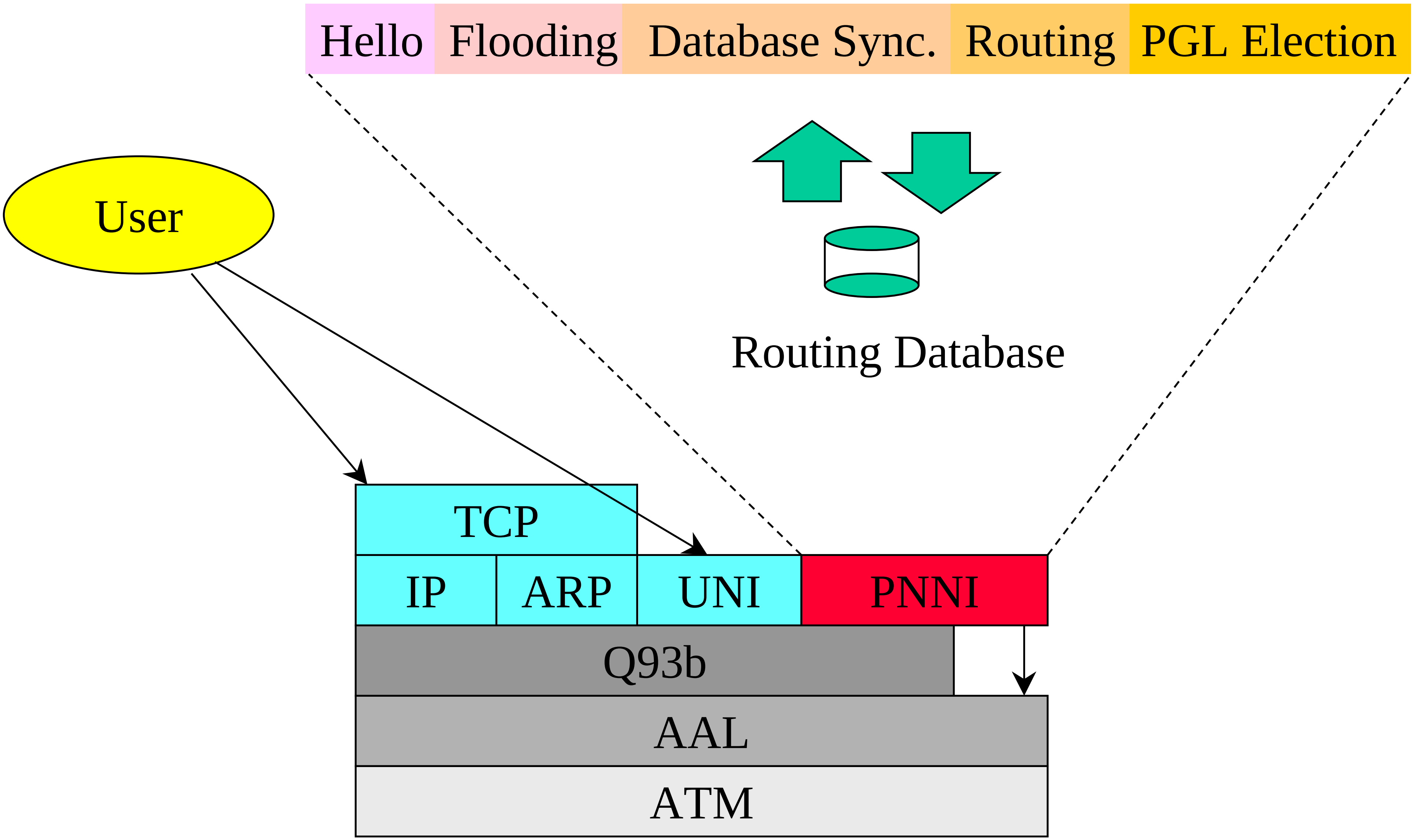
PNNI Global Routing Infrastructure Protection (PGRIP)

Livio Ricciulli, Pierangela Samarati,
Sabrina Di Vimercati, Patrick Lincoln



Hello Flooding Database Sync. Routing PGL Election

User

Routing Database

TCP

IP ARP UNI PNNI

Q93b

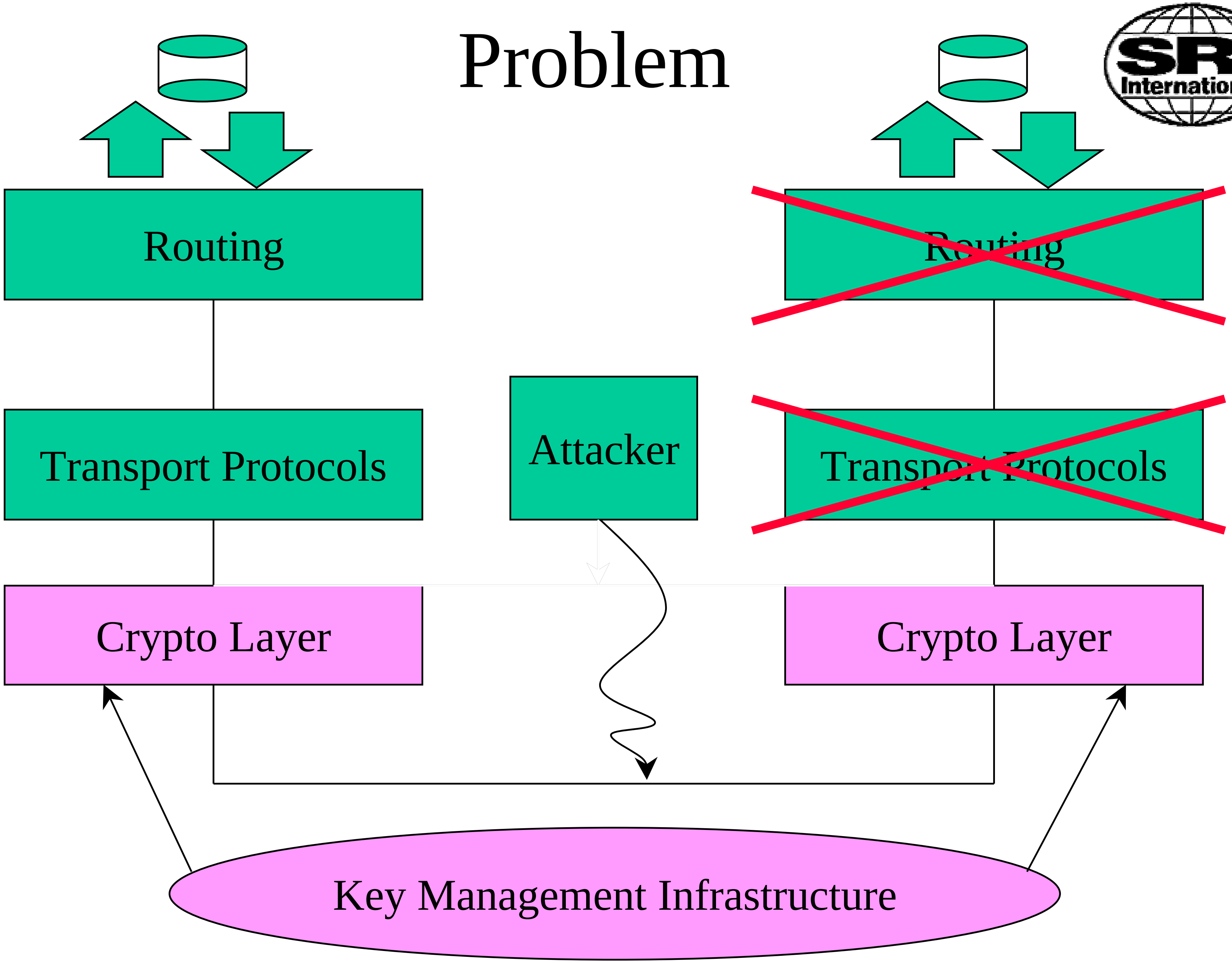
AAL

ATM

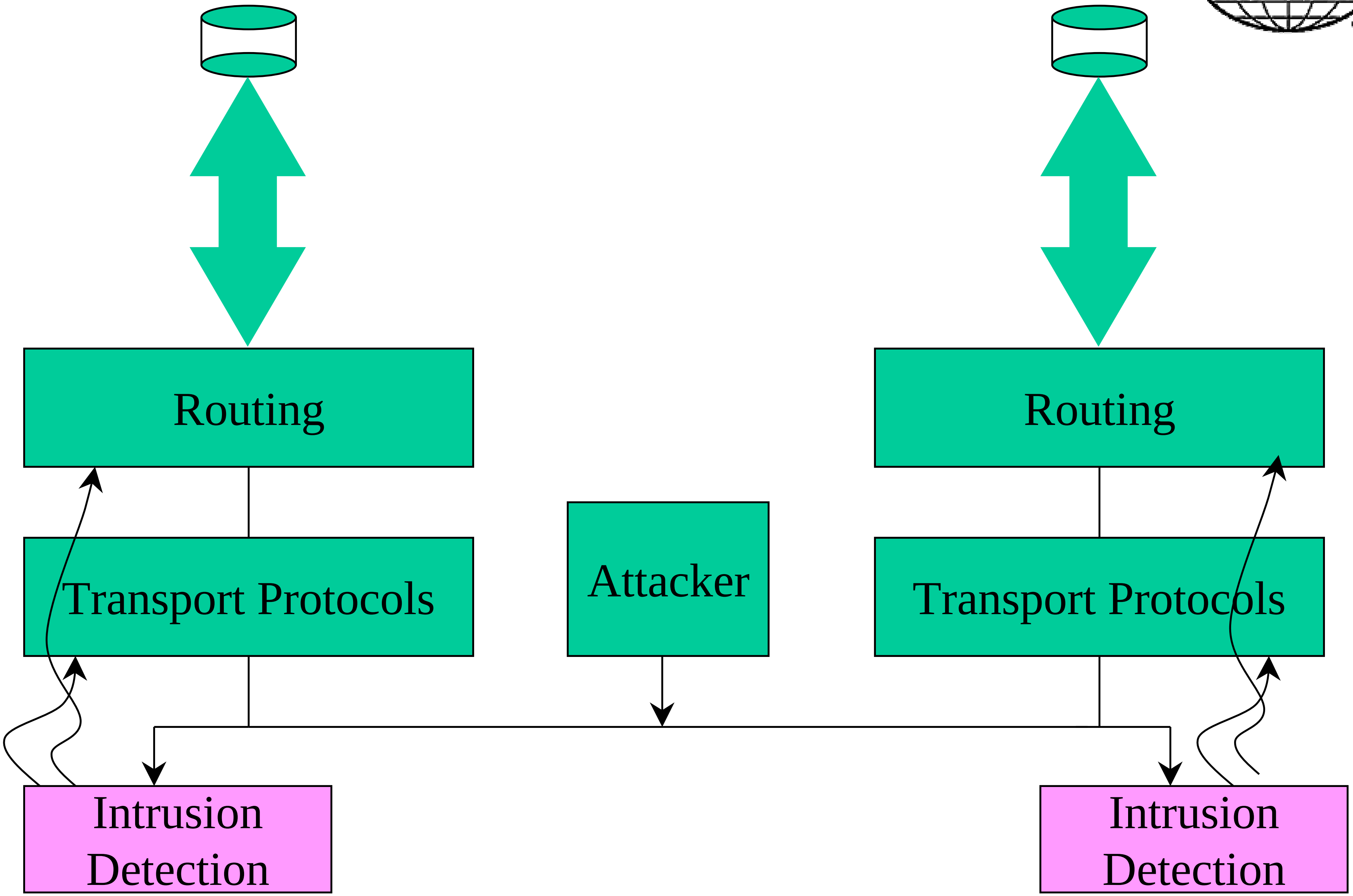
AAL=ATM Adaptation Layer

PNNI=Private-Network Network Interface

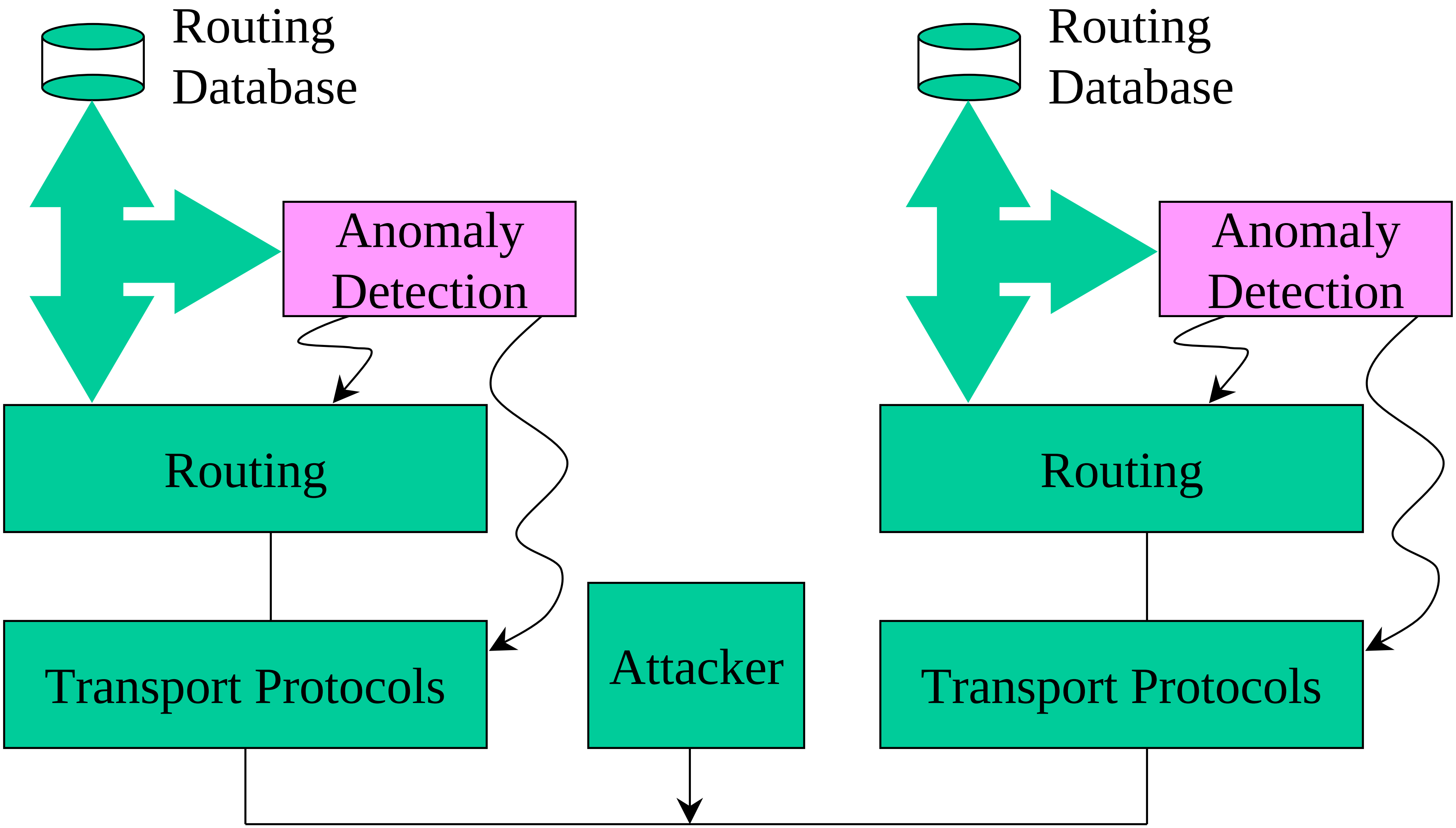
Problem


Routing
Transport Protocols
Crypto Layer
Attacker
Routing
Transport Protocols
Crypto Layer
Key Management Infrastructure

Intrusion Detection



PGRIP’s Anomaly Detection


Routing Database

Anomaly Detection

Routing

Transport Protocols

Attacker

Routing Database

Anomaly Detection

Routing

Transport Protocols

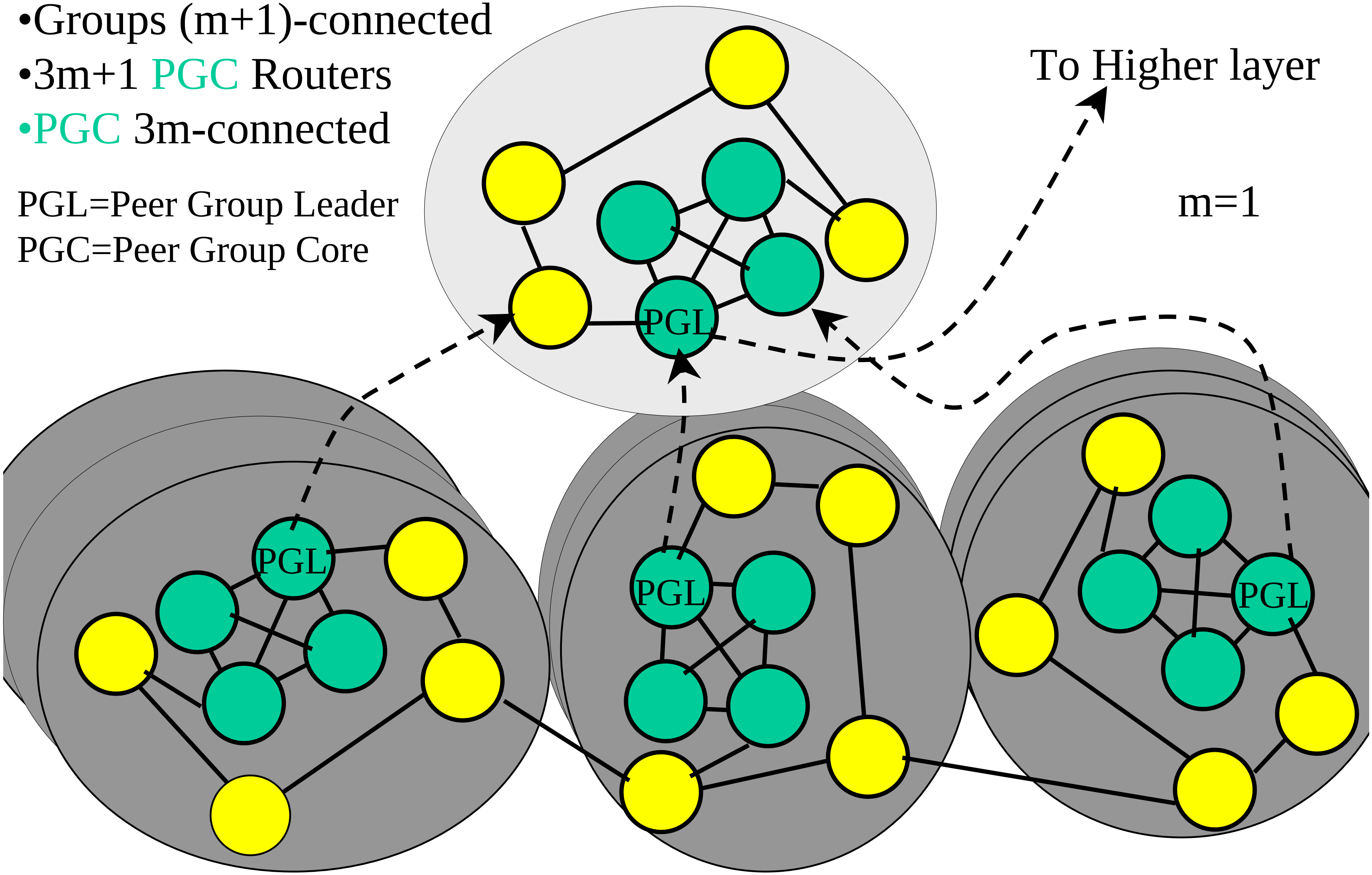
Advantages

- Higher level abstraction
- More portable
- Reactive rather than preventive
- Cryptographic layer optional
- Handle spontaneous and Byzantine faults in a unified manner

PGRIP's System-level Design

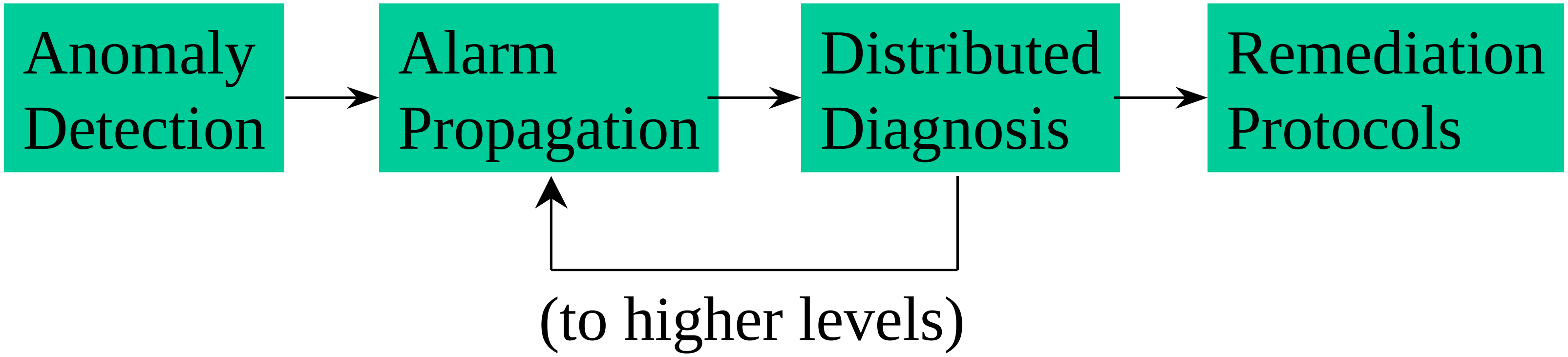
- •Groups (m+1)-connected
- •3m+1 PGC Routers
- •PGC 3m-connected

PGL=Peer Group Leader
PGC=Peer Group Core



PGRIP's Node Level Architecture

- Allow to express anomalies without knowledge of protocols
- Filter and delegate alarms
- Interactive Consistency protocol to increase resilience
- Fix problems in a reactive manner


Anomaly Detection

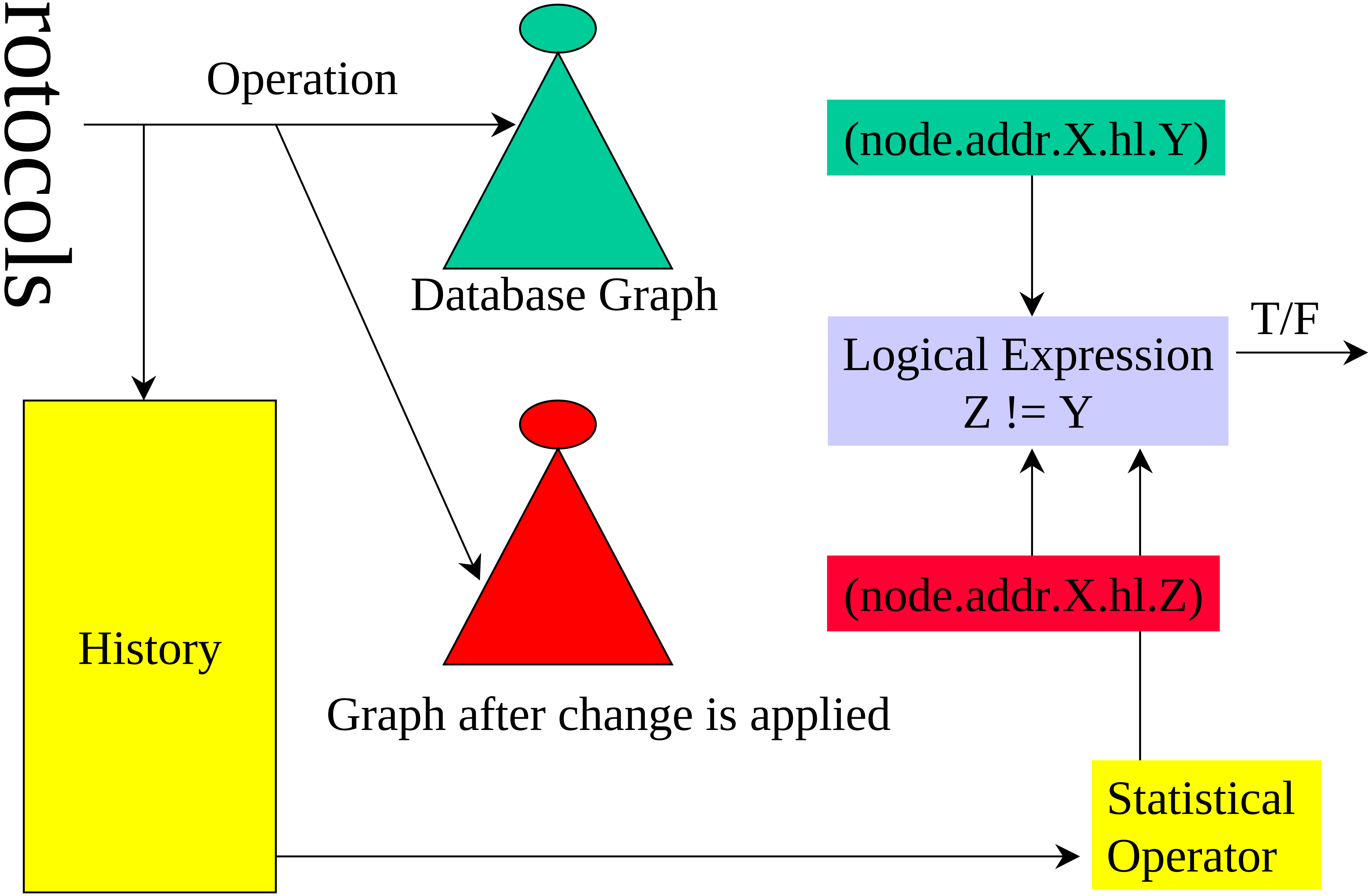
Alarm Propagation

Distributed Diagnosis

Remediation Protocols

(to higher levels)

Anomaly Detection



Protocols

Operation

Database Graph

Graph after change is applied

History

(node.addr.X.hl.Y)

Logical Expression
Z != Y

T/F

(node.addr.X.hl.Z)

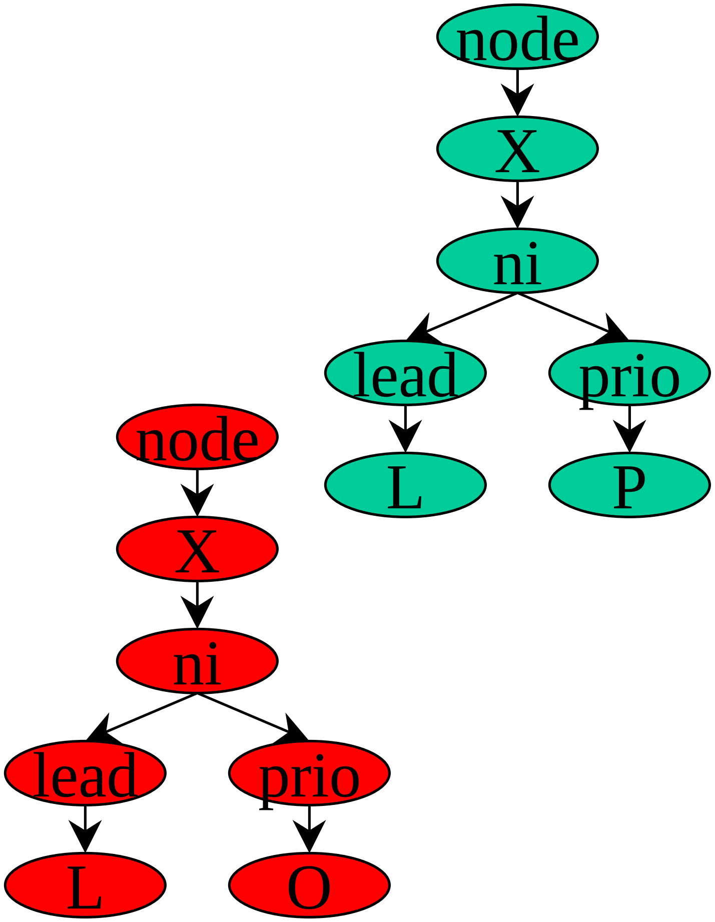
Statistical
Operator

Rules

- Operation
  - Add(path_exp), Update(path_exp), Delete(path_exp)
- State
  - path_exp + statistical info
- Condition
  - Logical expression
- Alarm
  - Unique anomaly identifier

Path Expressions and Conditions

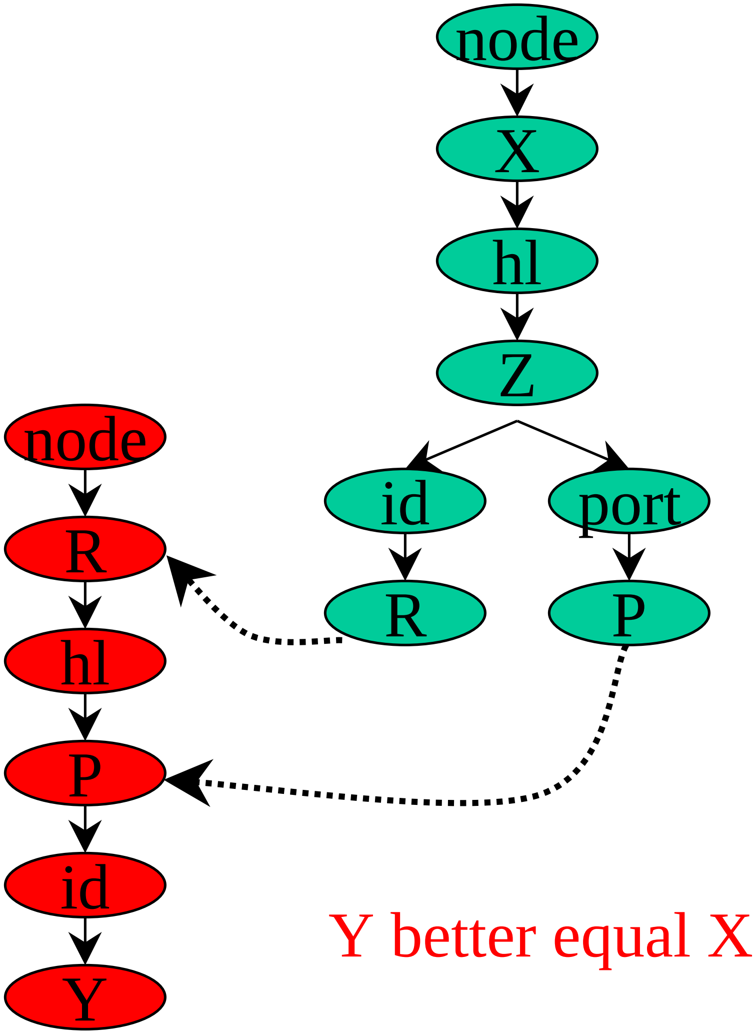
- Operation
  - – Update(node.X.ni)
  - – node.X.ni.priority.P
  - – node.X.ni.leader.L
- State
  - – node.X.ni.priority.O
  - – node.X.ni.leader.L
- condition
  - – P≠O



If X does not change leadership status, changing its priority is anomalous

Path Expressions and Conditions

- Operation
  - – Update(node.X.hl.Z)
  - – node.X.hl.Z.id.R
  - – node.X.hl.Z.port.P
- State
  - – node.R.hl.P.id.Y
- condition
  - – Y≠X



Y better equal X!

R knows that: My port P is connected to Y

X says: I am connected to port P of node R

Alarm Propagation

1. Always filter and log alarm
2. Pass alarm to diagnosing module
3. If we do not know how to diagnose, pass alarm up in the routing hierarchy

Diagnosing Module

- Each PGC router receives same alarms
- Each PGC performs diagnosis independently
- After the diagnosis, the PGC routers use an interactive consistency protocol to agree on result (conclusion is guaranteed).
- If no useful diagnosis is reached, give alarm back to alarm propagation module
- If we found the fault pass fault to resolver

Resolver Module

- Use some mechanism to fix fault
  - If there is a bad router, preempt it
    - PGC routers sign and propagate preemption packets
    - If at least 3m core routers preempt X, delete X from the database and discard all packets coming from X
  - If there is a suspicion that X lied, ask X's neighbors to synchronize their database
    - Turn on cryptographic mechanism to verify integrity of information
    - If do not have cryptography, make sure route does not go through X

Conclusion and Future Work

- Design is very scalable and robust
- Fault tolerance principles are useful and should be exploited more
- Expand this work to non-ATM routing and pursue inter-operation
- Implement anomaly detection module and formulate and deploy some useful rules
- Research on Byzantine fault diagnosis
- Design robust reconfiguration protocols to repair routing faults