Wireless Systems Security

EE/NiS/TM-584-A/WS

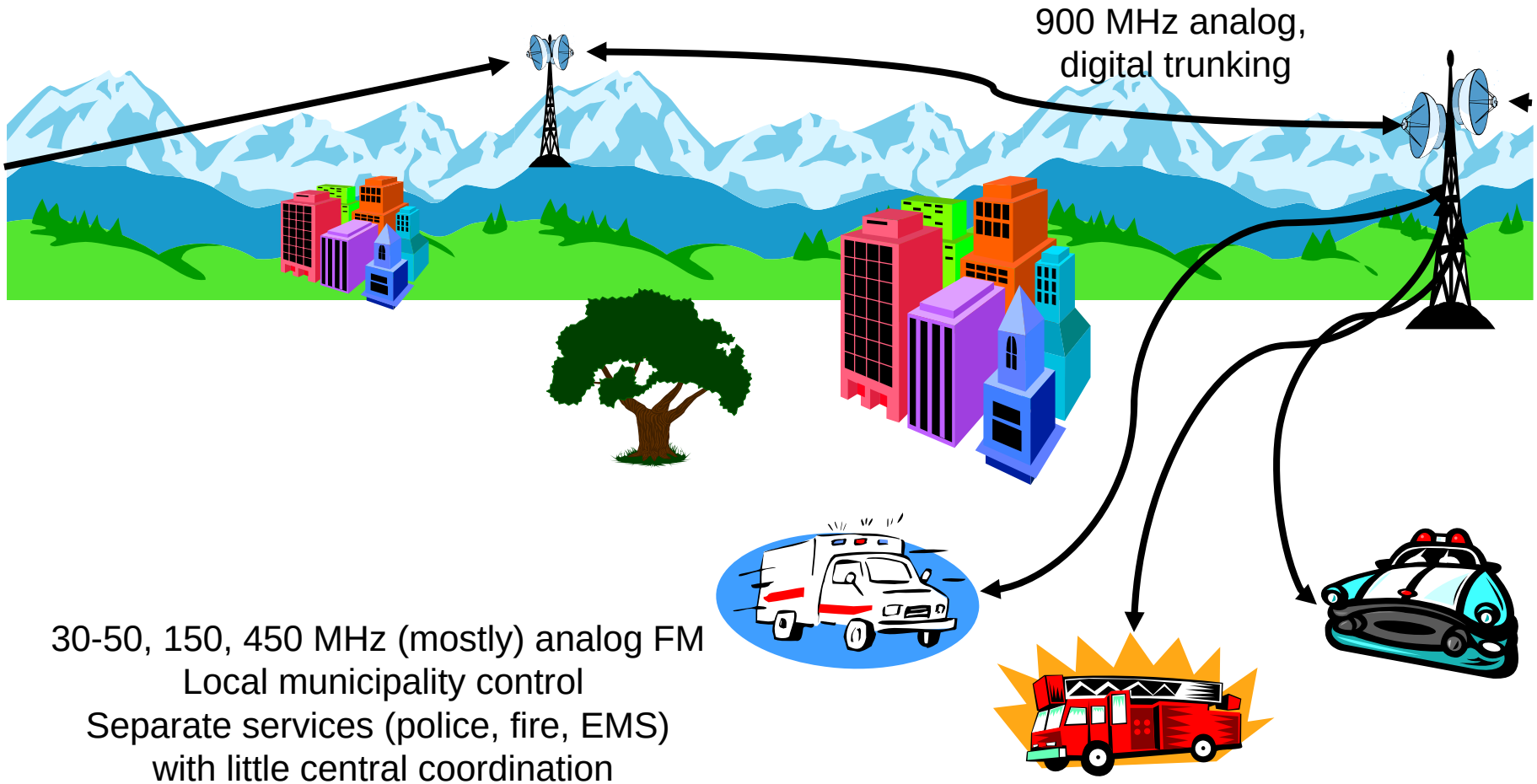
Bruce McNair
bmcnair@stevens.edu

Week 6 - Wrapup

Case Study 2

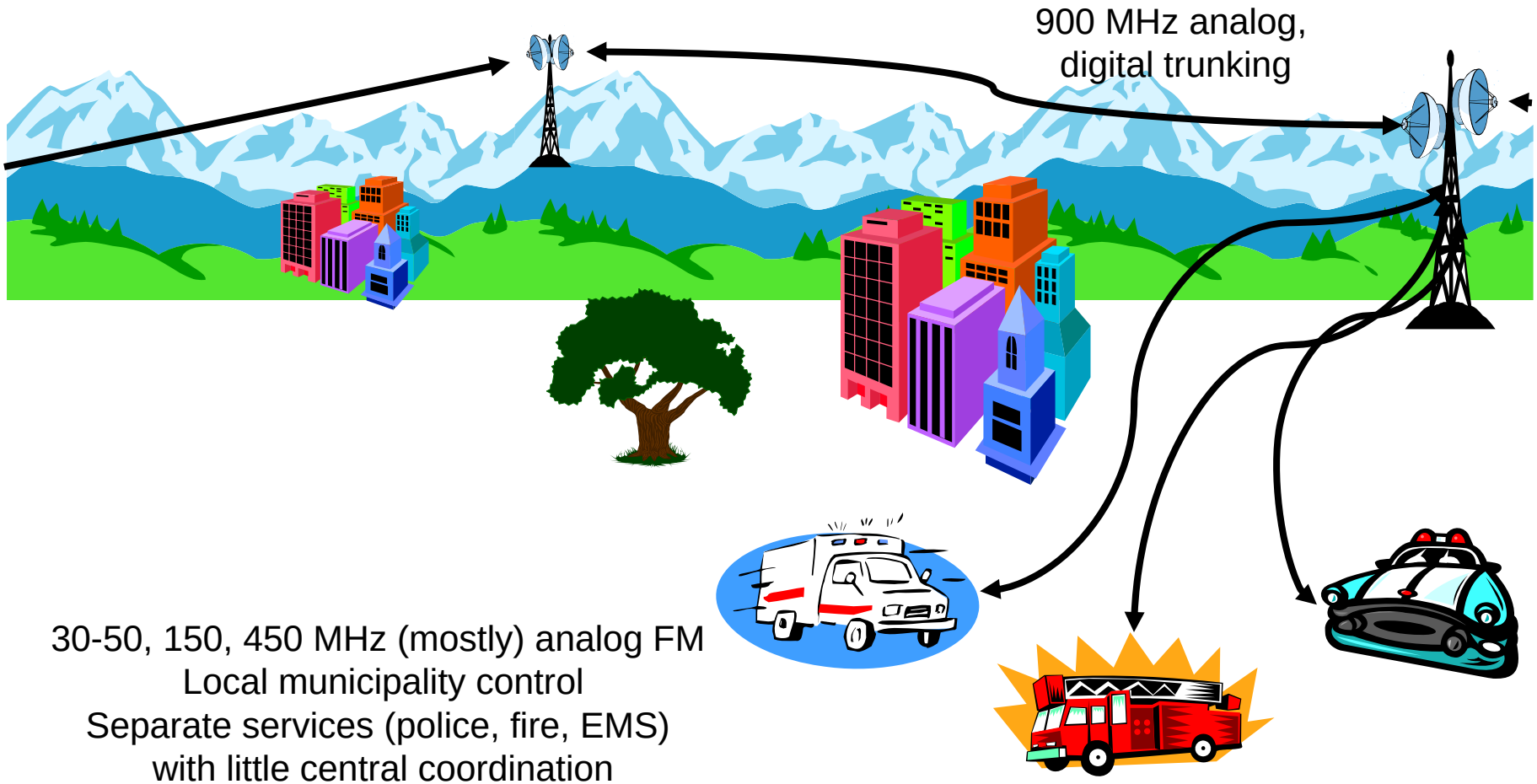
Summary and observations

Case 2 – Public Safety Wireless Networks

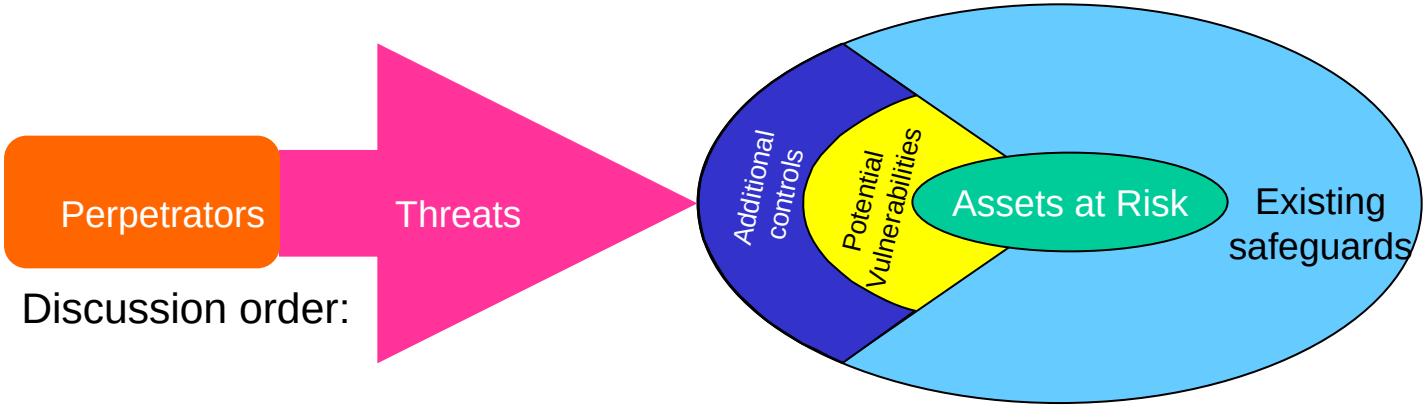


30-50, 150, 450 MHz (mostly) analog FM
Local municipality control
Separate services (police, fire, EMS)
with little central coordination
Some point-to-point; heavy use of RF repeaters

Case 2 – Public Safety Wireless Networks

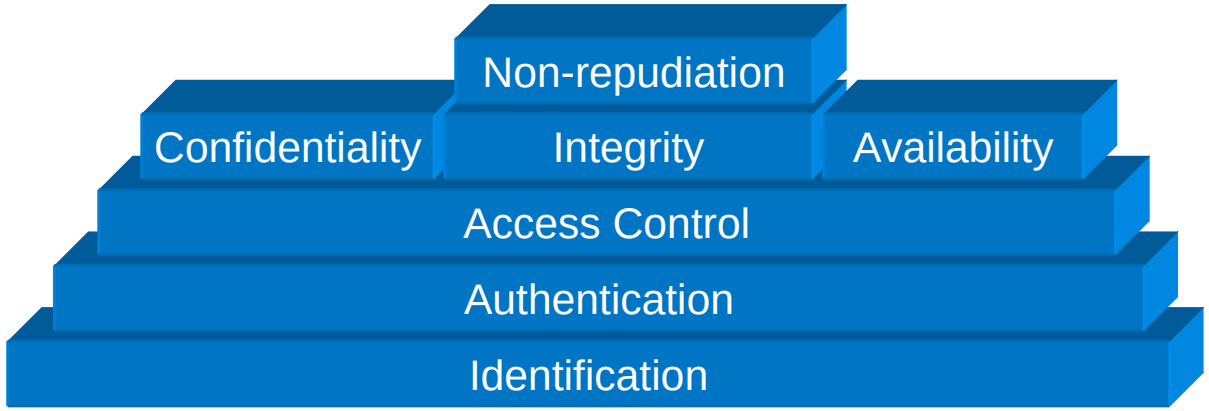


30-50, 150, 450 MHz (mostly) analog FM
Local municipality control
Separate services (police, fire, EMS)
with little central coordination
Some point-to-point; heavy use of RF repeaters



Discussion order:

- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls



Assets

Mobility
Equipment (Relay equipment, HTs, vehicular)
Frequencies
Codes being used
Information being carried
- *Driver's license number*
- Criminal record
- Address
- Credit card numbers

Secret operations
Tower
Antennas
Receiver
Lives of public service personnel
Ability to communicate important information in a timely manner
Actual communications transaction
Location of activity/event
Availability of communications link
Physical infrastructure – towers, radios, antennae
Bandwidth
First responder's lives
DB of private information (e.g., NCIC)
Property and lives of citizens to be protected

Perpetrators

Drug dealers
Criminals (organized crime)
Ham radio operators
Media
Teenagers
Spys
Lawyers
Terrorists
Thrill seekers
Curious listeners
Nature
Equipment vendors
Taxi drivers
(Foreign governments)
Curious listeners
Personal rivals
Disgruntled employees/officers
The media
Hackers
Accidental interferers
Service/equipment provider
Competitor

Threats

Listening
Inserting false information/transmission
Steal BW
Physical destruction of infrastructure
Try to access private information/DB
listen to police call and get to scene of accident/crime and interfere with operations
Exposure of sensitive people or operations (e.g., undercover)
Disruption of prosecution or other long-term operation
Perpetrator learns frequency of operation and then jams/intercepts
Public discovery and access to location of operation/event
Natural disaster, failures
Terrorist attack
Power failure
Jam link
- ***By accident***
- ***For fun***
- ***For profit (e.g., rob bank and prevent response)***

Intercept vehicles
Broadcast false information
Arrive at scene, tamper with evidence
Theft (looting)
Create diversion
- verify its success

Put police, fire, EMS lives in danger
Exposure of private information thru media, damaging a case in progress
Blackmail
Commit crime
Cause damage to receiver (e.g., local EMP)
Identity theft
Cut down tower
Generate signal to cause intentional distortion to jam link
Disrupt/spoil ongoing operation or investigation
Eavesdropping
Steal bandwidth
Generate false transmissions to confuse
Tamper with signal
Rebroadcast over public broadcast radio
Make communications undependable

Existing Safeguards

Encryption
Codes
Proprietary radio systems, proprietary protocols
Hidden frequency of operation
Abitilty to direction-find transmitters
Transmitter generated ID code
Human safeguards:
- Procedures
- Codes
- Recognition of voices

Frequency hopping
Penalties/regulations

Sting operations and false operations to catch miscreants
Physical protection of facilities
Redundancy of facilities
Emergency hot spares

Password protection of DB access
Choice of modulation technique
Protection against jamming
Digital transmission
Legal sanctions/penalties
Management of system
Honeypots
Power control
OOB signaling
Control of equipment distribution
Backup system/facility
Battery or emergency power

Vulnerabilities

Scarce spectrum
Interference
Human error in operations
Spectrum is accessible anywhere
Link is accessible anywhere
RF technology and hacker technologies are widely available
Carelessness
Elevation of antenna/tower attracts lightning
Confusion of modulated signal with noise/interference
Inability to disguise location of transmitter
Known protocols
Leakage of operational information
Budget limitations
Inadequate penalties do not deter misbehavior
Immoral society
Lack of interoperability

Fixed frequency of operation.
Analog transmission
Mostly unencrypted
voice (general operations)
- data (DB access)

generally accessible transmitter and other facilities
no central coordinatoion
interoperability
funding
limited spectrum
inadequate legal penalties
lack of enforcement of legal penalties
inteference
insufficient back up power
flawed software
homogeneous network
failure during system overload/catastrophe

Additional Controls

Profiling attackers
Beamforming
Intrusion detection
Software validation
System validation against security needs [*ASSESSMENT*]