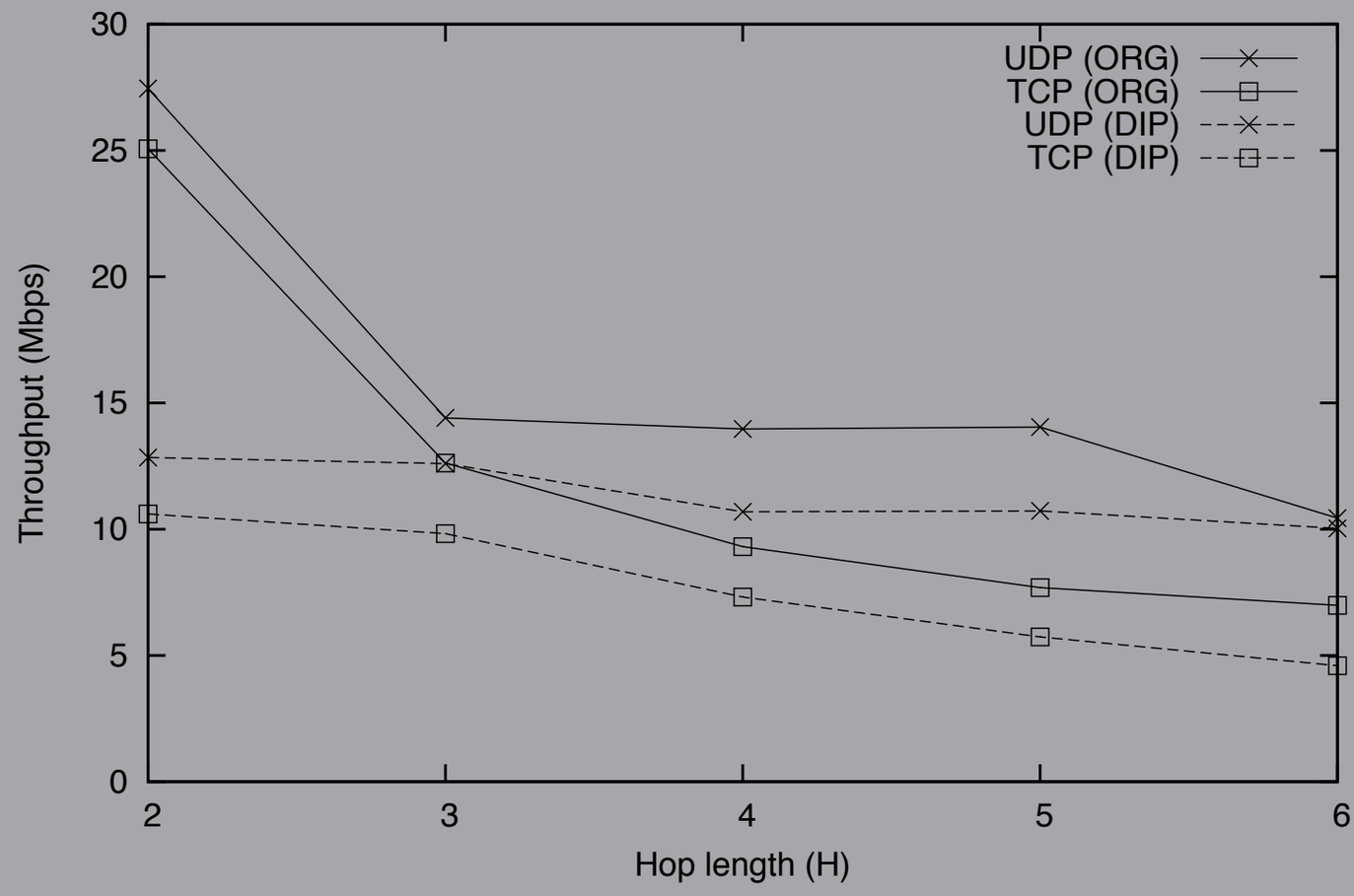
TCP throughput



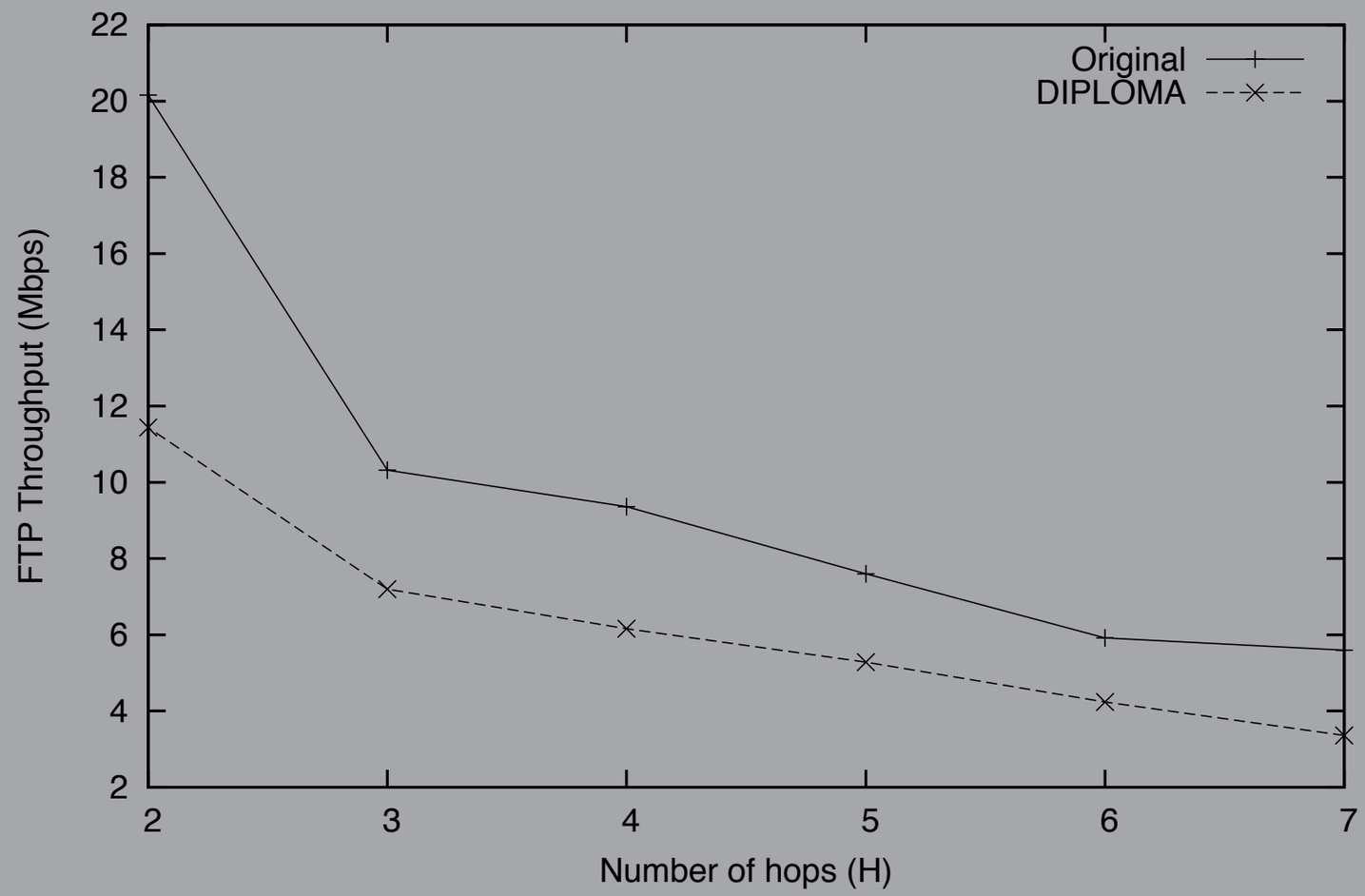
UDP throughput



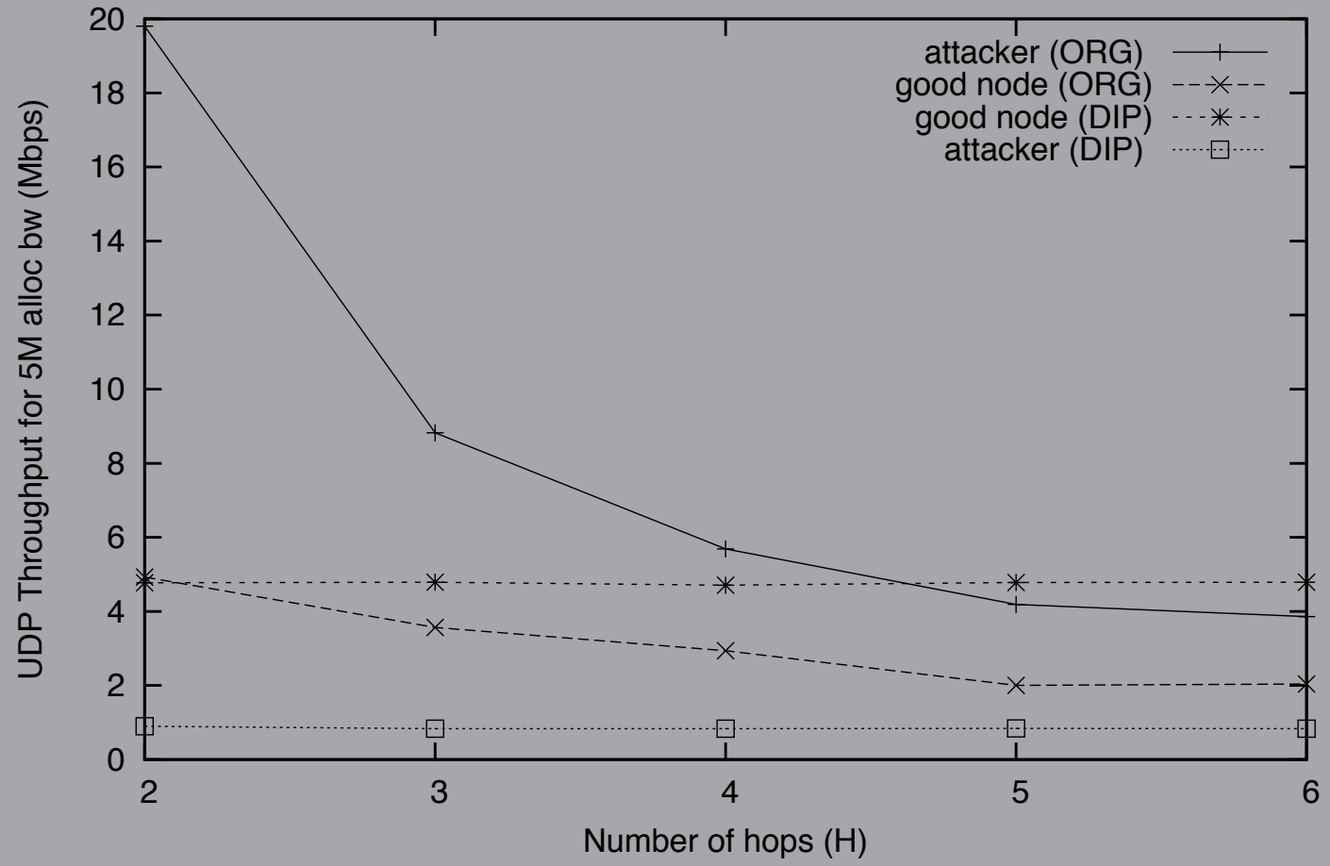
Throughput


UDP (ORG)
TCP (ORG)
UDP (DIP)
TCP (DIP)
Throughput (Mbps)
Hop length (H)
0
5
10
15
20
25
30
2
3
4
5
6

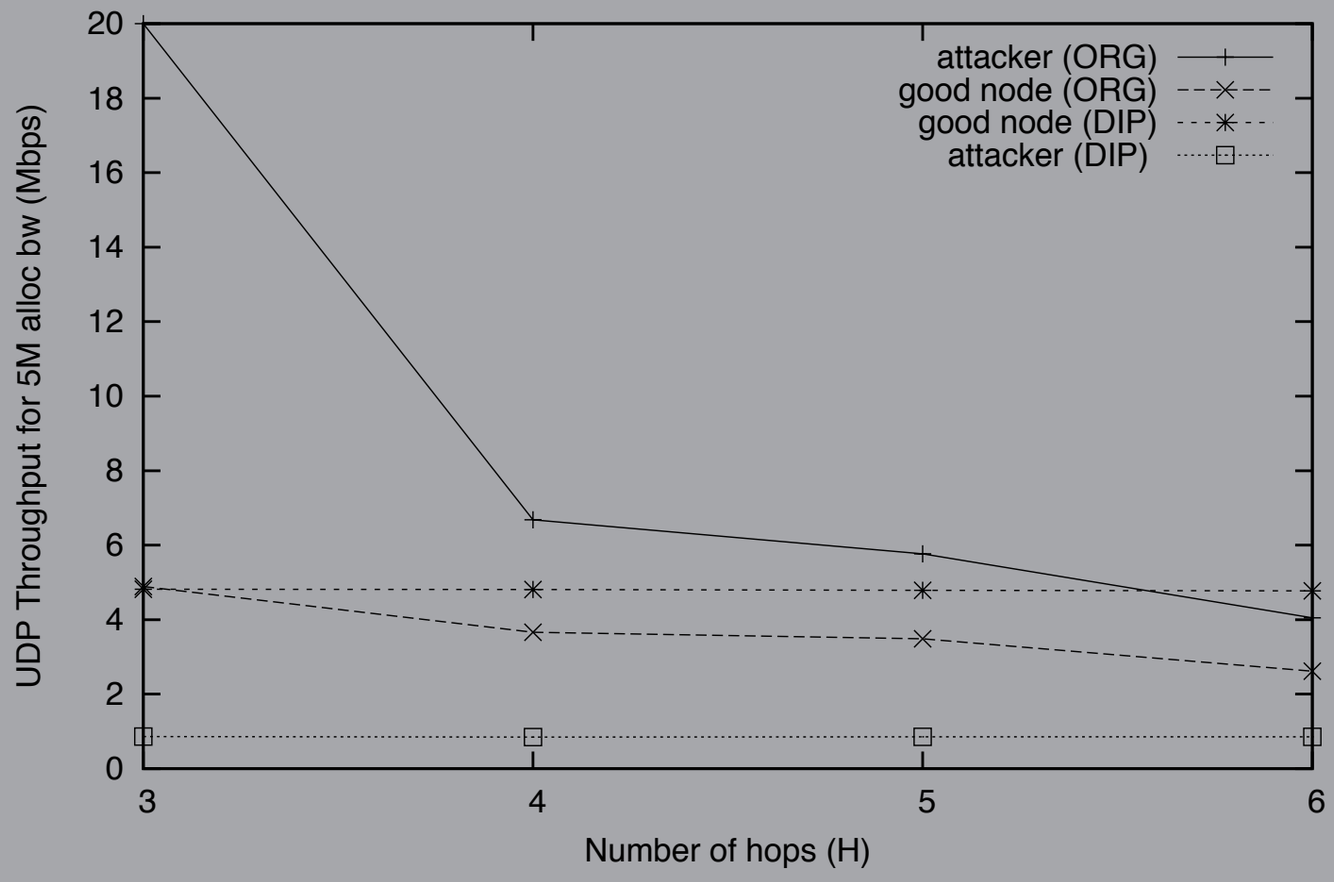
FTP throughput



Attack resilience (local attacker)



Attack resilience (distant attacker)



Other experiments

- Similar experiments for multicast
  - different topologies, streaming audio/video applications
- Capability misuse detection based on distributed auditing

- However, static topologies
  - challenge: introducting (experimenting with) realistic mobility
    - mechanism? model?
- What about policy generation?

Summary

- MANETs are an interesting problem domain
  - resource constraints, trust model, operational environment
  - clean-slate vs. add-on security?
  - realistic experimentation is challenging