Securing the Nimrod Routing Architecture

Karen Sirois and Stephen Kent
BBN Corporation

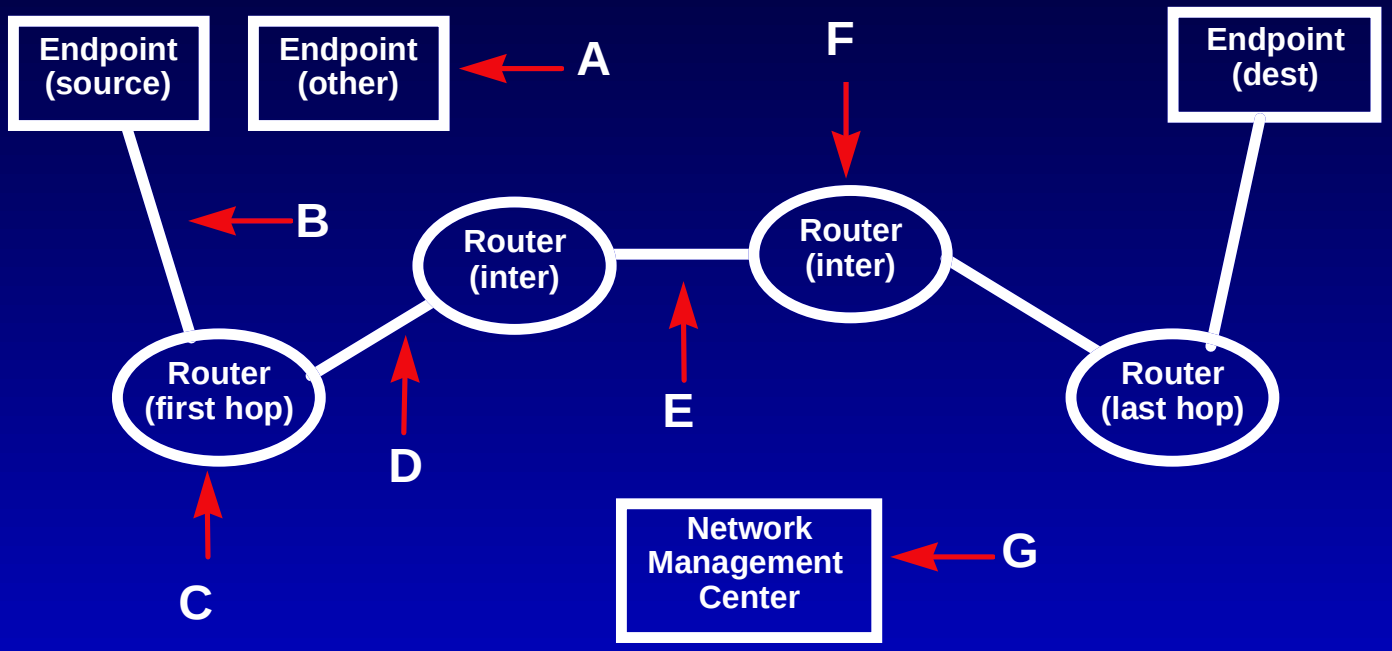
Outline

- Analysis methodology
- Points of attack
- Nimrod routing architecture
- Nimrod security requirements
- Countermeasure design for Nimrod

Analysis Methodology

- Security focus: countering denial of service attacks
- Identify architectural elements
- Derive requirements using a hybrid approach
  - correct operation scenarios
  - attack driven
  - countermeasure driven
- Base countermeasures on security requirements, Nimrod protocols and available mechanisms

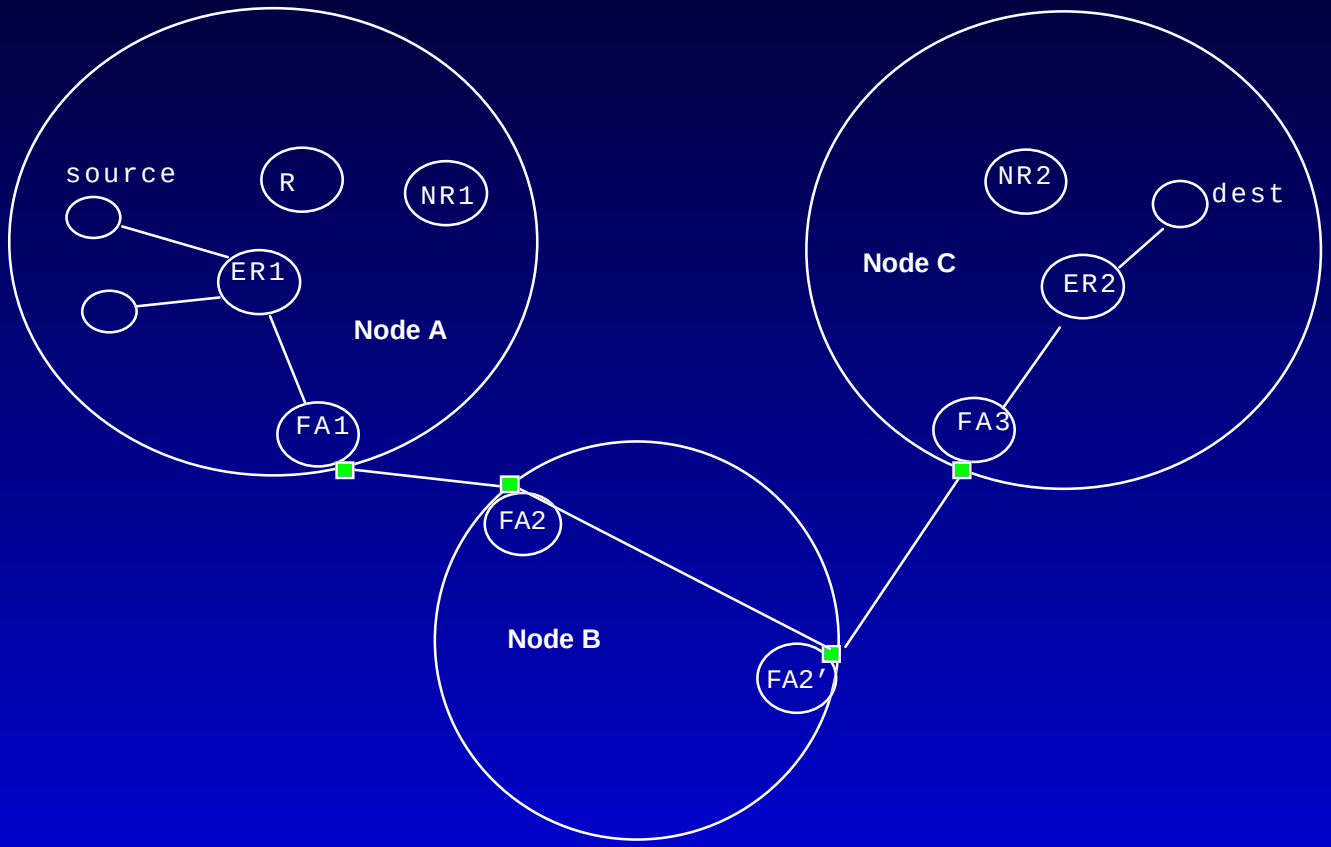
Points of Attack



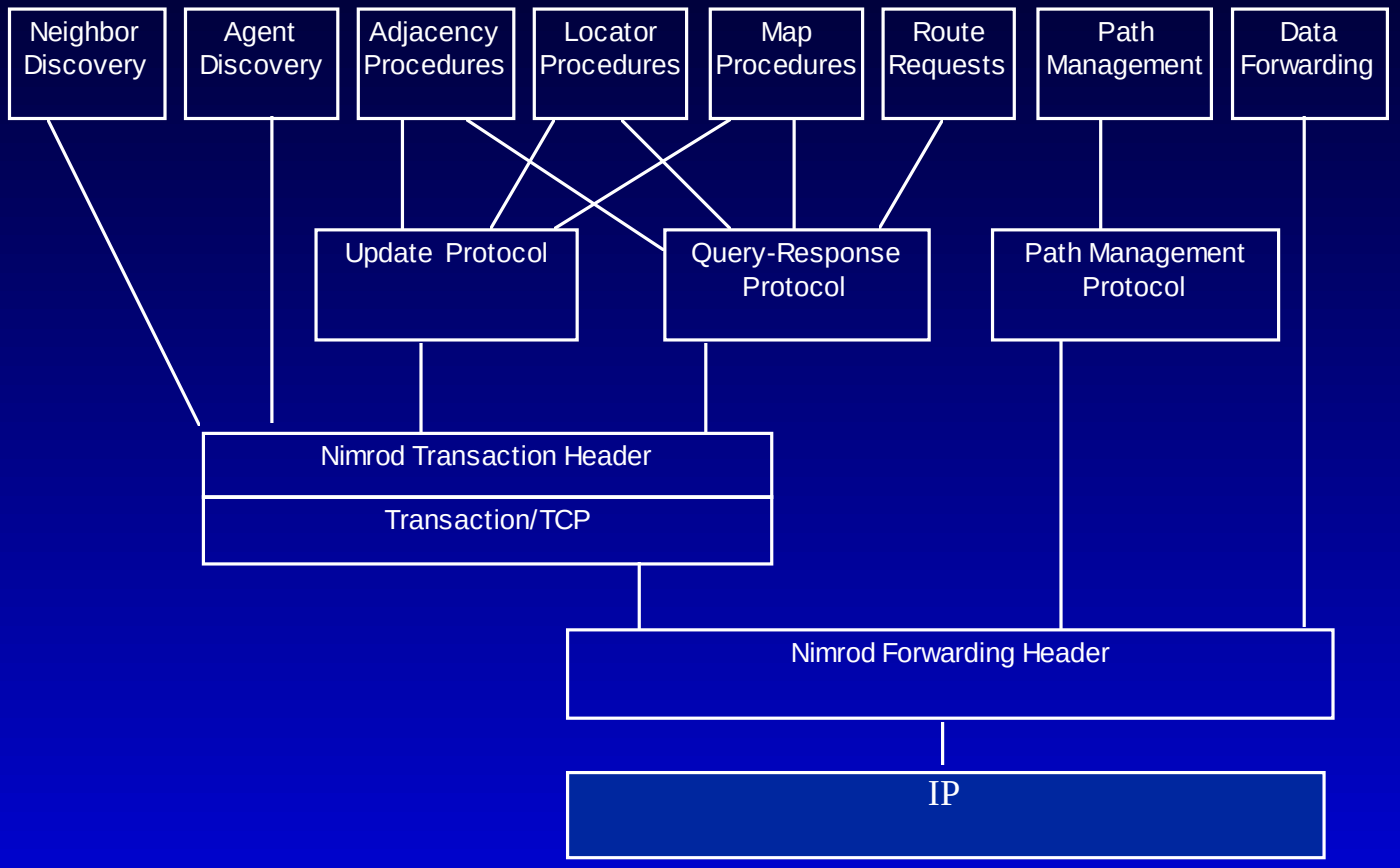
Nimrod Routing Architecture

- Service specific routing
- Scaleable architecture
- Basic entities
  - nodes: comprised of agents
  - endpoints
- Distributed databases
- Link state maps
  - produced locally (by each node)
  - restricted distribution

Forwarding Example



Nimrod Protocol Structure



Nimrod Security Requirements

security service / protocol	Data Origin Authentication	Peer Entity Authentication	Rule-Based Access Control	identity-Based Access Control	Connectionless Integrity	Sequence Integrity	Confidentiality	Non-Repudiation
Neighbor Discovery	X				X	X		
Agent Discovery	X				X	X		
Locator Procedures	X			X	X	X	X*	
Map Procedures	X				X	X	X	X
Adjacency Procedures	X			X	X	X	X*	
Route Requests	X				X	X	X*	X
Data Forwarding	X				X	X		
Path Setup/Accept	X		X	X	X	X	X*	X
Path Teardown	X		X	X	X	X	X*	X
Path Status	X				X	X		
Path Ack	X				X	X		

Countermeasure Design

- IPSEC protection
- Digital signatures
- Timestamps
- Access control and non-repudiation

IPSEC protection

- IPSEC ESP with anti-replay (in tunnel mode)
  - provides authentication, integrity and replay protection.
  - uses keyed hash with windowed sequence numbers
  - requires (pairwise unique) shared secrets between neighboring agents
  - encryption optional, but not required
  - more efficient to compute and more inclusive than AH
- Employed to protect both neighbor discovery and subscriber traffic

Digital Signatures

- Provides multicast authentication and integrity on an “end-to-end” basis
- Useful for non-repudiation and access control
- Update, Agent Discovery and Path Management protocols as well as Query-Response protocol
- RSA signature algorithm and sha-1 hash algoithm
- Use X.509 (v3) certificates

Timestamps

- Provides anti-replay protection as well as ensuring message timeliness
- Timestamp window with saved hash values mechanism
- Increasing timestamp mechanism
- Clock adjustments

Access Control and Non-Repudiation

- Use identity-based access control
- Cache specific messages to support weak non-repudiation service

Summary

- Security requirements analysis for Nimrod was fairly complex
- Proposed countermeasures are a mixture of reliance on a lower layer security (IPSEC-ESP/AR) plus integration of Nimrod-specific measures, plus shared-secret establishment
- Our solution not a perfect one:
  - Byzantine attacks still pose hard problems, given real world performance requirements
  - this analysis and the proposed countermeasures don’t address many implementation vulnerabilities