

SMASNET:

Secure Mobile Adhoc Sensor Network

<http://cs.uccs.edu/~smanet/>

A NISSC Sponsored Project

C. Edward Chow (PI)

Paul J. Fong

Ganesh Godavari

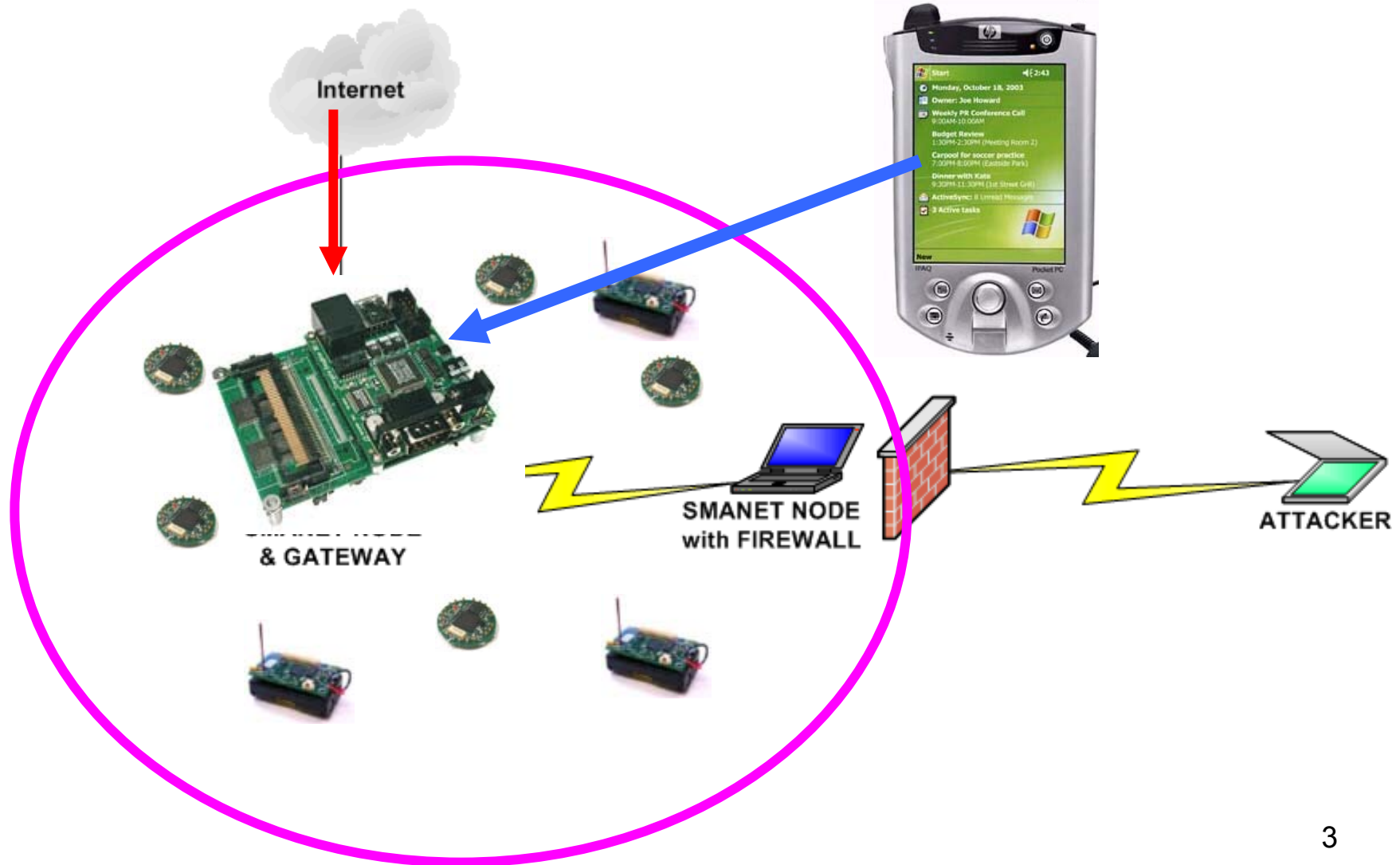
Department of Computer Science
University of Colorado At Colorado Springs

Part of this work is based on research sponsored by the Air Force Research Laboratory, under agreement number F49620-03-1-0207. it was sponsored by a NISSC summer 2003 grant.

Goal

- Provide First Responders with timely secure sensor information.
- Integrate Wireless Sensor Nodes with Secure Information Delivery Devices.
- Explore techniques for deploying wireless sensors. Both preplanned and dynamically.
- Investigate sensor algorithms for detecting and verifying movement
- Develop secure group communications among sensors, gateway, and access devices.

Secure Access to/among Wireless Sensors



Mac Filtering based SMANET

```
#!/bin/sh
# NODE-FILTER
# eth0: wireless port
# eth0 is sole communications port
# DROP all wireless packets from the INPUT and FORWARD
  chains
# except those with the following MAC addresses:
#   00:09:B7:7B:B2:58 Cisco 350 PCI
#   00:0A:B7:8B:5C:1D Cisco 350 PCMCIA
# Set default policy on INPUT & FORWARD chains to DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
# Apply INPUT chain filtering to wireless port eth0
iptables -A INPUT -i eth0 -p ALL -m mac --mac-source
  00:09:B7:7B:B2:58 -j ACCEPT
iptables -A INPUT -i eth0 -p ALL -m mac --mac-source
  00:0A:B7:8B:5C:1D -j ACCEPT
# Apply FORWARD chain filtering to wireless port eth0
iptables -A FORWARD -i eth0 -p ALL -m mac --mac-source
  00:09:B7:7B:B2:58 -j ACCEPT
iptables -A FORWARD -i eth0 -p ALL -m mac --mac-source
  00:0A:B7:8B:5C:1D -j ACCEPT
```

Node Firewall Filter

```
#!/bin/sh
# GATEWAY-FILTER
# eth0: gateway port
# eth1: wireless port
#
# DROP all wireless packets from the INPUT and
  FORWARD chains
# except those with the following MAC addresses:
#   00:09:B7:7B:B2:58 Cisco 350 PCI
#   00:0A:B7:8B:5C:1D Cisco 350 PCMCIA
# Set default policy on INPUT & FORWARD chains to
  DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
# ACCEPT all packets on gateway port eth0
iptables -A INPUT -i eth0 -p ALL -j ACCEPT
iptables -A FORWARD -i eth0 -p ALL -j ACCEPT
# Apply INPUT chain filtering to wireless port
  eth1
iptables -A INPUT -i eth1 -p ALL -m mac --mac-
  source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A INPUT -i eth1 -p ALL -m mac --mac-
  source 00:0A:B7:8B:5C:1D -j ACCEPT
# Apply FORWARD chain filtering to wireless port
  eth1
iptables -A FORWARD -i eth1 -p ALL -m mac --mac-
  source 00:09:B7:7B:B2:58 -j ACCEPT
iptables -A FORWARD -i eth1 -p ALL -m mac --mac-
  source 00:0A:B7:8B:5C:1D -j ACCEPT
```

Gateway Firewall Filter

Authenticate Access

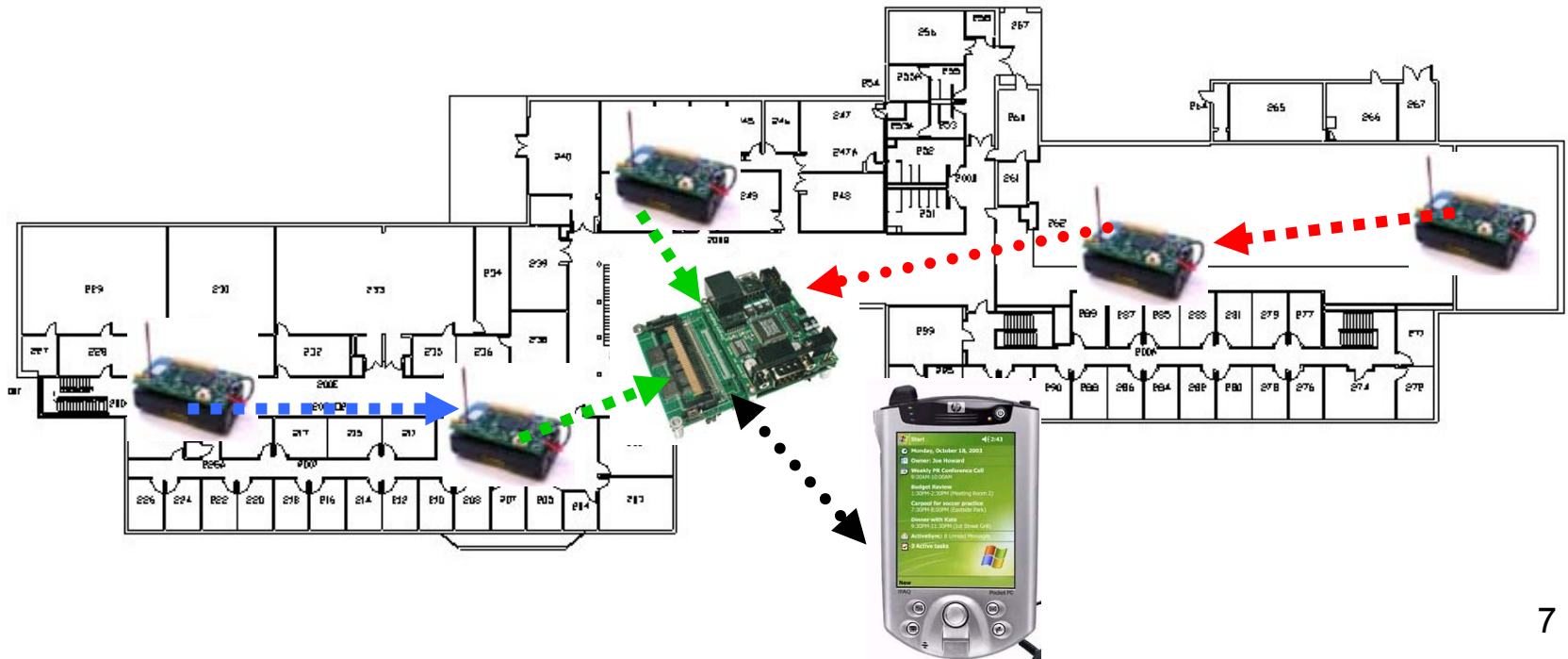
- Mac address-based access not secure.
- Apply PEAP/TTLS certificate-based authentication for Wireless Mobile Ad Hoc Network Access.
- Share Radius servers or each node in the group served as a radius server.

Related Security Problem

- Develop Secure Ad Hoc Distance Vector (SAODV) Routing.
- Avoid black hole routing attack.
- Develop Firewall+IDS for intrusion handling and compromise node detection.

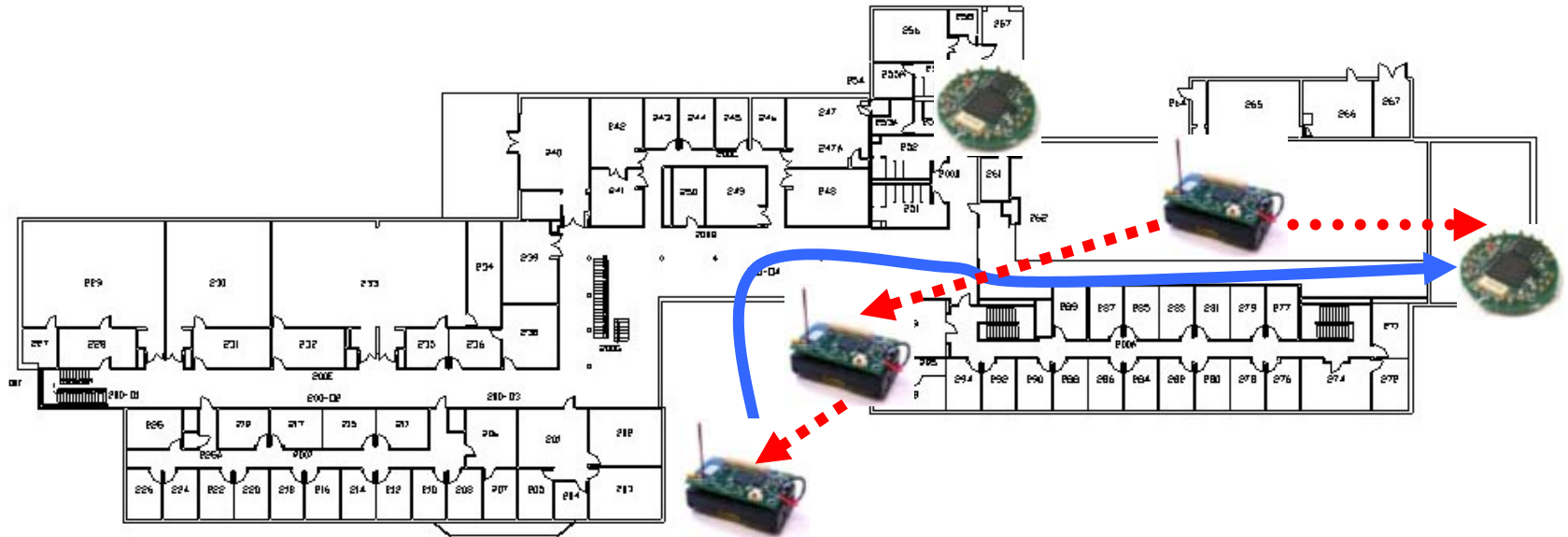
Scenario 1: Preplanned Wireless Sensors

- Building is surveyed and deployed with wireless sensors and include floor plan info in the gateway device.
- When there is fire, first responders can tap into the secure wireless sensor network to find the condition of the building and over with the floor plan picture.



Scenario 2: Dynamically Deploy Sensors

- Fire Fighter drops the wireless sensors along the route in.
- If sensors detects temperature increase or location movement!!, they relay the date through multiple hop wireless sensor network to both the team inside and the team outside.



Secure Access to Sensor Network

- Terrorist may access the sensors and information on the gateway.
- Need authentication for secure access.
- Need encryption for avoid sniffing by terrorist.
- Need redundancy for fault tolerance and verifying the sensor results.

WSN Devices We are Exploring

- Wireless Sensors:
 - Mica2 motes
 - 433MHz Radio; Atmega128 processor, Flash memory
 - mount additional sensor board for Temperature, Magnetic, Light, Accoustic measurements.
 - Red, Green, Yellow Leds.
 - Mica2dot motes
 - 433MHz Radio; Atmega128 processor, Flash memory
 - Built-in temperature measurement.
 - One Red Led.
- Stargate Sensor Network Gateway
 - With 802.11b and Fast Ethernet for relay info
 - Fast StrongArm Processor and more memory
- PDA or Laptop with Mobile Ad Hoc Network and Secure Groupware as information delivery devices