SAND2007-6213P

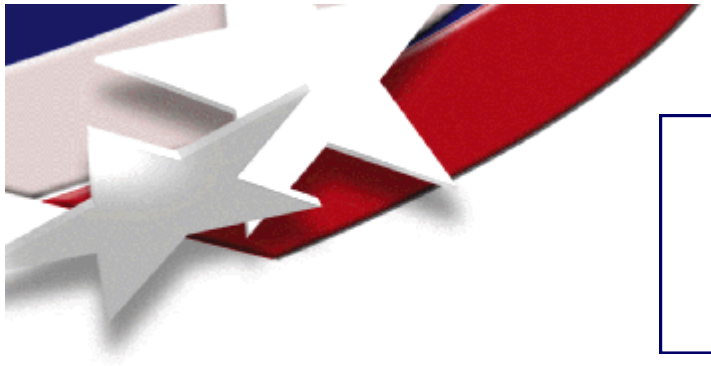
Security Challenges with Wireless Technology

SAG S&T Panel Meeting, 26-27 September, 2007

William Young, Ph.D
Sandia National Laboratories
Network Assurance and Survivability
Department 5616
wfyoung@sandia.gov
505-844-8327

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories



Presentation Purpose

- Given: The rapid adoption of wireless technologies
  - Low deployment costs
  - Flexibility
  - Operational advantages

- Approach: Frame a dialogue about security and availability issues associated with wireless communication systems
  - Must be balanced with the benefits
  - Solutions are not simple technology fixes or add-ons

Sandia National Laboratories

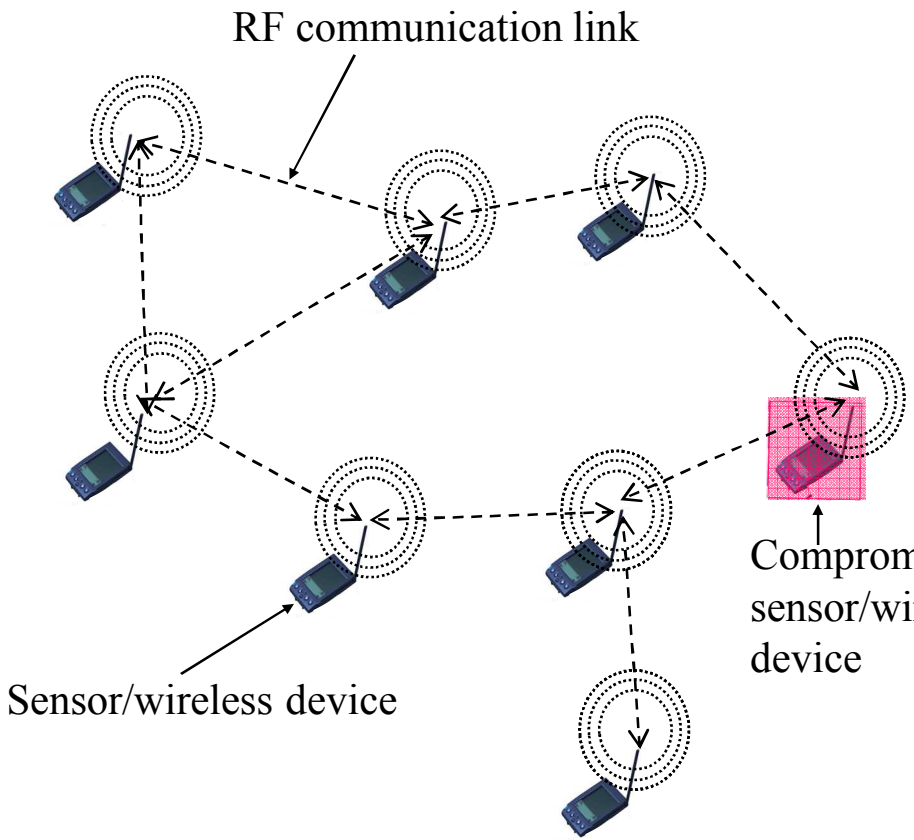
Facts About Wireless Technology

1. Adversaries have near zero-cost access to your transmission medium
2. Adversaries will gain access to our wireless devices
3. Wireless networks require more complex media sharing protocols
4. Ad hoc networks require more complex routing algorithms
5. Wireless devices have unique radio frequency signatures
6. Low-probability of detection (LPD) is difficult to achieve an ad hoc network.
7. Cryptographic protections have a much higher relative cost than wired networks
8. Operation environment is unknown and often harsh (physically and electrically)

In general, wireless devices are power and computationally limited, and are also often highly mobile

Sandia National Laboratories

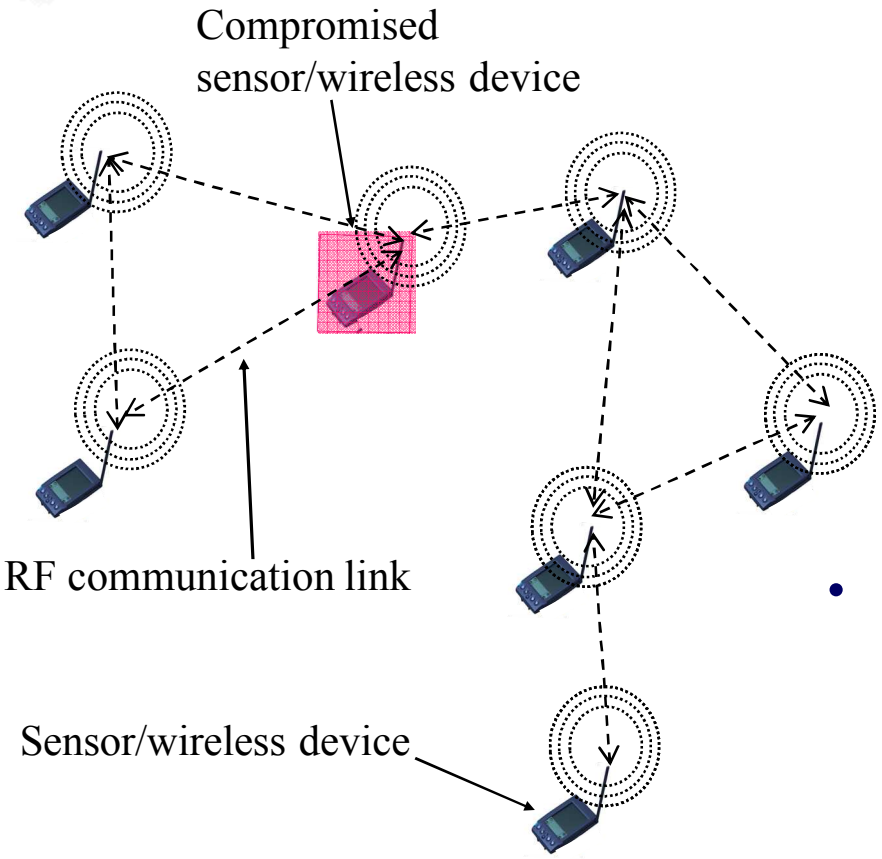
Wireless Technology Can Enable Distributed Sensor Networks



- Perimeter Access
  - Denial of service (DoS) on devices in RF range
  - Control plane manipulation
- Passive Observation
  - Traffic/information flow analysis
- Information Assurance (IA) Issues
  - Cryptographic processing for user data adds overhead
  - Key management is problematic
  - Need some exposed information to efficiently and dynamically form a network
  - Complex routing algorithms are need to offset node failure (or compromise)

Sandia National Laboratories

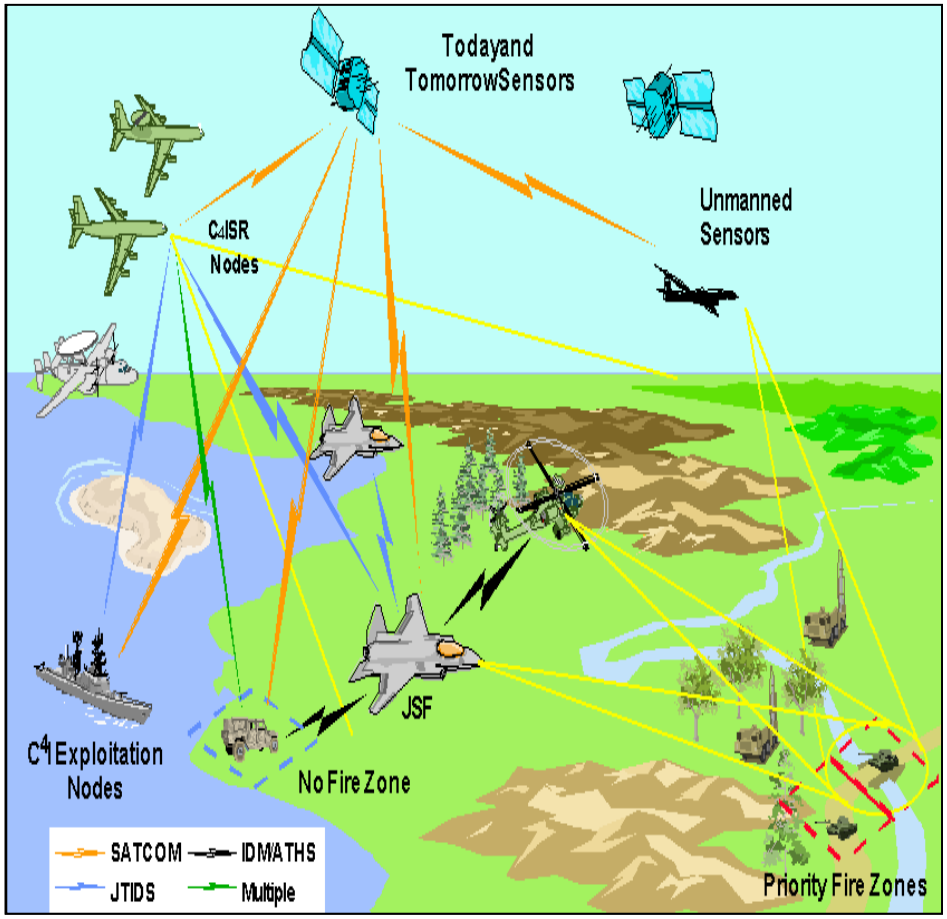
Distributed Wireless Networks (cont.)



- Compromise node centrally located
  - Man-the-middle attacks
    - Replay altered messages
    - Message flooding
    - Intermittent RF jamming (increase power level)
  - Control plane manipulation
    - Intermittently disrupt of the critical communication link
    - Segment of the network
    - Force network route convergence
- User data usually takes a multi-hop path
  - Consumes power and processing time
  - Potentially exposes data and system activities

Sandia National Laboratories

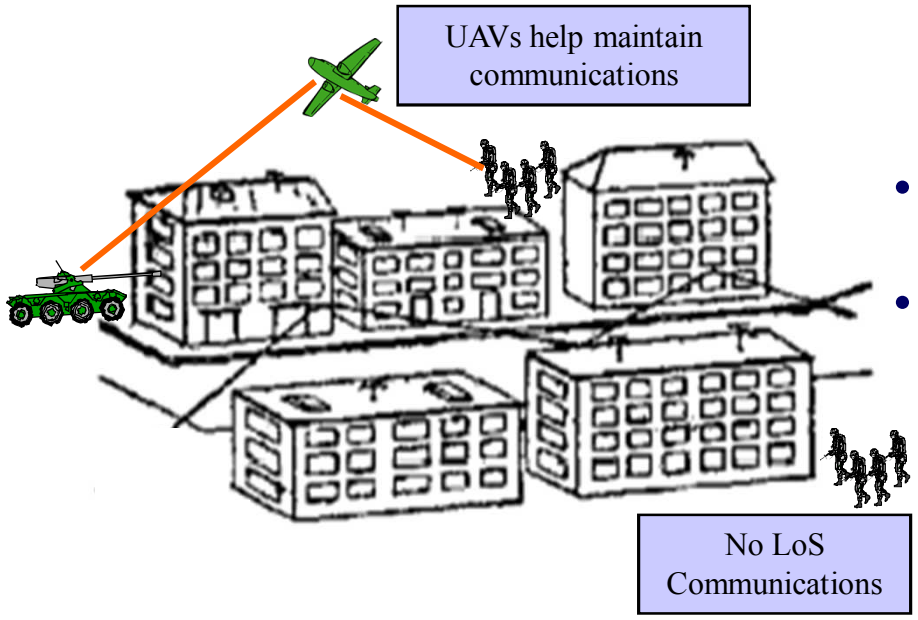
Wireless Technology is Critical to Modern Tactical Networks



- Difficult to maintain network connectivity
  - Dynamic frequency spectrum allocation
  - Complex routing protocols
- Introduction of new network protocols can create additional challenges
  - IPv6, Radio Open Shortest Path First (ROSF) routing protocol
- Self-interference due to number of users in limited RF spectrum
- Multiple platforms supporting a wide range of radio capabilities
  - Low-power sensors, wireless LANs, UAVs, satellites, hand-held radios, etc.

Sandia National Laboratories

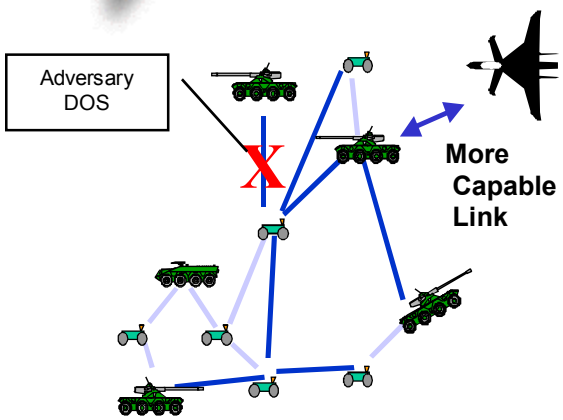
Urban Environments Present Significant Availability Challenges

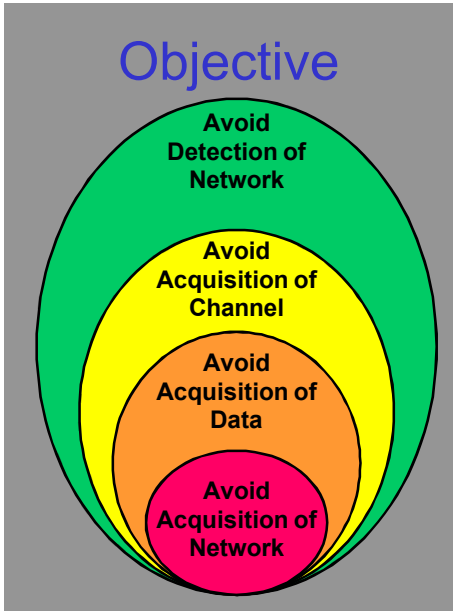


- Urban RF propagation is more complex
  - Limited line-of-sight communications
  - Multi-path interference
  - Difficult to predict and model
- Higher frequencies generally do not penetrate buildings well
- RF propagation into structures is highly specific to material content and frequency
  - RF shielding by window treatments
  - Metal reinforcing rods and beams
  - Internal contents such as manufacturing equipment
- IA approaches
  - High power RF
  - Multi-hop networks

Sandia National Laboratories

Security in wireless communications requires a system solution





Environment:

- Resource Constraints
  - –RF Bandwidth
  - –CPU Limitations
  - –Battery Size
- RF Stressors & Issues
  - –Environmental Interference
  - –Terrain Interference
  - –Adversarial Interference
  - –Covertness; LPI/LPD
  - – Antenna placement
- Network
  - –Dynamic Topology & Mobility
  - –Scalability

Approaches:

- Cryptography
  - –Low-Power Approaches
  - –Threshold
- Non-Cryptography
  - –Redundant Routes
  - –Source Route Switching
  - –Onion Routing
  - –Encapsulation
  - –Sequence Numbers
  - –Time Stamp
  - –Intrusion Detection
  - –Directional Antennas
- TRANSEC Approaches

Sandia National Laboratories

Questions?

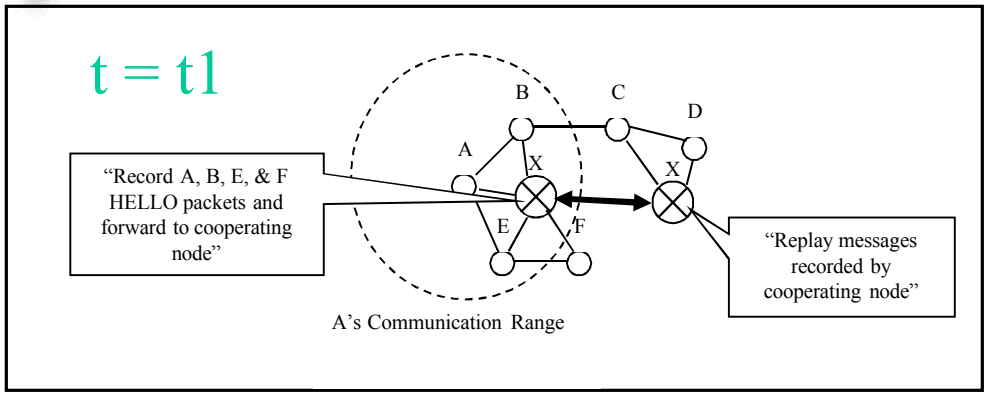
Sandia National Laboratories

Additional Technical Content

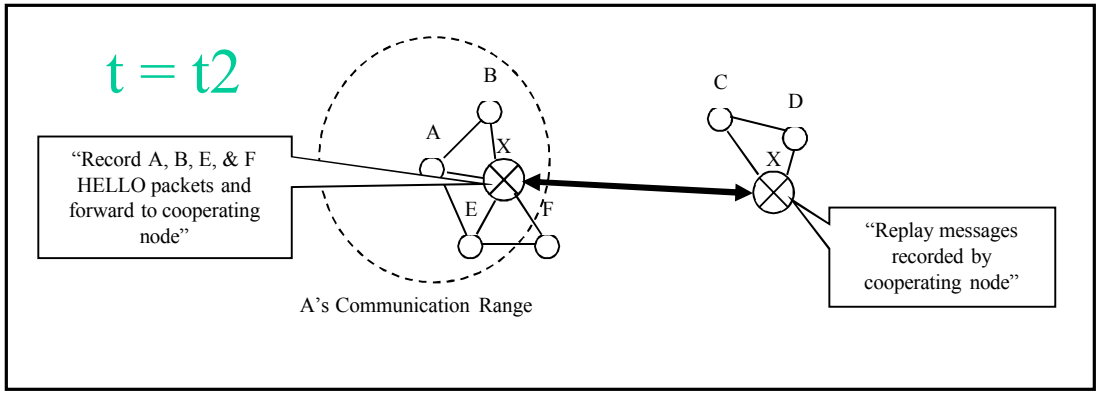
- Network Segmentation via Control Plane Replay Attack
- Distributed Wireless Network Information Assurance (IA) Approach
- Example analysis of securing media access control
- Data throughput reduction when cryptography is used
- Impact of IPv6 on FCS
- Survivable Key Management in Wireless Ad Hoc Networks

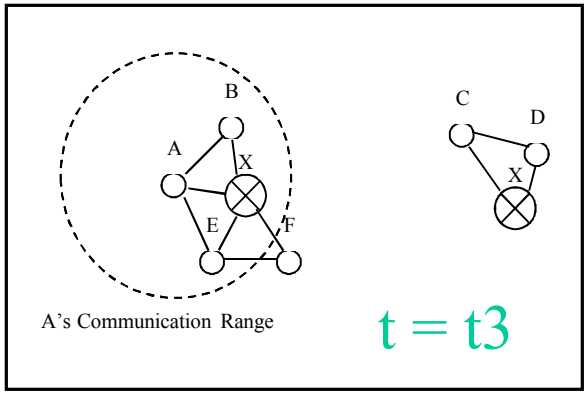
Sandia National Laboratories

Network Segmentation via Control Plane Replay Attack



Cooperating adversary nodes can partition network by recording and replaying control-plane data frames





Sandia National Laboratories

Distributed Wireless Network Information Assurance (IA) Approach

Incorporate IA at appropriate layer

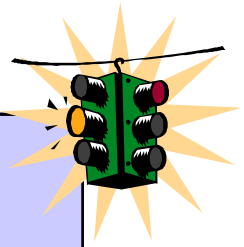
Protocol Stack

- Application
- Transport
- Session
- Presentation
- Network
- Link/MAC
- Physical

TRANSEC

User-Plane Data IA

- Security at the application
- Digital signatures, encryption
- SSL, HTTPS



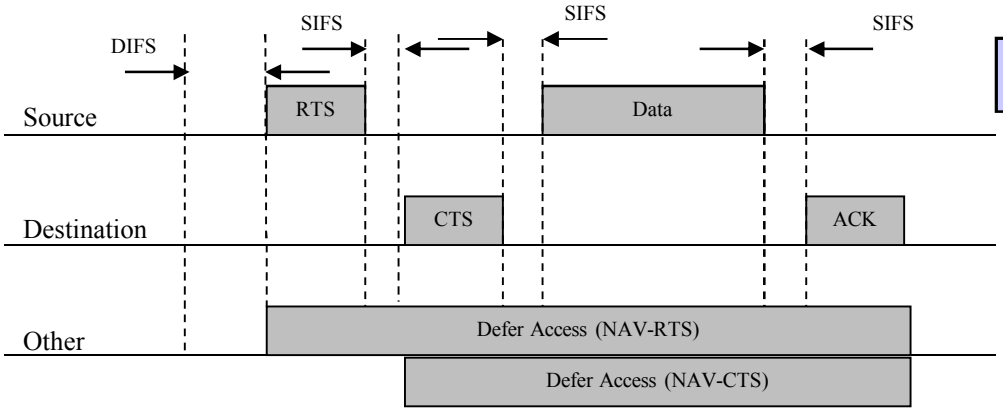
Control-Plane Data IA

- IA for control and network management information

Both Crypto & Non-Crypto Approaches

Sandia National Laboratories

Example analysis of securing media access control



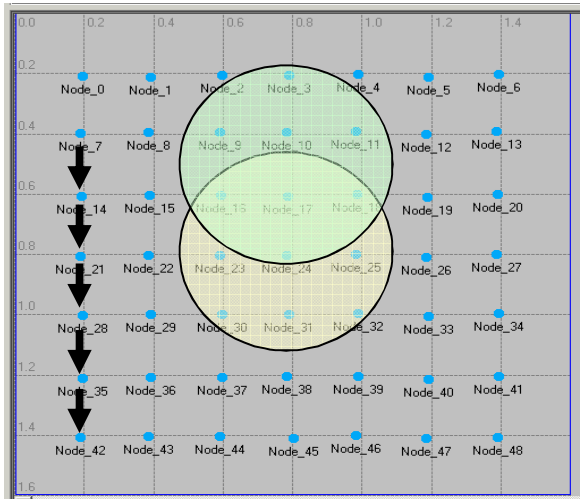
IEEE 802.11 MAC

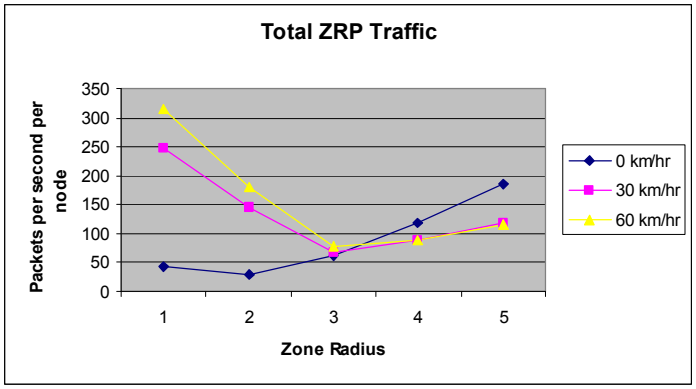
Cryptographic Processing Times

Signature Algorithm	Execution Time
MD5	100 megabits/sec (5.12microseconds/512bit block)
SHA-1	48 megabits/sec (10.7 microseconds/512bit block)
SHA-256	24 megabits/sec (42.8 microseconds/1024bit block)
RSA-512 Signature	1.92 ms
RSA-512 Verification	0.13 ms
RSA-1024 Signature	10.29 ms
RSA-1024 Verification	0.30 ms
RSA-2048 Signature	64.13 ms
RSA-2048 Verification	0.89 ms
DSA-512 Signature	1.77 ms
DSA-1024 Signature	5.5 ms

Sandia National Laboratories

Data throughput reduction when cryptography is used





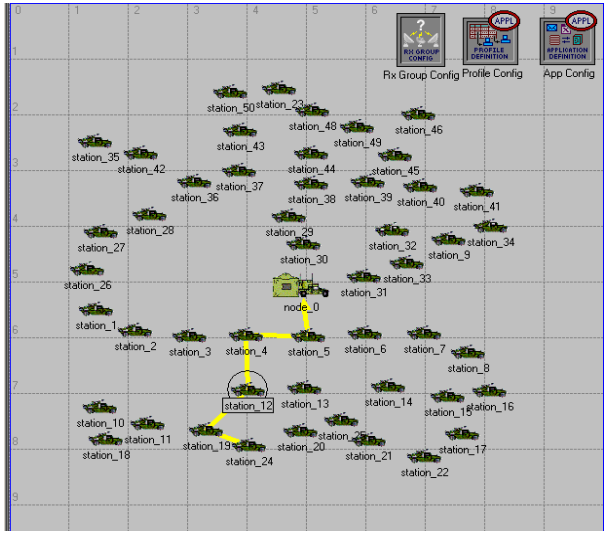
10 MHz Channel, 850 MHz Processor

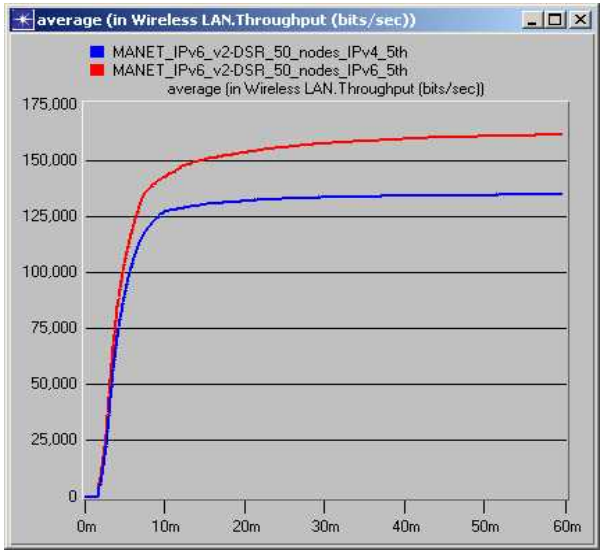
Time to process	Total messages transmitted	Contention	Available for application layer	Path length impacts	Final through put
	M	N=M/12	P=N-60	Q=P/5	R=512 Q
10us	1974	164.5	104.5	20.9	**10.7K**
100us	956	79.6	19.6	3.9	**1.9K**
1ms	155	12.9	none		**NF**
10ms	17	1.4	none		**NF**

Sandia National Laboratories

Impact of IPv6 on FCS

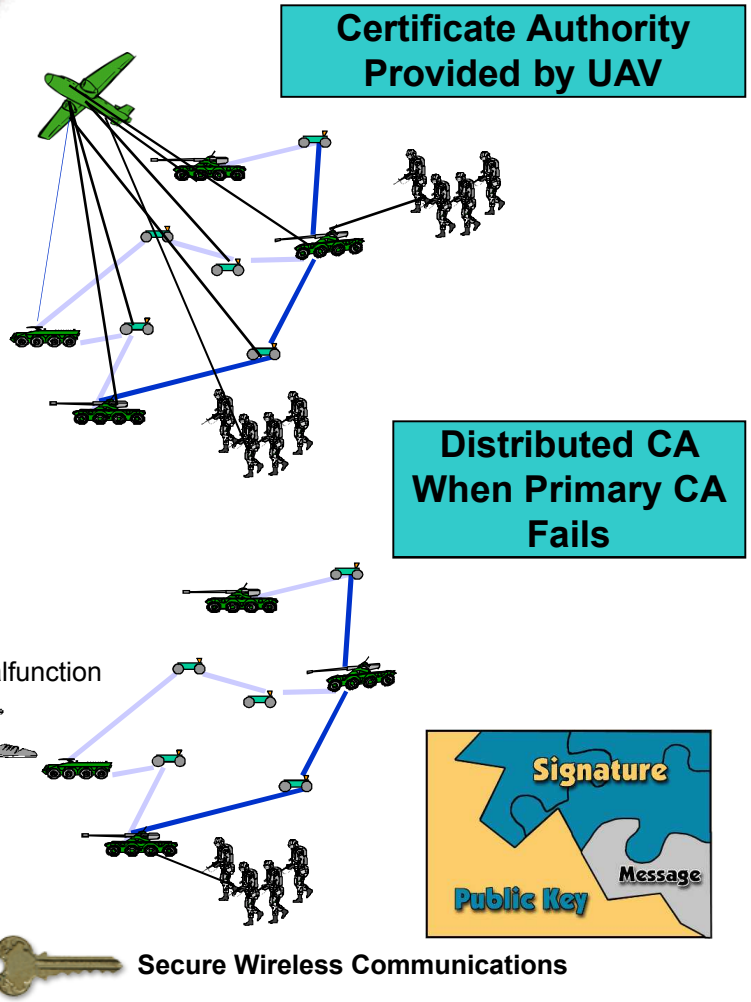
- Impact for high-bandwidth-utilization systems such as mobile, wireless systems used in FCS.
  - IPv6 increases the datagram header size.
  - Increase will result in additional bandwidth consumption and potentially the end-to-end delay.
- For the client/server example modeled under high-bandwidth-utilization operation the use of IPv6 required a 20% increase in bandwidth over the same system using IPv4.





Sandia National Laboratories

Survivable Key Management in Wireless Ad Hoc Networks



Problem:

No single compromised node should impact the integrity of the certificate process

Challenge:

- Create a distributed trusted authority from multiple ground nodes
- High availability and high security are conflicting requirements
- Necessary data exchanges feasible in a wireless ad hoc network operating in difficult communication environment

Approach:

- Use secret sharing
- Design/extend adaptive security for multi-layer networks

Sandia National Laboratories