SAND2008-7788C

MILCOM 08
ASSURING MISSION SUCCESS

Requirements and Architectures For Intrinsically Assurable Mobile Ad Hoc Networks (IAMANETs)

Scott Alexander
Telcordia
Piscataway, NJ

Brian DeCleene
BAE Systems
Burlington, MA

Jason Rogers
Naval Research Lab
Washington, DC

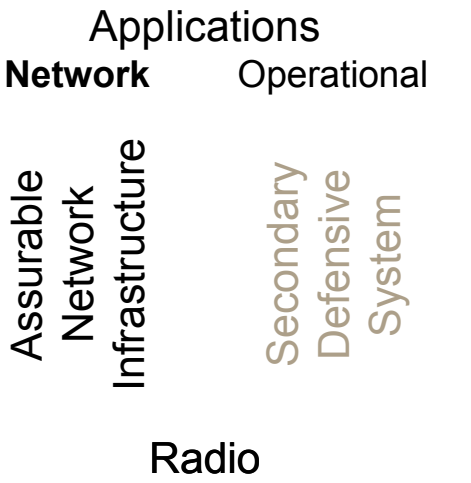
Peter Sholander
Sandia National Labs
Albuquerque, NM

San Diego, California
November 17–19, 2008

IAMANET Overview

- Goal: "Clean-slate" architecture to network security
  - *Address the root enablers of attacks (causes) rather than patch the holes (symptoms)*
  - *ANI : Build in intrinsic immunity to attack and increase visibility of adversary : Prevent*
  - *SDS : Execute targeted action against the adversary : Respond*
- Program demonstrating two approaches to rethinking our network infrastructure

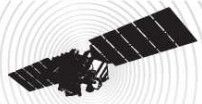
IP-based MANETs are vulnerable because original Internet design ignored information assurance



Internet design priorities

1. Multiplex existing networks	Most Important
2. Survive network/gateway loss	
3. Support multiple applications	
4. Support multiple networks	
5. Permit distributed management	
6. Be cost effective	Least Important (in practice, ignored)
7. Easy host attachment	
8. Resource accountability	

Metrics and Desired System Features



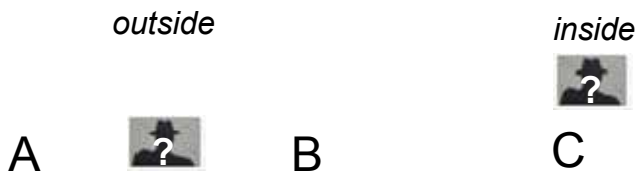
MILCOM:08
ASSURING MISSION SUCCESS

- **Desired System Features**
  - *Authenticate & Account for All Actions*
  - *Deny-by-Default*
  - *Byzantine Robustness to Insiders*
  - *Minimize Use of Trusted Hardware*
- **Metrics**
  - *Prevent attacks that negatively impact any 2-hop neighbors*
  - *Prevent exfiltration of operational information from the MANET*
  - *Perform as well as IP-based MANETs when both systems are not under attack*

AFCEA
IEEE COMMUNICATIONS SOCIETY
BAE SYSTEMS
Telcordia
Sandia National Laboratories

Threat Model

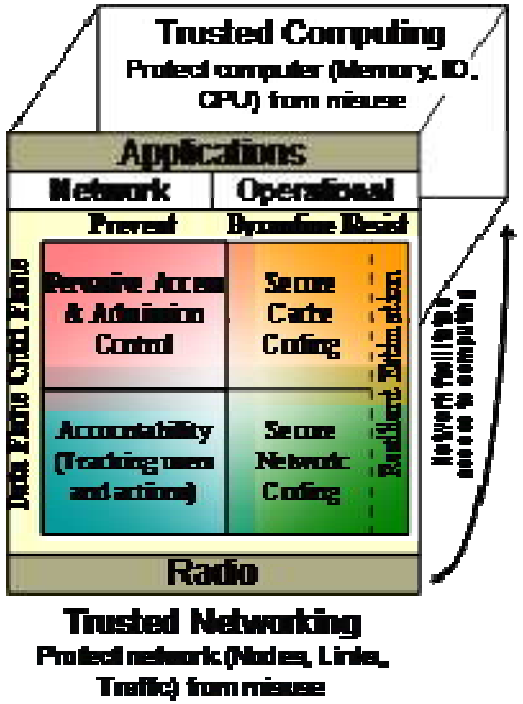
- High-Level Threat:
  - *Primary concern is cyberattack in the information domain.*
  - *IAMANET design should also consider social, physical, or cognitive threat domains.*
- Adversary capabilities in MANETs can be characterized based on:
  - *Wireless Channel*
    - *Receive/transmit any signal*
    - *Prevent any radio from transmitting or receiving*
  - *System Knowledge (full)*
  - *Physical Compromise (node capture)*
    - *Allows arbitrary behavior by an authenticated node.*
    - *Trusted hardware may limit access to some IAMANET APIs though.*



- Physical domain threats (damage/capture) and RF jamming are important for MANETs
  - *IP is robust against node/link loss*

Principles for Intrinsically Assurable Network Operation (PIANO)

- **System Model – Trusted Networking**
  - *Complementary to host-based security : Trusted Computing*
  - *Protect Network and Network Applications*
  - *Contain Attacks and Prevent Exfiltration, while Maintaining Network Performance*
- **Build a model for cooperative networking around core principles**
  - *Enabled by recent advances in network coding, signature schemes, peer-to-peer content distribution and line-rate policy enforcement*
  - *BAE-lead team includes CalTech, LGS, MIT, Stanford, Univ. of MA, Univ. of TX*



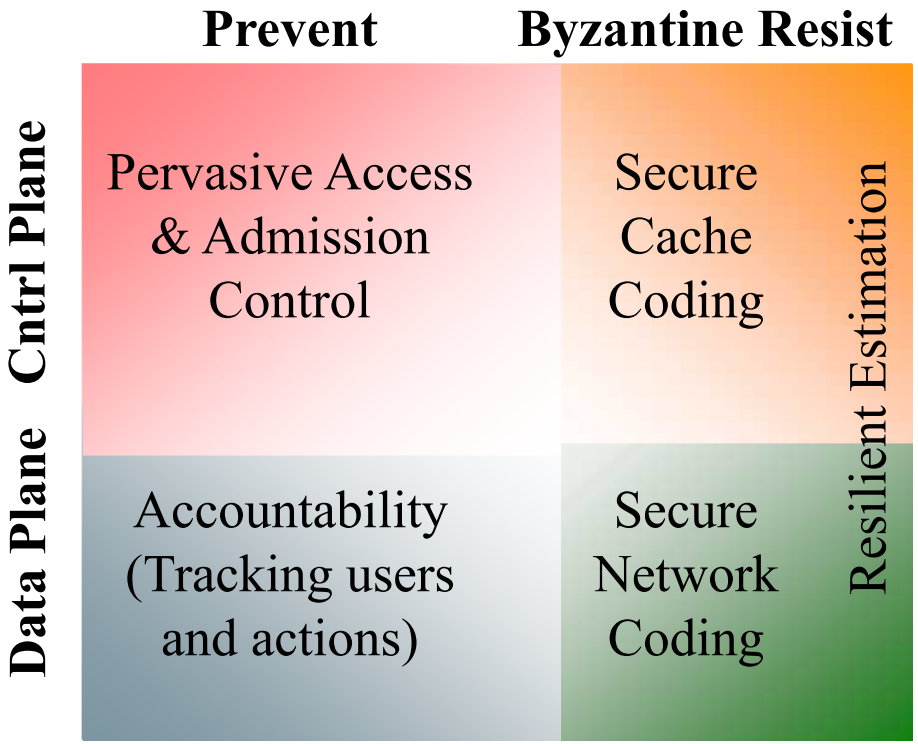
PIANO principles map to desired system features

PIANO's Core Principles

Deny-by-default access prevents unauthorized network use and control signaling. Protects network state info.

Strong Identity binding between network actors and traffic ensure accountability.

Data path parallelism with resistant coding ensures data delivery despite attacks.

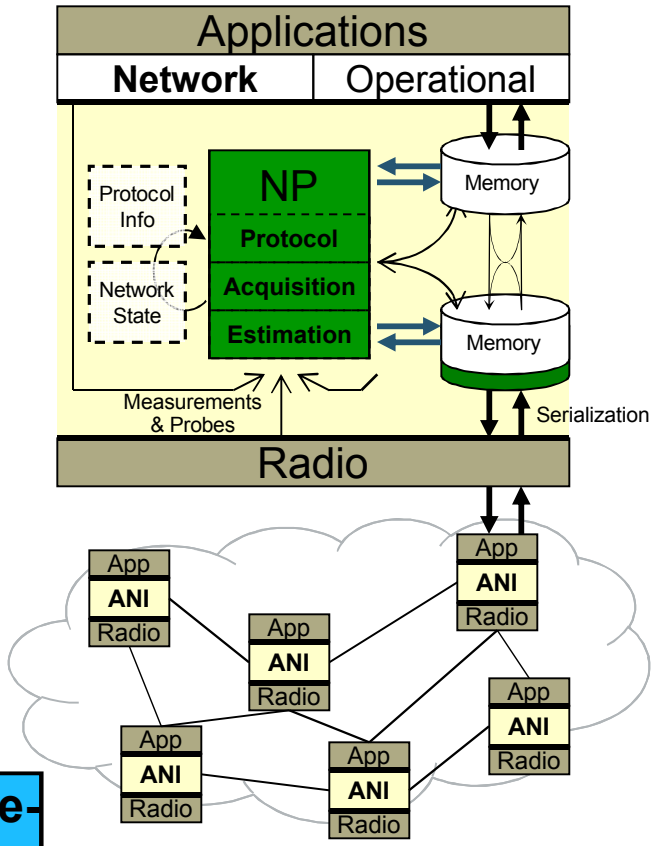


Account for adversary within local network estimation

Data path parallelism with resistant coding ensures data delivery despite attacks.

Current Network Node Model

- Network Protocol (NP) develops model of the relevant network conditions
  - Estimation: Measurements and probes used to estimate network characteristics like link quality or the onset of congestion
  - Acquisition: Control signaling used to share estimates of network characteristics with other nodes
- Protocol signaling based on perceived model of the network with state information
  - Signaling based on timers and "finite state"
  - Messages are assembled in open memory
  - Messages are serialized per a priori defined bit-format

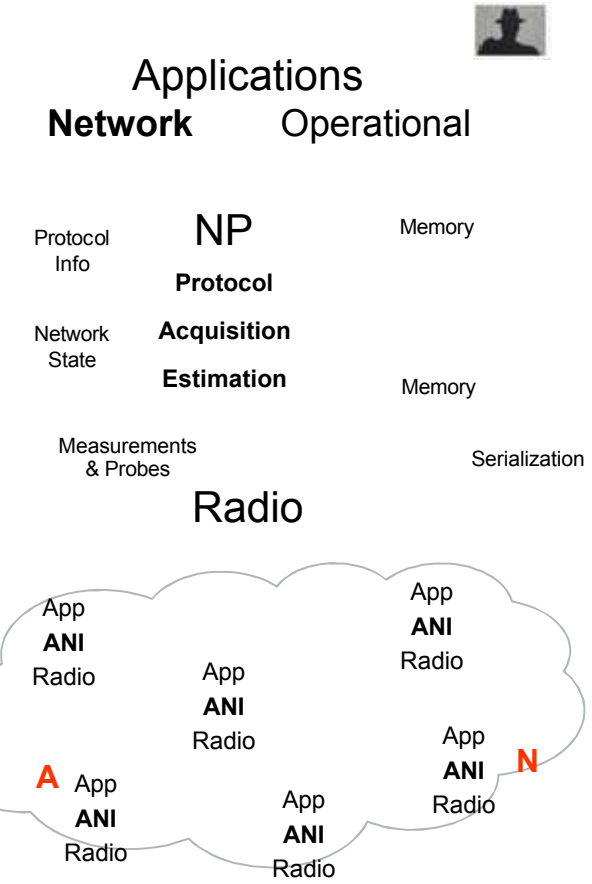


Let's examine vulnerabilities and PIANO's principle-based solutions

Vulnerability – Impersonation & Manipulation

MILCOM:08 ASSURING MISSION SUCCESS

- Adversary has unfettered access to memory where packet construction is occurring and subsequent radio for transmission
  - Impersonation: Construct “false” messages attributed to others
  - Packet Manipulation: Anonymously modify packets from others
- Trusted Computing Solution : Protect network memory and radio such that only trusted components can access



Attack Vector Notation

Adversary (Launch pt)

Node Vulnerability

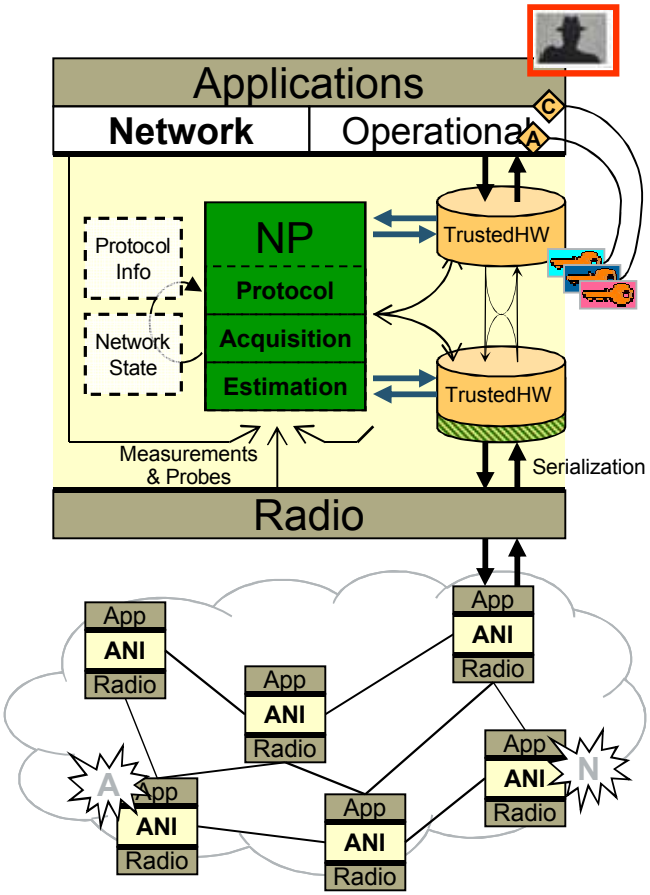
A Target

Traffic can be accessed and manipulated anonymously

Vulnerability – Impersonation & Manipulation

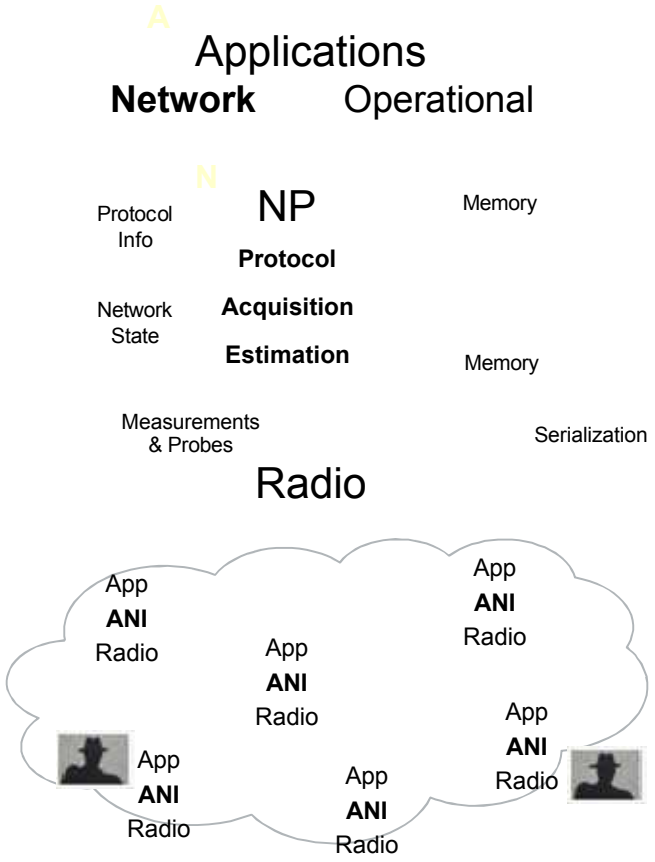
- Adversary has unfettered access to memory where packet construction is occurring and subsequent radio for transmission
  - Impersonation: Construct "false" messages attributed to others
  - Packet Manipulation: Anonymously modify packets from others
- PIANO Solution: Allow generic access to radio but enforce strong accountability → At least we know who to blame
  - Establish trusted area for packet construction
  - Anyone can construct/modify packets but they are accountable
  - Once extracted from trusted area, further modifications are prevented

Strong Identity and Trusted Hardware provide Accountability



Vulnerability - Exfiltration

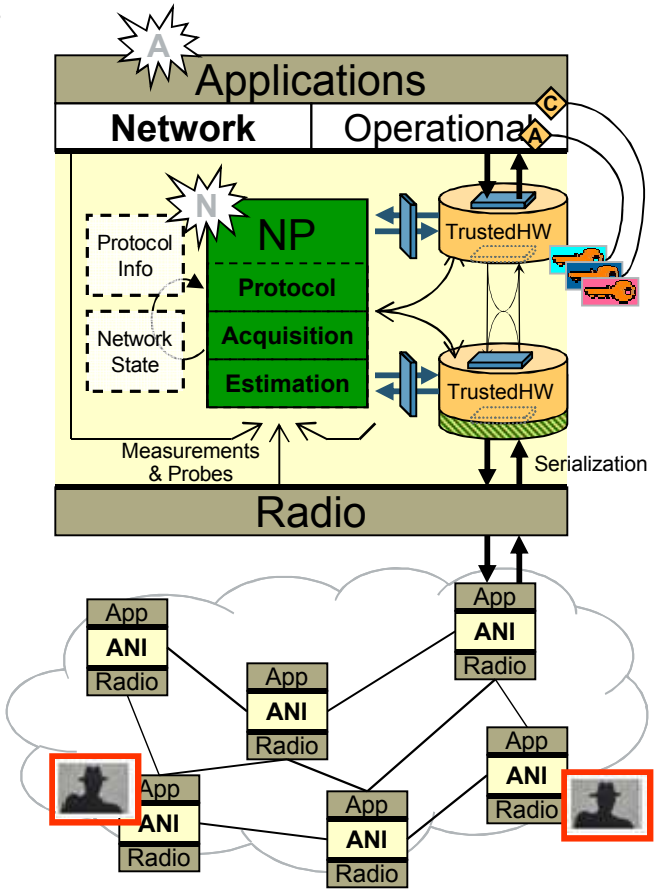
- Adversary exploits gaps in security policy enforcement for access to disallowed services
  - Retrieve operational information (exfiltration)
  - Manipulate network services like routing tables
  - Consume network resources by forwarding traffic that is not consistent with security policy



Lack of security policy "M" associated with traffic flows

Vulnerability - Exfiltration

- Adversary exploits gaps in security policy enforcement for access to disallowed services
  - Retrieve operational information (exfiltration)
  - Manipulate network services like routing tables
  - Consume network resources by forwarding traffic that is not consistent with security policy
- Deny-by-default policy services enforce security policy “M” – Gaps default to closed
  - Define algebra and properties of policy
    - Axiomatic Policies – Minimum enabling set
    - Bootstrapping – How to start the system?
  - Formal methods for validating the intrinsic security of the system

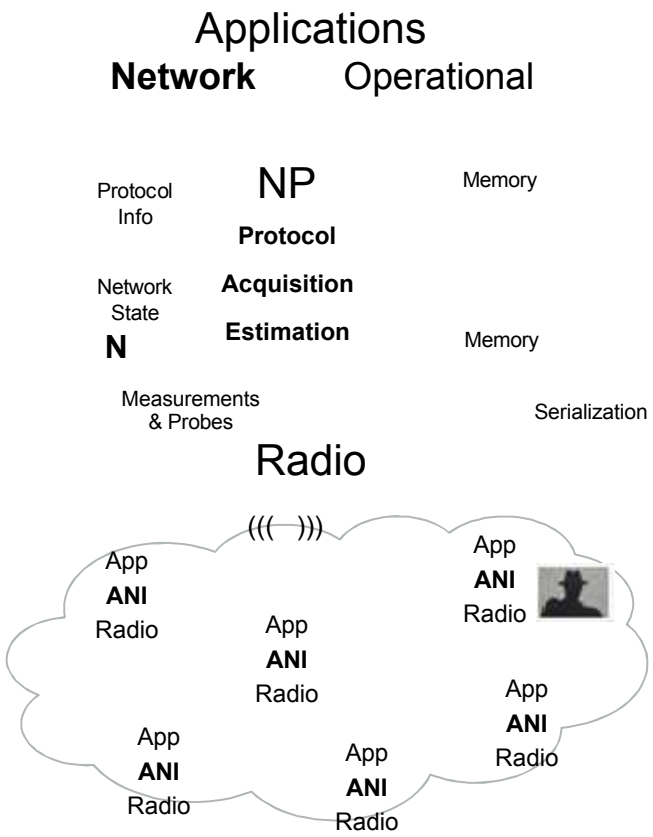


PIANO Policy Services enforce Security (not Resource) policy

Vulnerability – Network Modeling (Estimation)

MILCOM:08
ASSURING MISSION SUCCESS

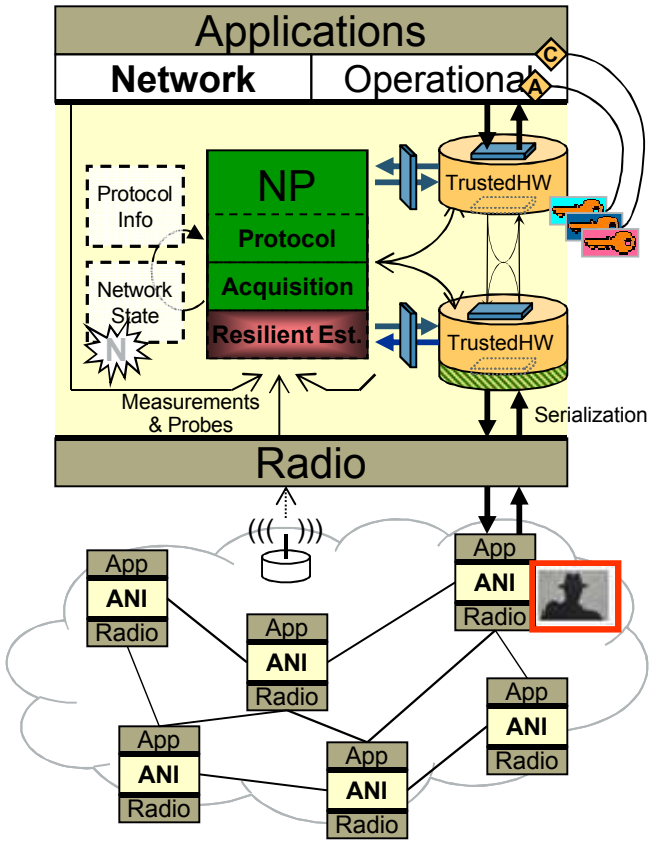
- Adversary interferes with node's ability to estimate key characteristics about the network
  - Generates cyclic interference to prevent convergence of link-quality estimation process
  - Delay measure probes to make certain neighbors appear congested
  - Adversary does not have to be element of the network (e.g., jammer)



Easy to manipulate how the node perceives the extended network

Vulnerability – Network Modeling (Estimation)

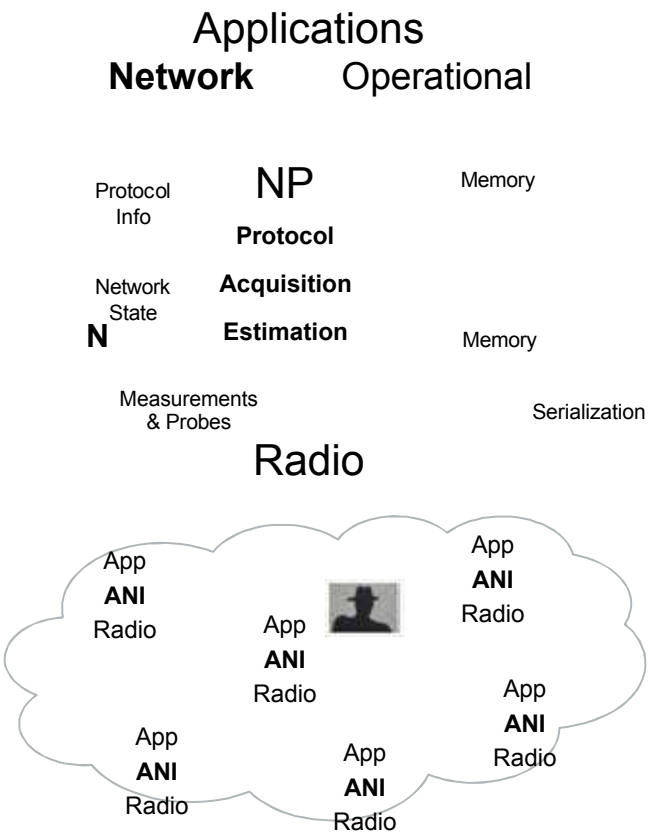
- Adversary interferes with node's ability to estimate key characteristics about the network
  - Generates cyclic interference to prevent convergence of link-quality estimation process
  - Delay measure probes to make certain neighbors appear congested
  - Adversary does not have to be element of the network (e.g., jammer)
- Resilient estimation accounts for intentional external influence on the measurement process



Resilient Estimation mitigates attacks against estimation processes

Vulnerability – Network Modeling (Data Acquisition)

- Adversary disseminates false information about the network's state
  - Local node unable to estimate information directly → Depends on other nodes
  - E.g., link-state information for nodes more than 2 hops away

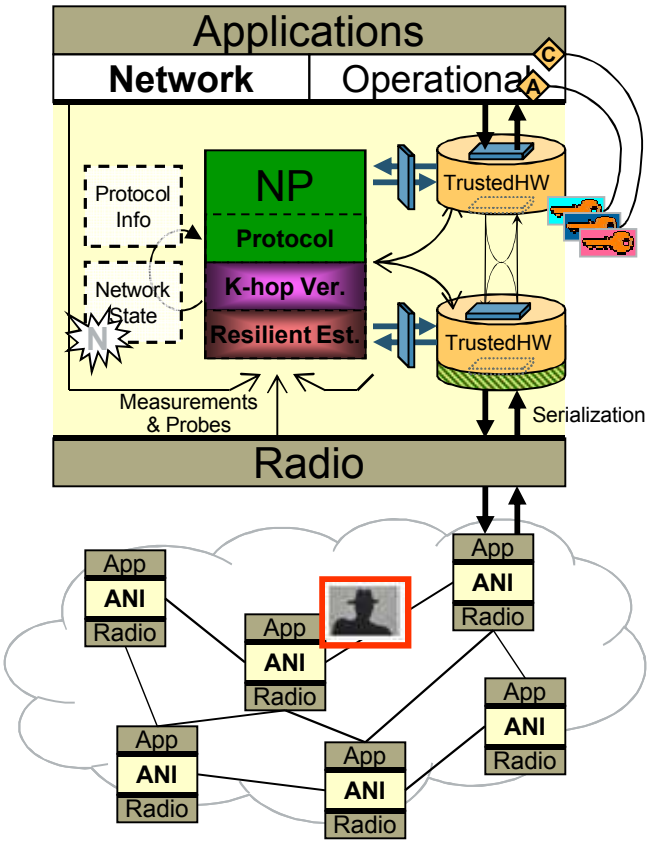


Adversary can lie about the network with impunity

Vulnerability – Network Modeling (Data Acquisition)

MILCOM:08
ASSURING MISSION SUCCESS

- Adversary disseminates false information about the network's state
  - Local node unable to estimate information directly → Depends on other nodes
  - E.g., link-state information for nodes more than 2 hops away
- K-hop Verification distributes credentialed state info among nodes in K-hop region
  - Detect and reject false information by exposing supporting evidence
  - Identification of misbehavior in the data plane (e.g., forwarding) and control plane (e.g., false topology information)

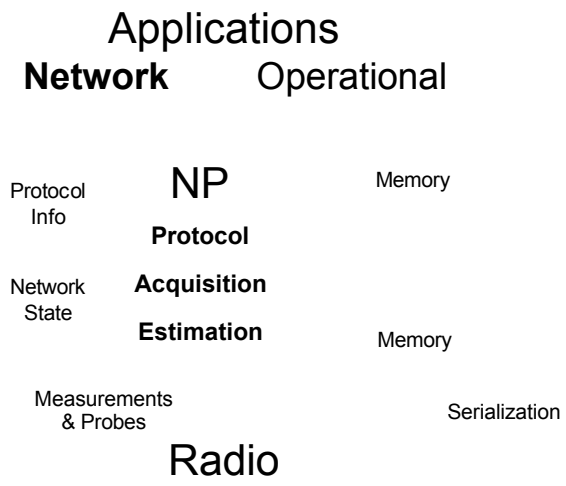


K-Hop Verification increases the transparency of events influencing a node

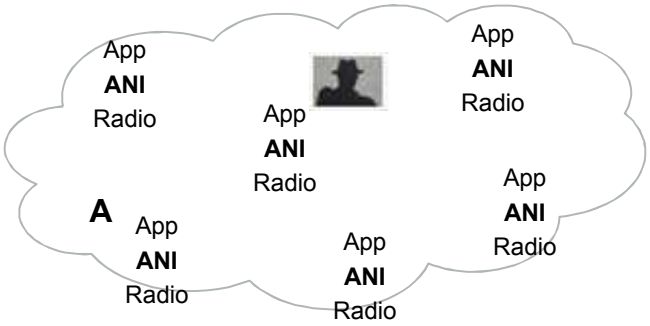
Vulnerability – Byzantine robustness of network

MILCOM:08 ASSURING MISSION SUCCESS

- Adversary exploits advantaged location within the network to drop, delay, mis-forward traffic
  - Routing: Jellyfish, Blackhole, Wormhole



Single Path of Failure

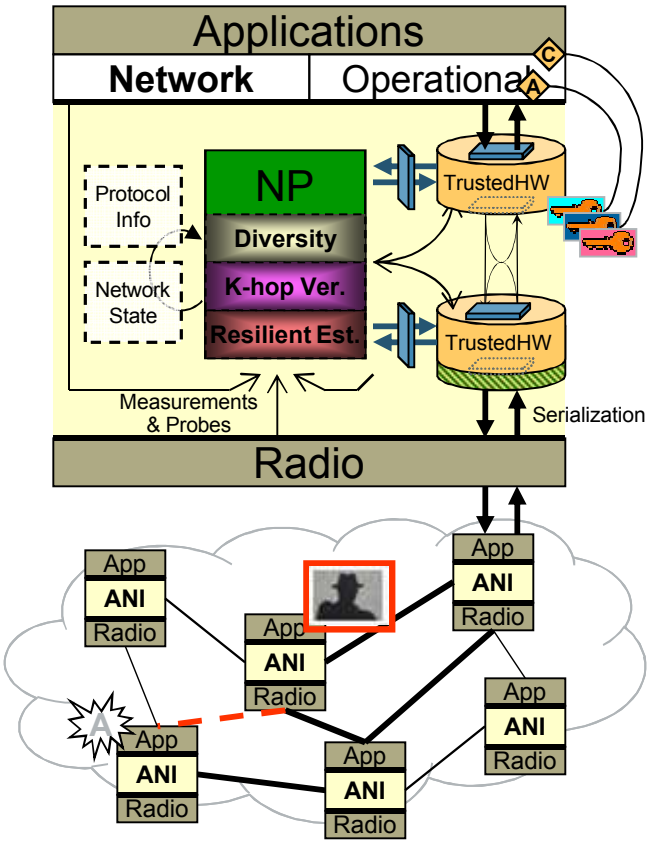


Classic networking places disproportional trust along single path

Vulnerability – Byzantine robustness of network

MILCOM:08
ASSURING MISSION SUCCESS

- Adversary exploits advantaged location within the network to drop, delay, mis-forward traffic
  - Routing: Jellyfish, Blackhole, Wormhole
- Forwarding over multiple paths spreads information across the topology
  - Reduces dependency on any single node in the network
- Coding over multiple packets spreads information across the temporal flow
  - Reduces dependency on any single packet's successful delivery
  - Partially hides details of packet's contents



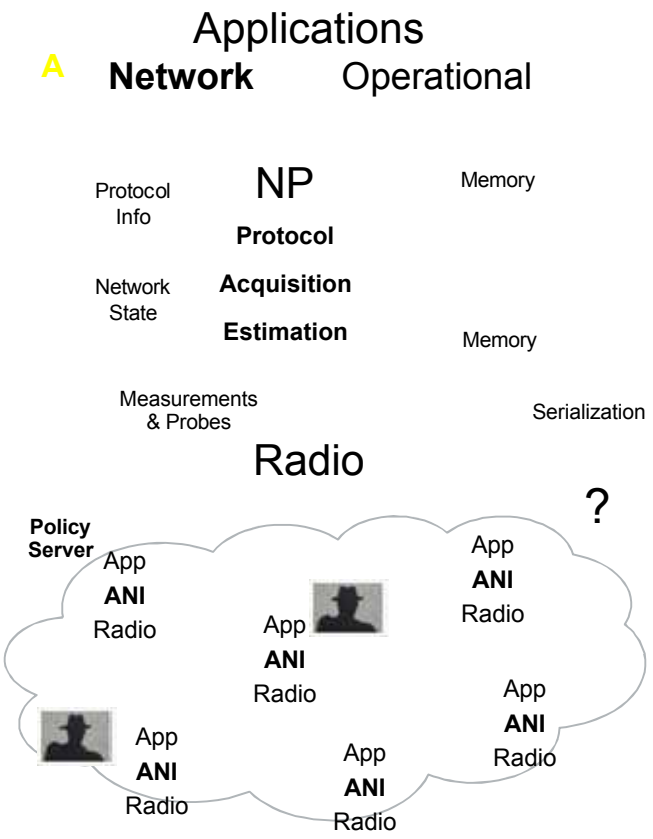
Network coding naturally combines packet coding and path diversity

IEEE COMMUNICATIONS SOCIETY
BAE SYSTEMS
Telcordia
Sandia National Laboratories

Vulnerability – Byzantine robustness of network data

MILCOM:08 ASSURING MISSION SUCCESS

- Adversary blocks access to shared network data required for operation
  - Block or delay access to policy cause deny-by-default eventually deny everything
  - Block or delay access to name services prevents resolution of server name to network address (e.g., DNS)



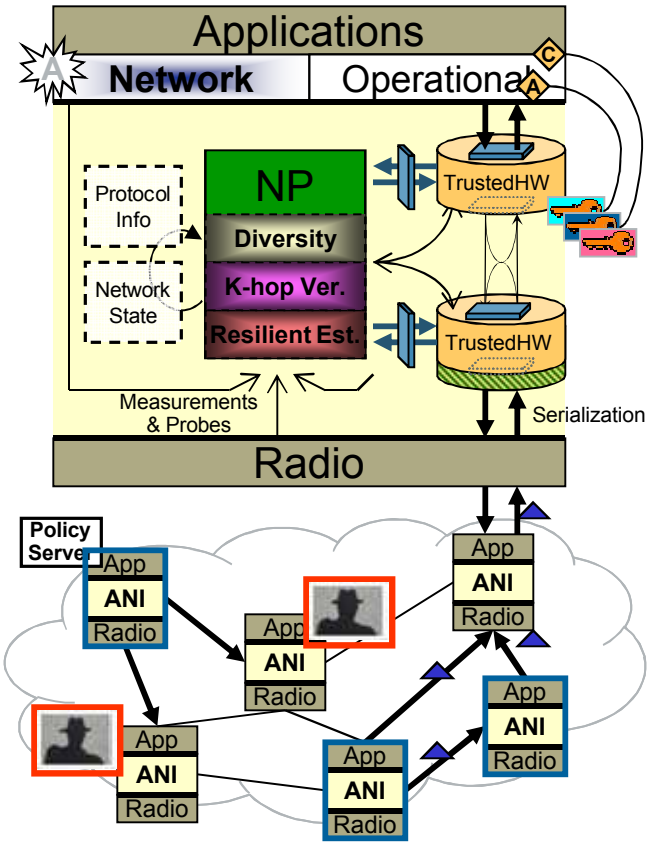
Single Point of Failure

Classic data storage places disproportional trust on single nodes

Vulnerability – Byzantine robustness of network data

MILCOM:08
ASSURING MISSION SUCCESS

- Adversary blocks access to shared network data required for operation
  - Block or delay access to policy cause deny-by-default eventually deny everything
  - Block or delay access to name services prevents resolution of server name to network address (e.g., DNS)
- Disseminate shared network data across multiple nodes
  - Trade distributed/replicated storage for security
  - Balance dissemination and fetch time
  - Provide immunity to network partitions

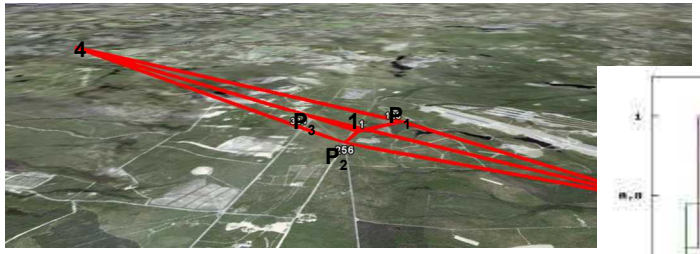


Cache Coding spreads storage of network information across multiple nodes

AFCEA IEEE COMMUNICATIONS SOCIETY BAE SYSTEMS Telcordia Sandia National Laboratories

Example of PIANO in Practice

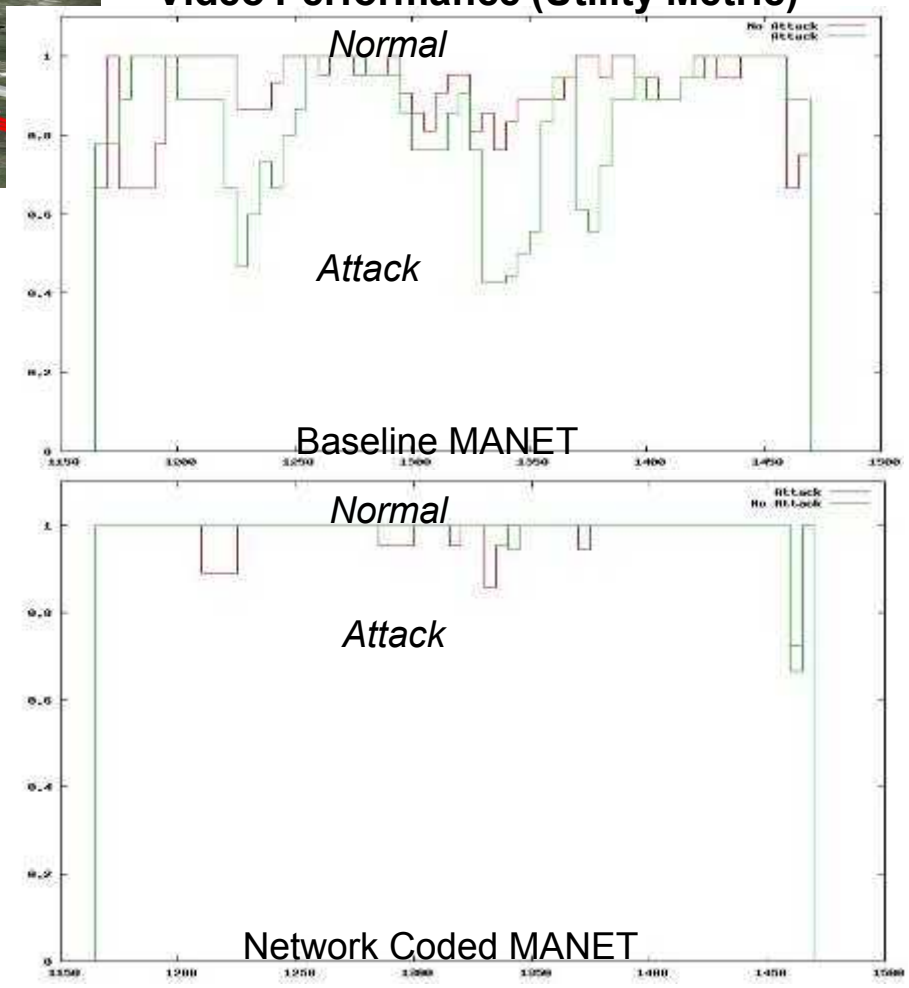
Lakehurst scenario w/ 4 traffic types



- Large data packets dropped during pink regions while control signaling forwarded
- Significant drop in quality relative to normal operation w/o PIANO
- Recovery time longer than original attack

PIANO has intriguing and powerful information assurance properties

Video Performance (Utility Metric)



Zodiac Architecture

- Architectural realization of “need to know” in the Dynamic Community of Interest
- End-to-end security: host and network apply the same security model cooperatively

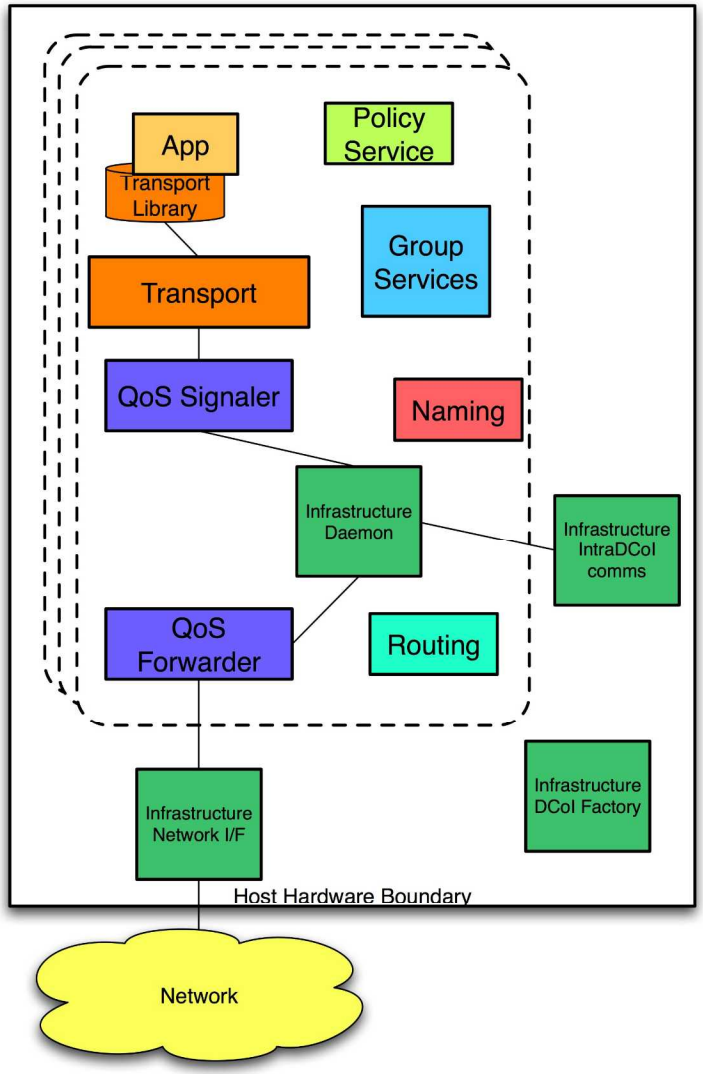
Dynamic Communities of Interest

MILCOM:08 ASSURING MISSION SUCCESS

- Dynamic group of networked nodes whose membership, application, and resources are controlled by policy
  - Dynamic: can be created for even ephemeral conversations
  - Membership: only those nodes with a need are allowed to join the DCoI
  - Single application: each DCoI supports one application, which allows policy and monitoring to be fine-grained
  - Policy: flexibility to meet mission needs means that different DCoIs are tailored to have different characteristics
- End-to-end security
  - Packets are tagged by DCoI to allow enforcement of DCoI policies in network
  - DCoIs are isolated in containers on host to avoid vulnerabilities in applications from allowing leakage of data in the hosts

Zodiac Node Architecture

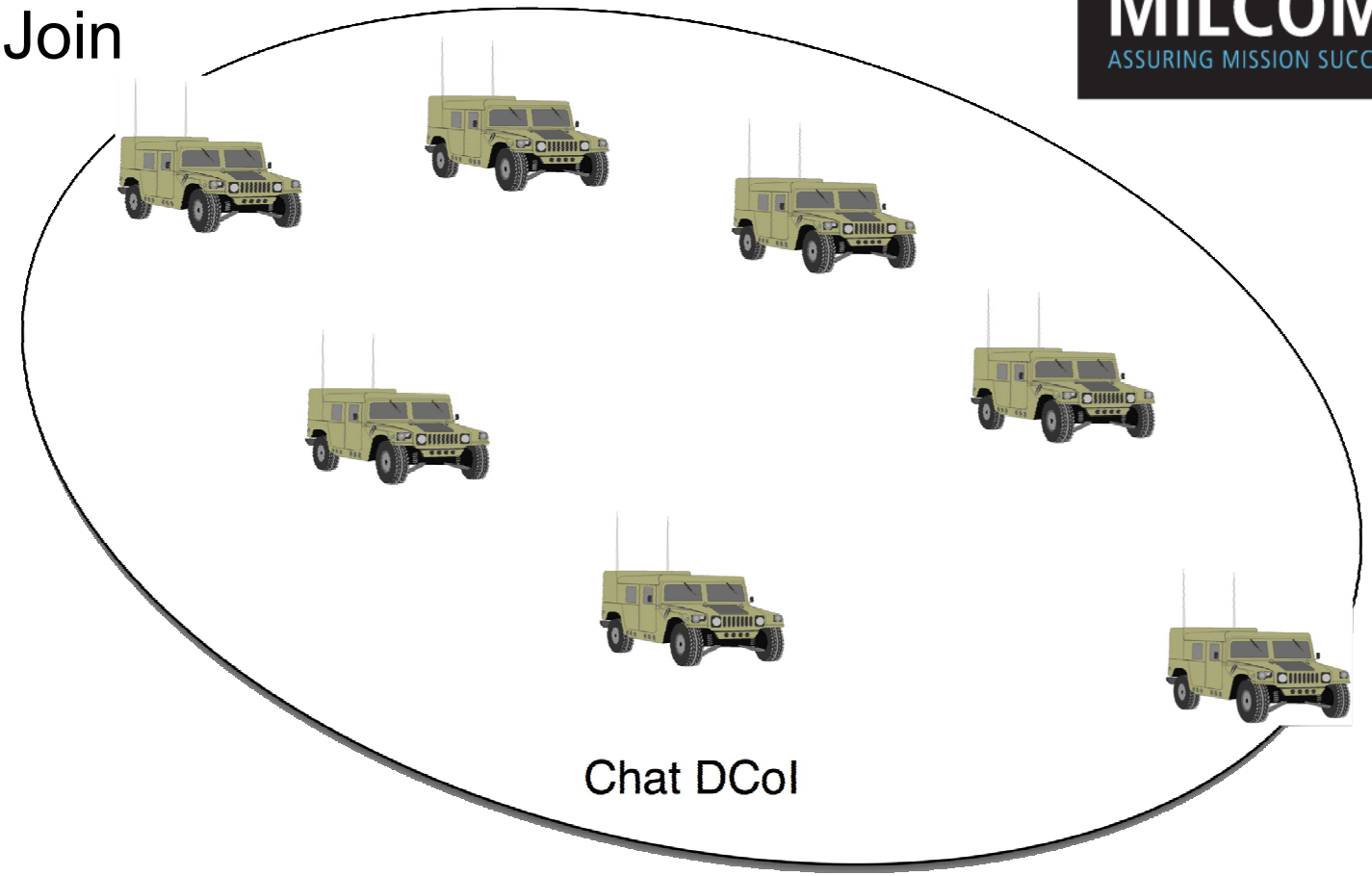
- Transport / QoS
  - TIA-1039 based
  - Used to limit attack access to resources as well as provide soft guarantees
- Group Services
  - Controls membership in DCoIs and arranges for key sharing
- Naming
  - Securely provides access to network data such as name to address maps
- Routing
  - Per-DCoI choice
  - Zodiac implements a geographic routing approach with multipath
- Host Services
  - Virtual machine containers are used to isolate data and processes within a host
- Policy
  - Provides mission flexibility in how Zodiac is configured and used



A Zodiac DCoI in the Network

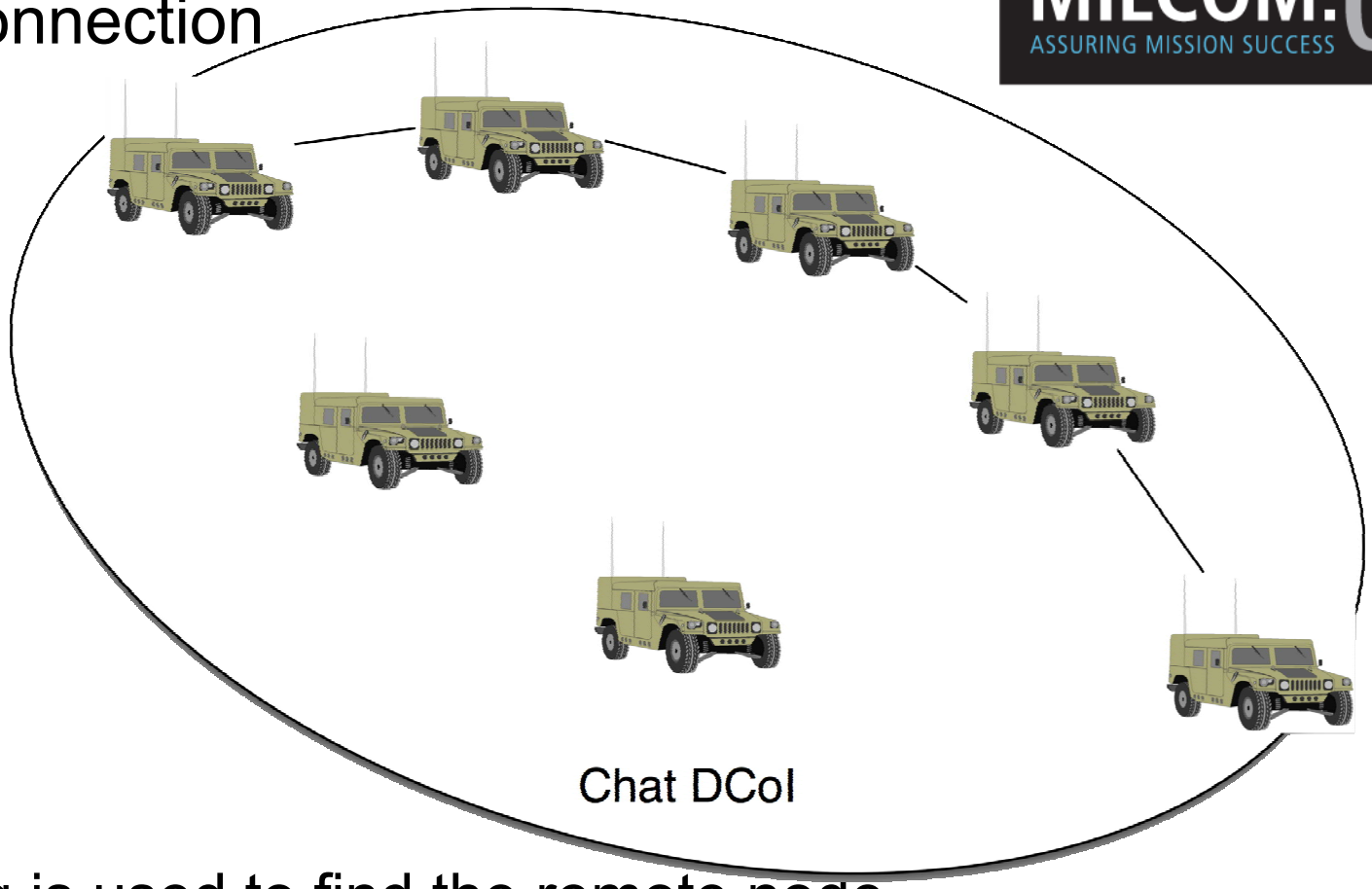
- Two units want to open a chat session

DCoI Join



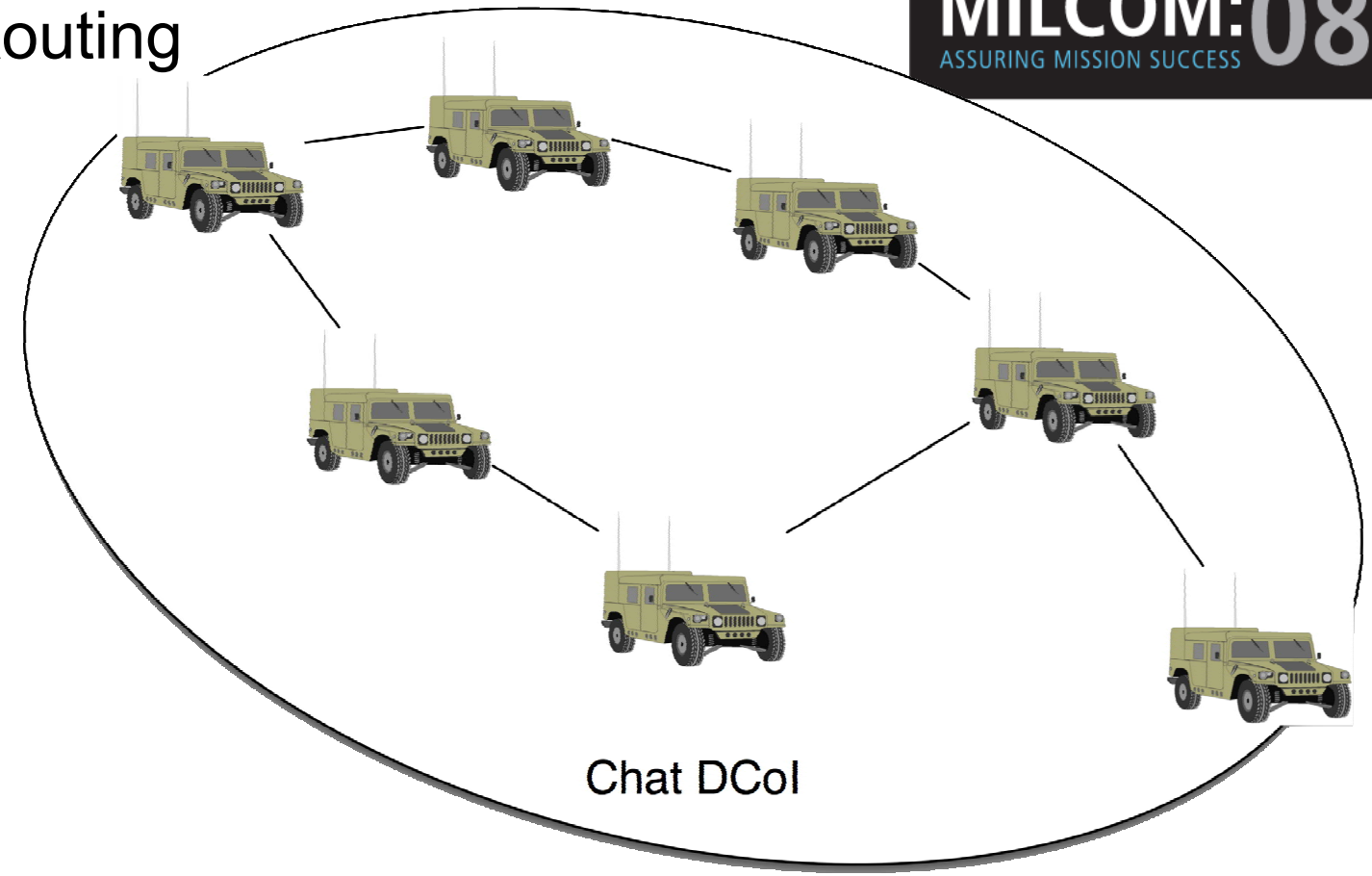
- They join an existing DCoI with other members
- Group Services checks the authorization for the join
- New containers are created to provide host security

Open Connection



- Naming is used to find the remote node
- A path is created
- Policy determines QoS limits

Multipath Routing



- In practice, multiple paths are chosen for availability and reliability

Zodiac Design Principles

- Fined-grained containment strategy
  - Per-DCoI keys, policies, and resource allocation
  - All traffic must be part of a DCoI including “control” traffic
  - Each forwarding node can determine if a packet is signed and encrypted as part of a known DCoI
  - Extension into the host provides mandatory access control that spans the hosts and the network
  - Provides deny-by-default and ensures authorization and authentication
- Comprehensive hop-by-hop enforcement
  - Each host is responsible for enforcing policies and mechanisms that defend itself, the DCoI, and the network
  - Because we are concerned about Byzantine nodes, we reduce our reliance on enforcement external to the host
- Diversity of services and data
  - Where possible, services are distributed, redundant, or both
  - Increases the number of nodes that an attacker must capture
  - Improves throughput in face of failing networks

Zodiac Security Results

MILCOM:08
ASSURING MISSION SUCCESS

Confidentiality	• Encryption • Narrow DCoI scope • Dispersity splits up messages • DCoIs limit information transfer	• Group & Crypto Services • Policy, Resource Allocation • Routing • Host Security
Availability	• Redundant paths • Redundant servers • Geographic routing to find disjoint paths • QoS signaling • Strict, policy-based allocation and policing	• Routing • Naming, Policy, Group & Crypto Services • Routing • Resource Allocation • Policy, Transport, Resource Allocation
Integrity	• Per-hop content filtering • Encryption and authentication of communications • Authentication of join requests	• Transport, Policy, Routing, Group & Crypto Service • Transport, Group & Crypto Service, Policy • Group & Crypto Service
Safety	• Configuration/ policy is DCoI-specific limiting impact of configuration error	• Policy
Reliability	• Virtual machines allow low-overhead, clean restart following failure or as remediation	• Host Security

AFCEA IEEE COMMUNICATIONS SOCIETY BAE SYSTEMS Telcordia Sandia National Laboratories