Center for Wireless Network Security

WiNSeC

STEVENS
Institute of Technology

Dr. Patrick White
Assoc. Director – WiNSeC
Office: 201-216-5028
pwhite1@stevens-tech.edu

October 29, 2003

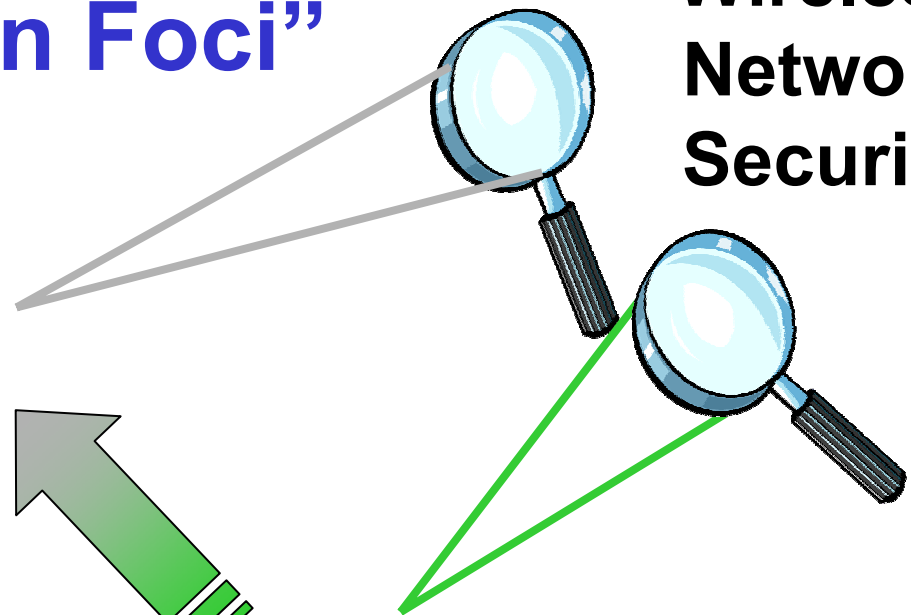
Wireless Network Security Center (WiNSeC)

Principal areas of focus:

- Secure, robust wireless communications technologies for Homeland Defense and Security:
  - Physical layer vulnerabilities, including anti-jamming/eavesdropping
  - Spectrally efficient communications
  - Interoperability of wireless systems
  - Energy efficient sensor networks
  - Wireless cyber counter measures
- Situational awareness tools for C^2
  - Visualization of sensor data
  - Decision aids
- Secure communications networks and command/control facilities for First Responders

Initial funding from DoD – administered by Picatinny Arsenal

"Twin Foci"



Wireless Network Security

TestBed / Analysis

Research

Technology Commercialization/ Enterprise Development

Multi-Environment

SUBURBAN

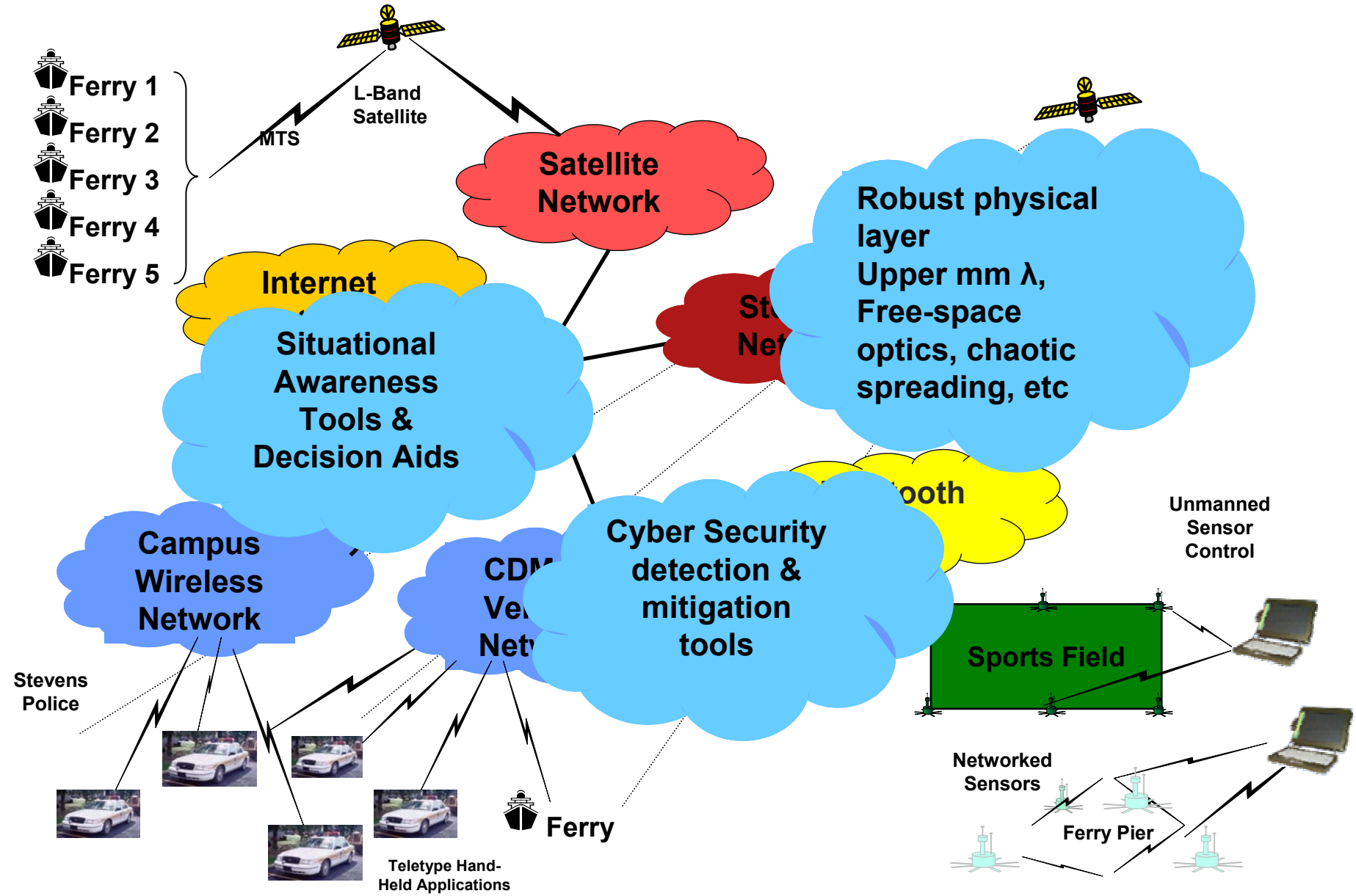
URBAN

MARITIME

- Background radio noise
- Multipath
- Shadowing …

If it works here …

Multi-Network Test Bed



WiNSeC Research

Information Assurance

- Secure and Reliable Wireless Sensor Networking
- Distributed Access Control
- Privacy Preserving information sharing
- Robust Multimedia Networking

Physical Security

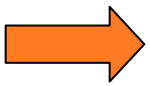
- Secure Network Infrastructure
- Smart Antennas for Interference Suppression
- Modeling and Simulation Tools
- Secure Protocols for Wireless Applications
- RF Transmission Power Management and Detection: Chaotic Direct Sequence Spread Spectrum

Network Management

- Visualization: Sensor Data
- Secure and Sound Decision Tools
- Cyber Security Risk Analysis and Evaluation

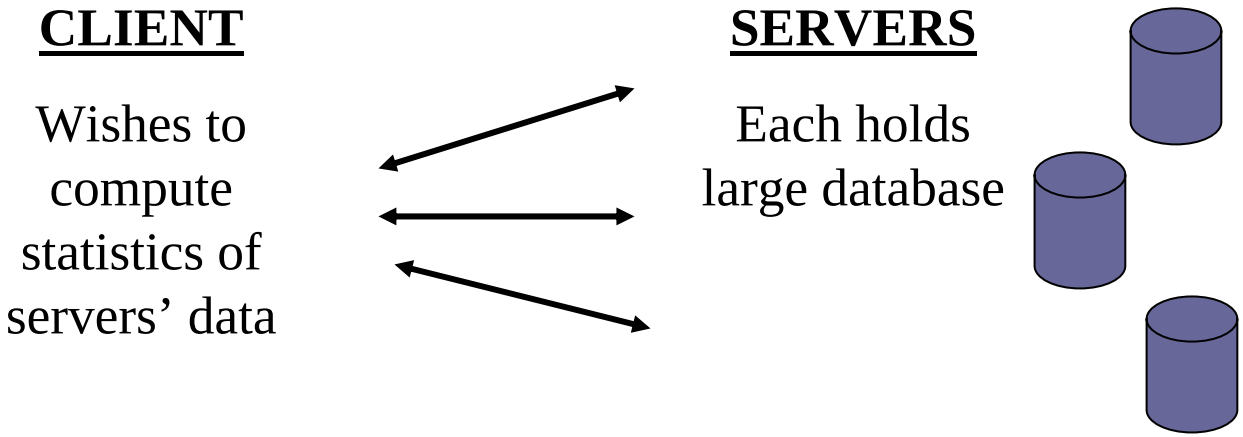
Privacy-Preserving Information Sharing (Rebecca Wright)

Allow multiple data holders to collaborate to compute important (e.g., security-related) information while protecting the privacy of other information.



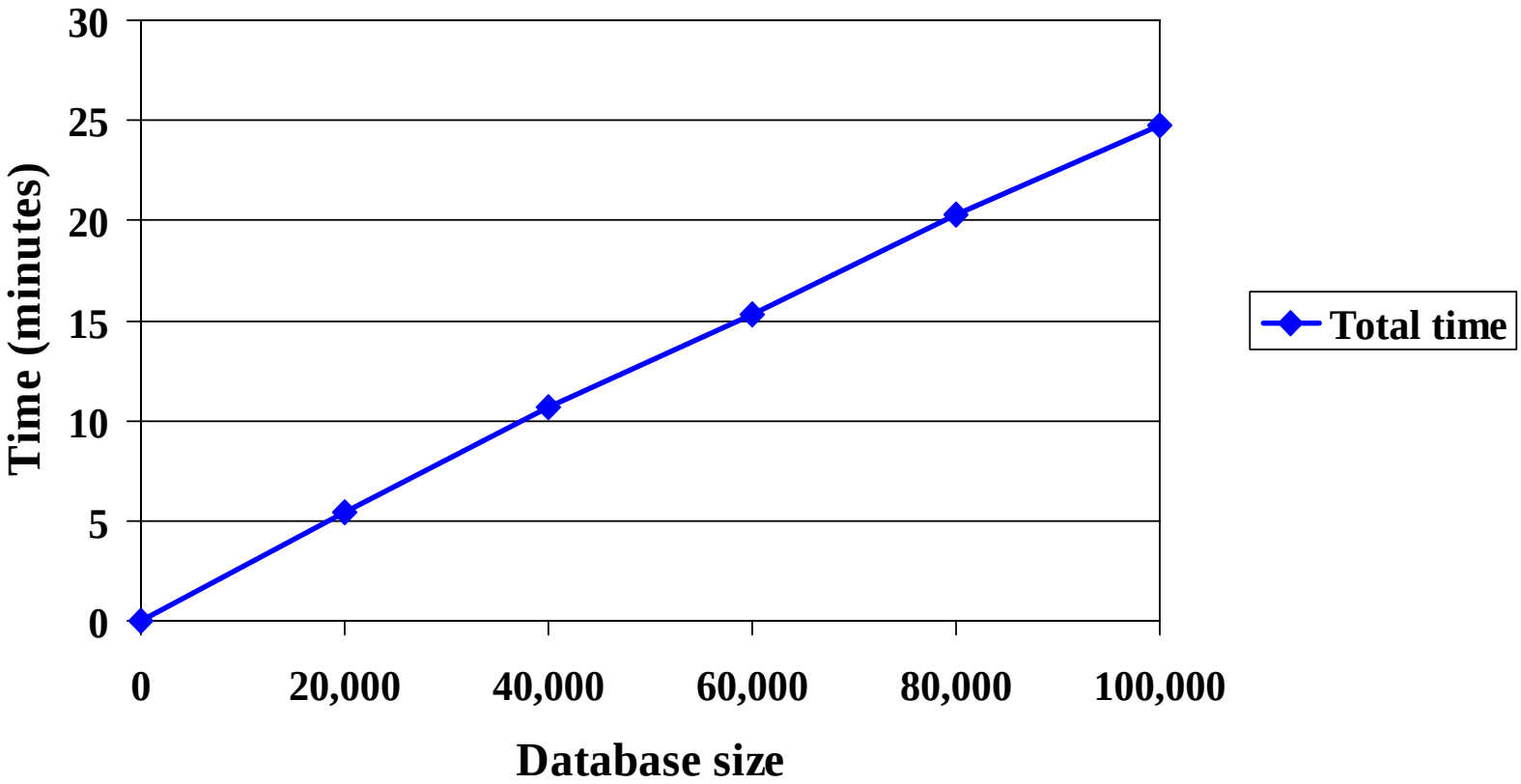
Particularly relevant now for agencies that would like to share sensitive information

Privacy-Protecting Statistics

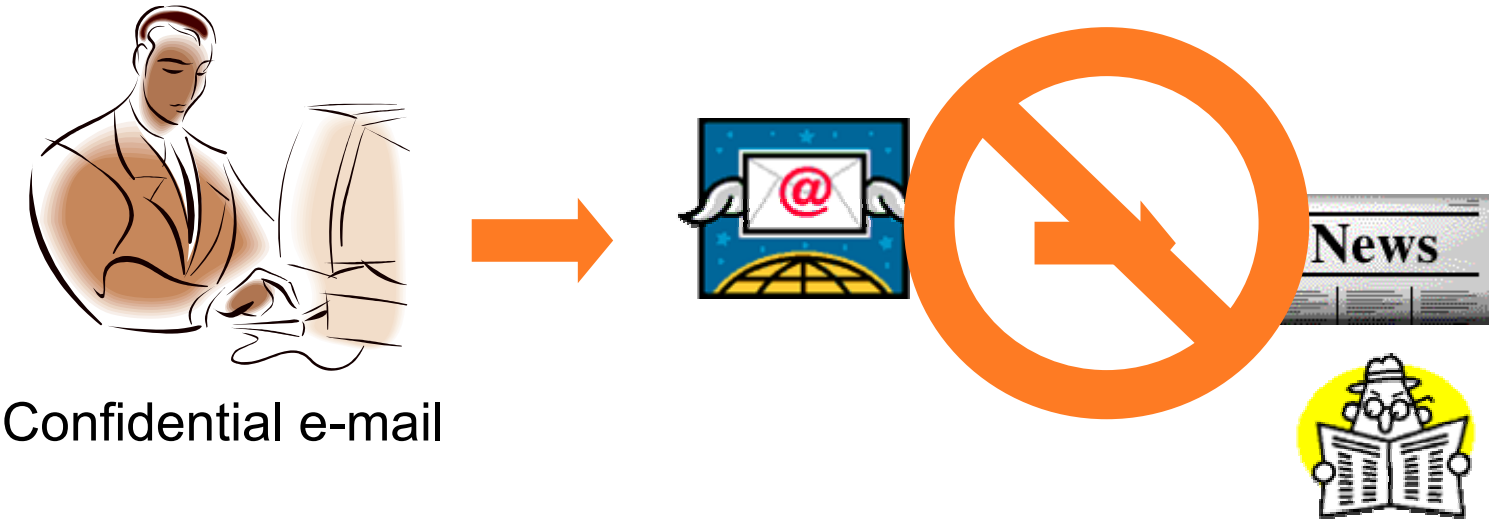


- Parties communicate using cryptographic protocols designed so that:
  - Client learns desired statistics, but learns nothing else about data (including individual values or partial computations for each database
  - Servers do not learn which fields are queried, or any information about other servers' data
  - Computation and communications are very efficient

Initial Experimental Results



Type-Based Distributed Access Control (Dominic Duggan)



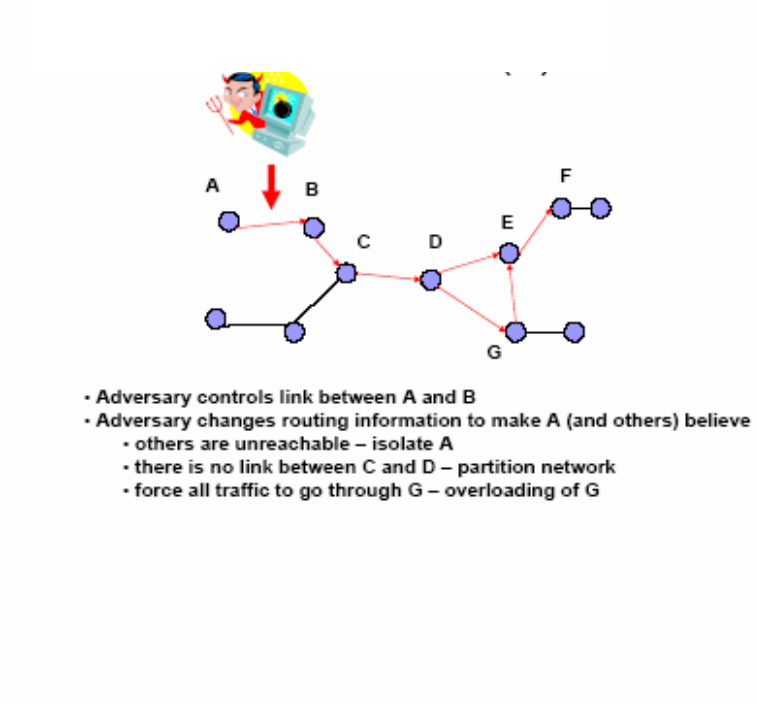
Confidential e-mail

Problem: Data leaving owners environment has limited protection

- Investigate use of type checking in combination with key and data encryption to maintain owner control
  - Data protected by type and encryption
  - Copy operations on local and/or remote machines controlled by type checking

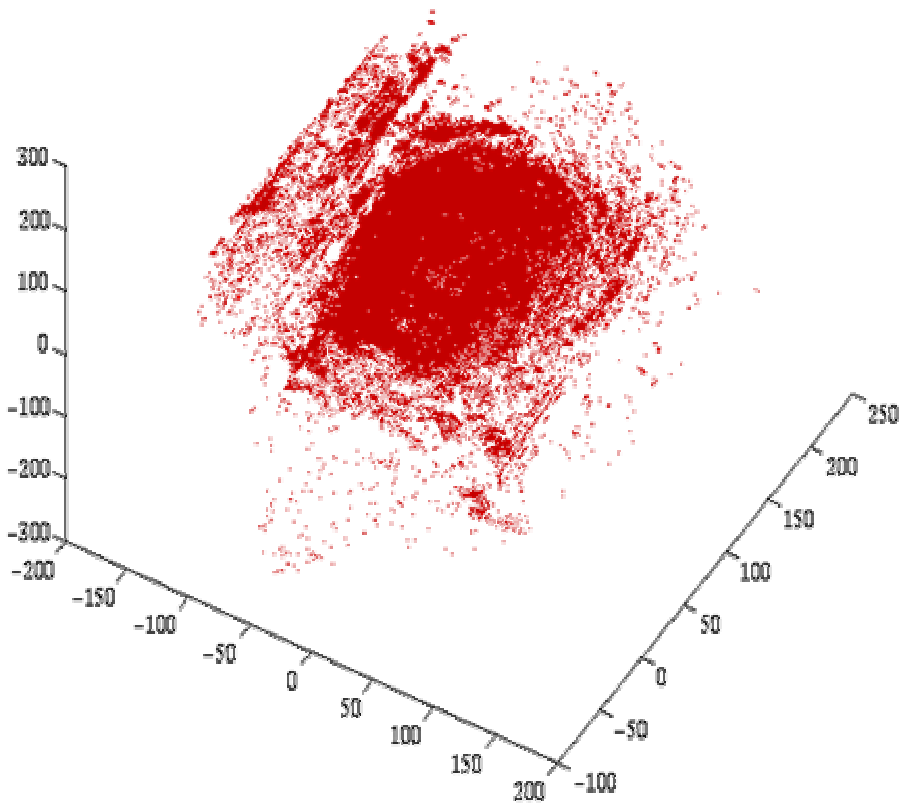
Cyber Security (Susanne Wetzel)

- Explore vulnerability of Ad-Hoc Sensor network fields to a variety of cyber and/or combination (cyber/physical) attacks that disrupt routing tables:
  - Disconnect network nodes
  - Degrade good-put
  - Hi-jack traffic to/from selected nodes
  - Force traffic through a limited number (1?) of nodes to degrade performance, deplete power, etc.



Visualization of Noisy Sensor Data (George Kamberov)

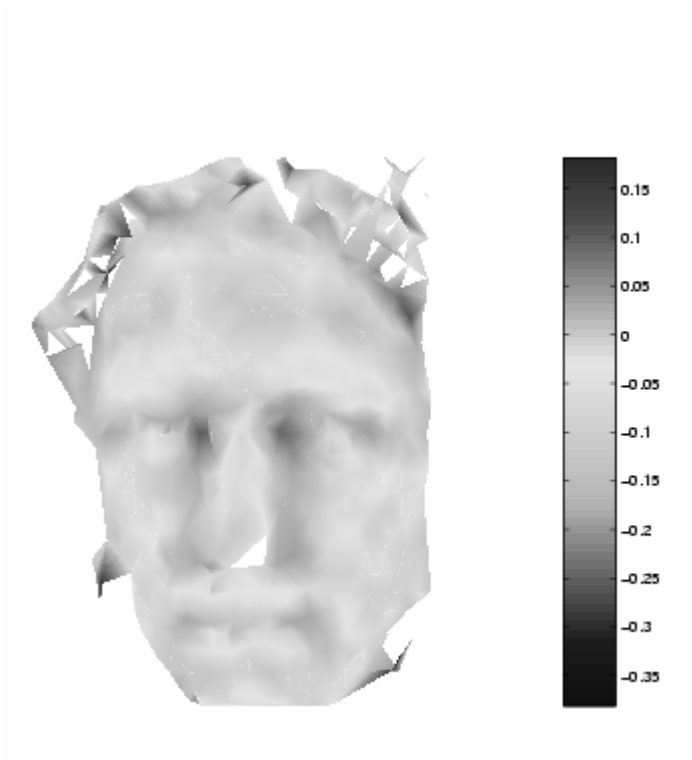
Noisy Input Data



Clean Data

Processing Results & Reconstruction

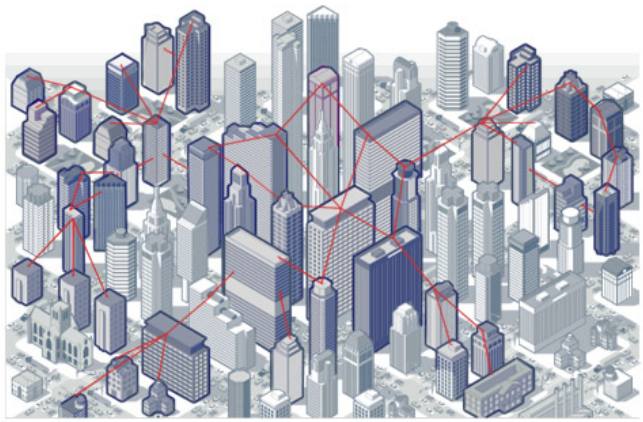
Facial Reconstruction



Facial Feature Line-Based Grids

Photo-Realistic Rendering of Facial Models with Dynamic Texture Mapping

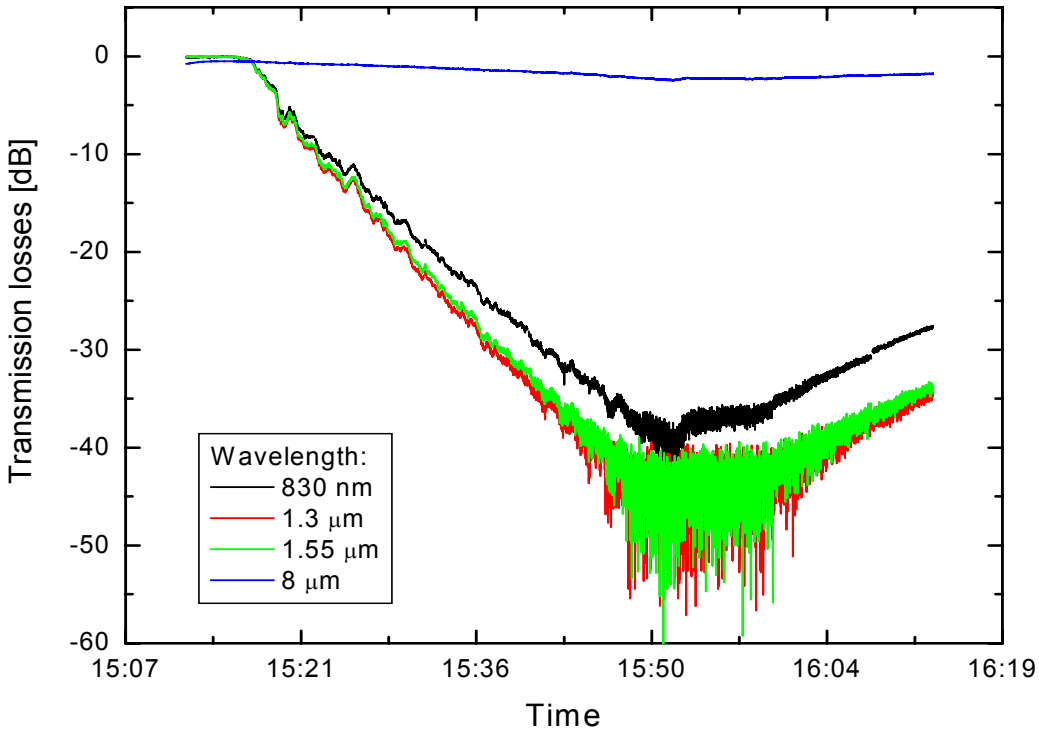
Long λ Laser for Free Space Optics (Rainier Martini)



- Quickly deployed, low cost alternative for access link
  - No digging required – install, aim and go
- Broadband ≥ 10 Gbps capable
- Difficult (impossible?) to intercept or jam
- But typical wavelengths, 830/1330/1550 nm, susceptible to heavy fog

Funded by DARPA

FSO Losses in water fog

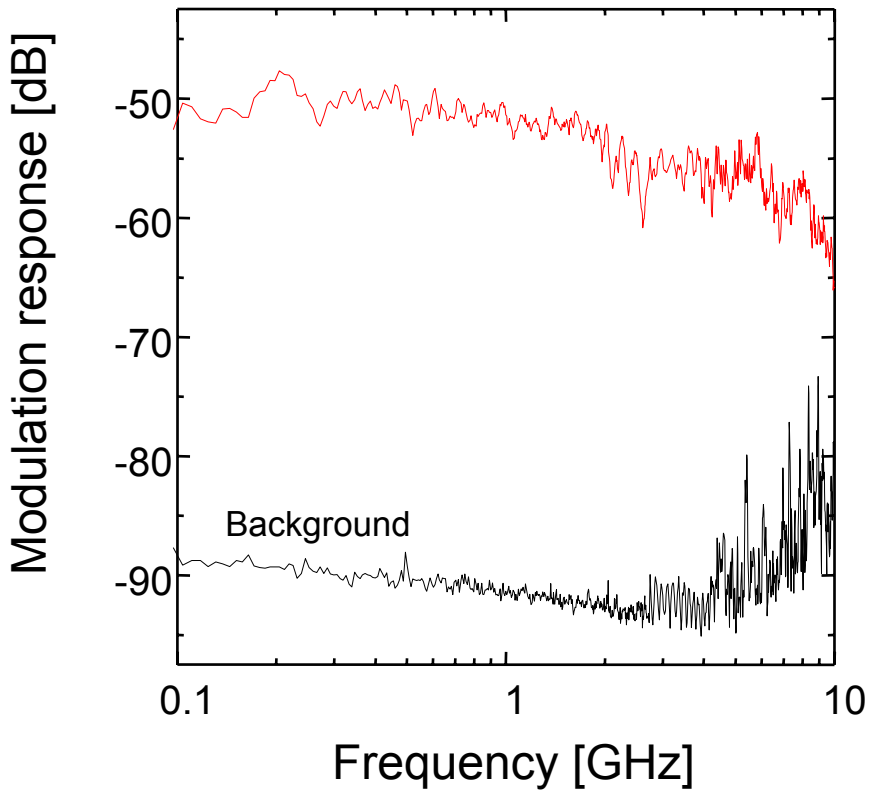


Fog concentration increased with time

- 1.3μm & 1.5μm strongest losses (> 40dB)
- 830nm strong losses (~40dB)
- 8μm nearly no losses (~3dB)

- MIR link allows transmission under extreme fog conditions, no strong differences for classical NIR systems.

QC laser: High modulation bandwidth at 8μm

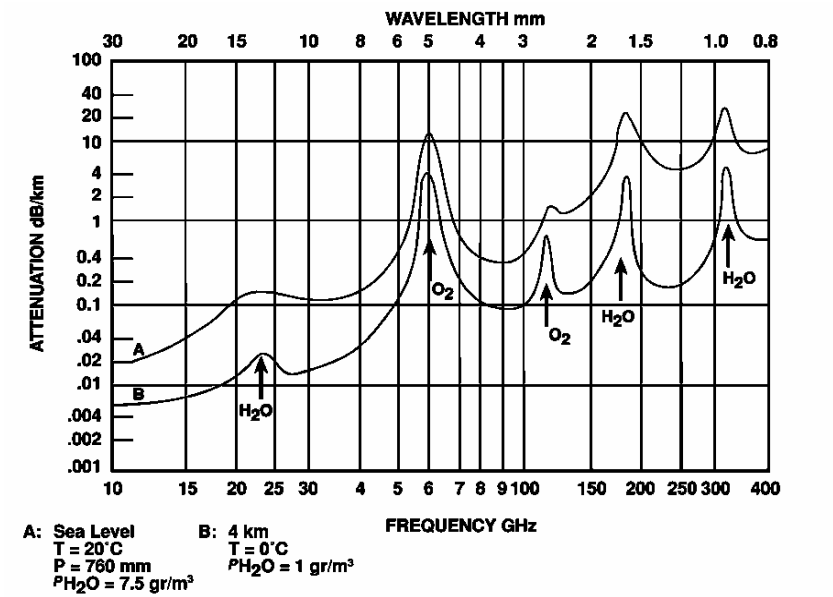


- High frequency limit greater 10 GHz !
- Flat response
- Background due to electrical noise and free radiation
- SNR ~40 dB up to 5 GHz

- No resonance visible

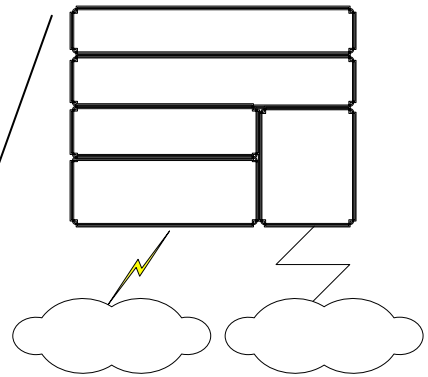
Upper MM-Wave Radio > 28 GHz

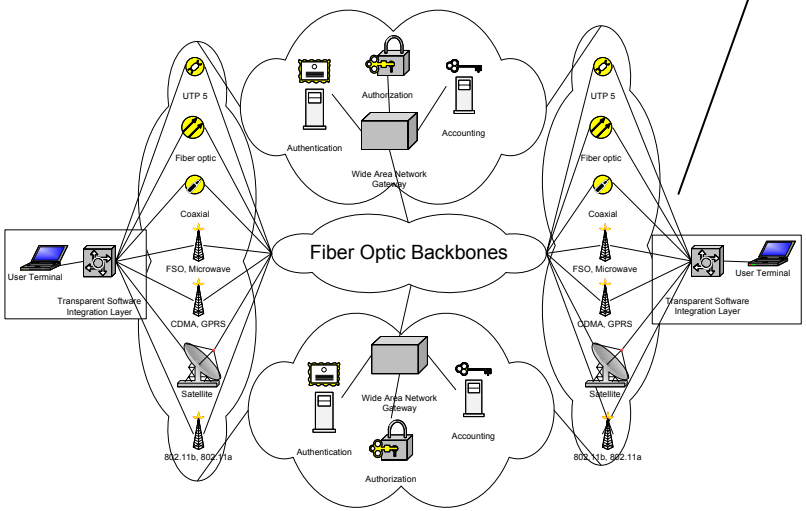
- High capacity, e.g., 10 Gbps, point-to-point Ethernet up to 1km
- High frequency reuse – narrow beams cover small areas (less beam divergence, more limited propagation)
- With high O_2 absorption, can provide in-building security; e.g., confine propagation to room.
- Also minimal interference, guaranteeing relatively clean signal reception.
- Less susceptible to fog, but more sensitive to heavy rain



Network Research Test Bed (NSF)

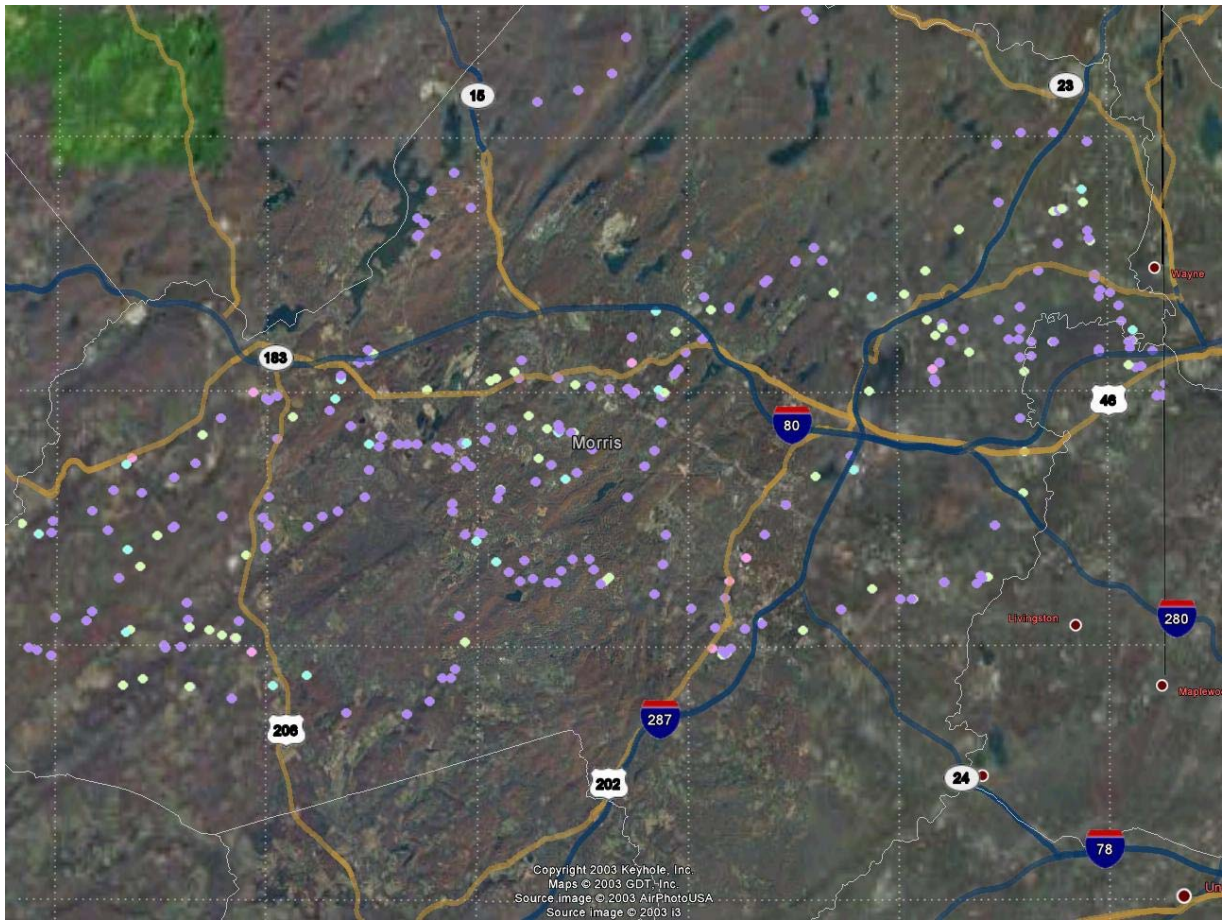
- Simultaneous connectivity to multiple networks
- Automatic selection of network with best available capability
- Maximize availability/performance & Coverage



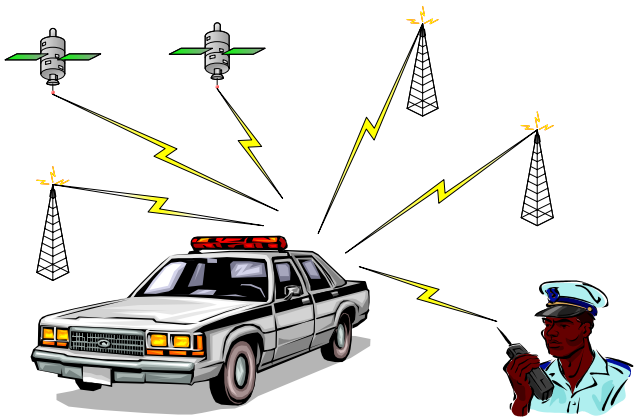


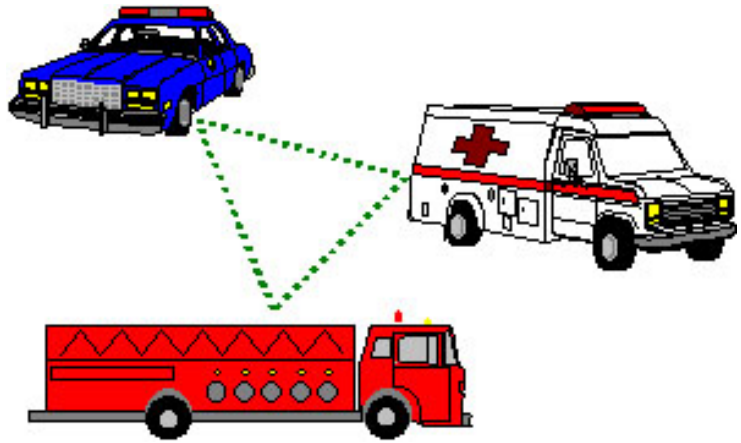
- Optimize spectral & energy efficiency
- Provide extra dimension in security

Network of Networks for Public Safety



A Hybrid Solution for Coverage and Interoperability





- Car maintains connectivity (via software radio) to multiple wireless networks – interoperability **<u>with</u>** national coverage, minimal dead spots
- Messages automatically sent to network with best instantaneous performance
- Outside the car, option to use the car to relay messages
- Most modifications limited to radio in the car, minimizing cost and deployment interval

GPS

Iridium/Globalstar/Inmarsat

Thank You

Patrick White
Center for Wireless Network Security