Wireless Systems Security

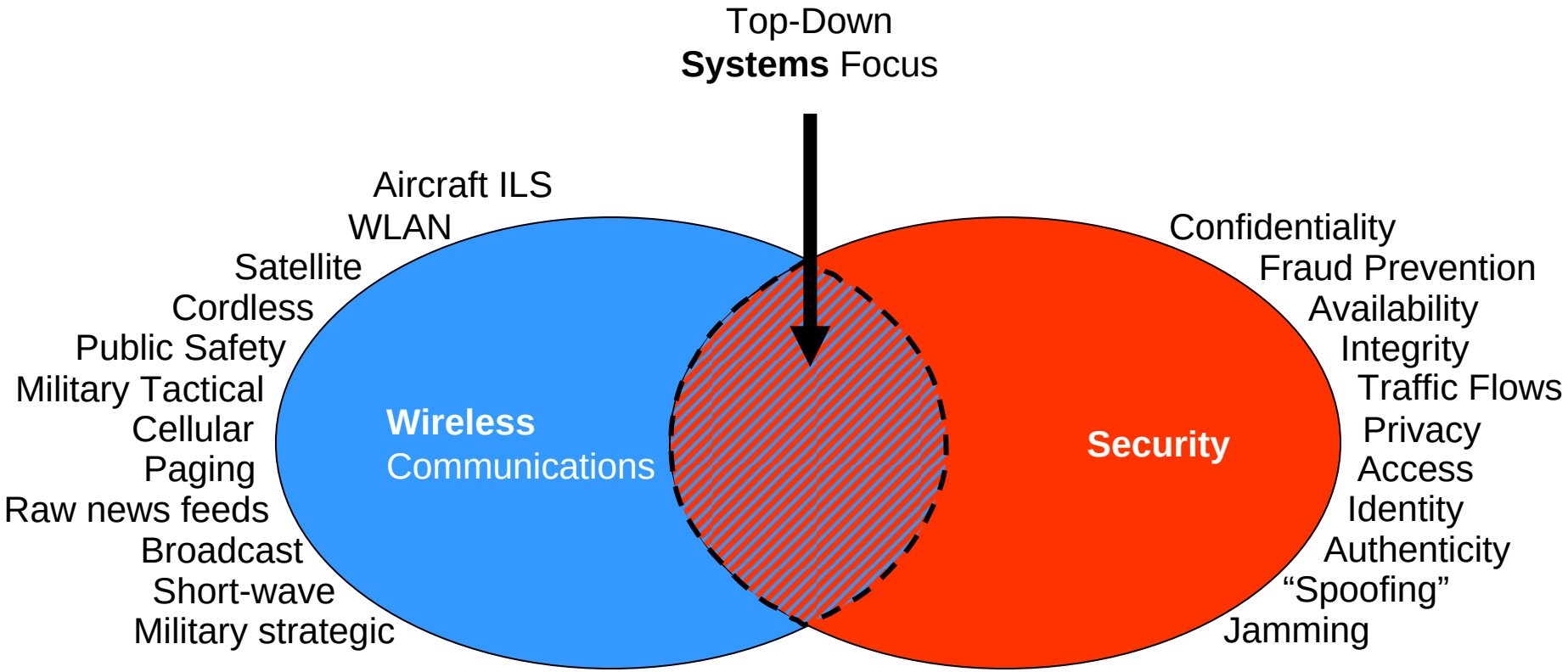
EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

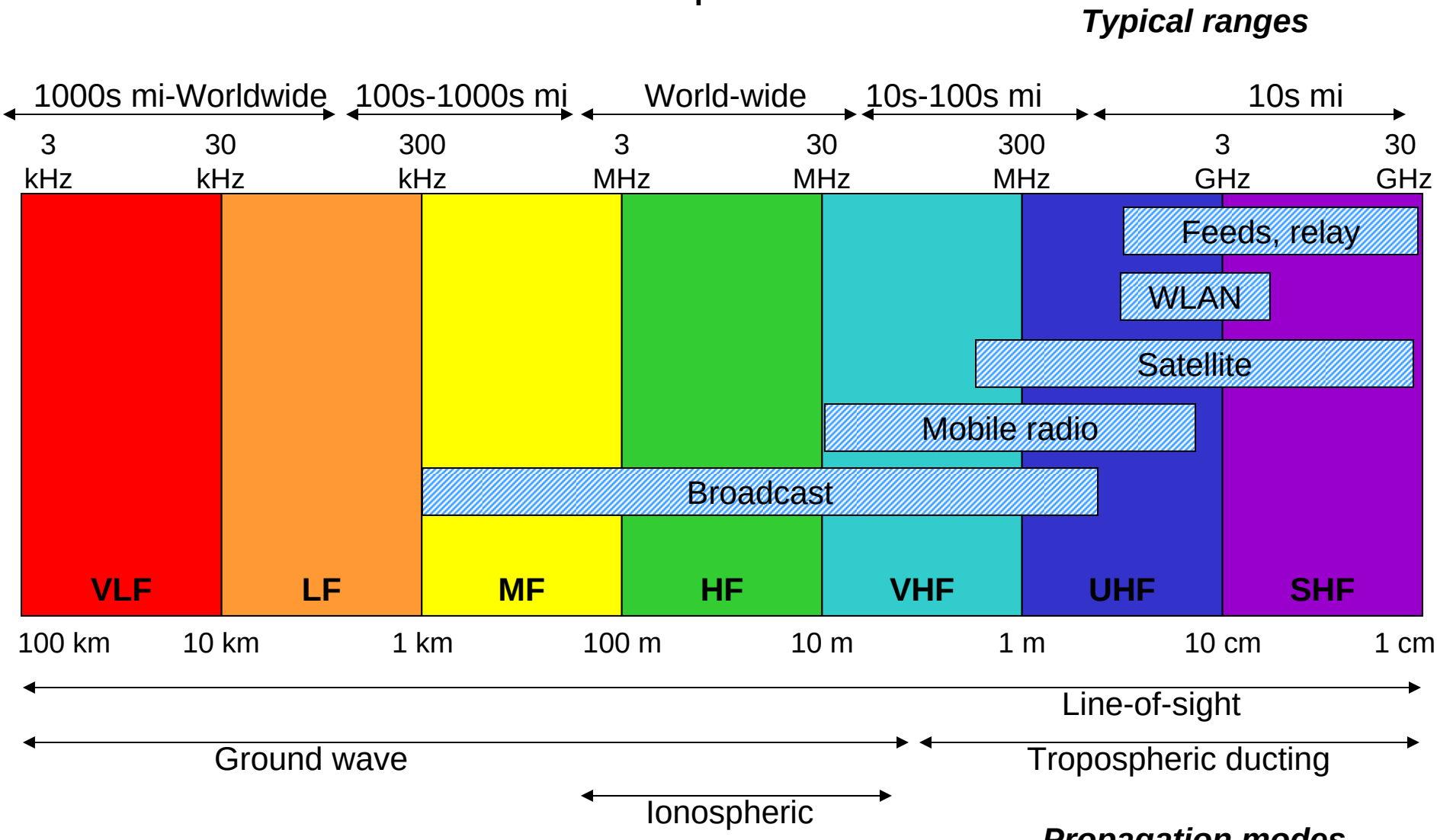
Wireless Systems Security

Class 12 – Wrap-up and Future Directions

The Intersection of Wireless and Security

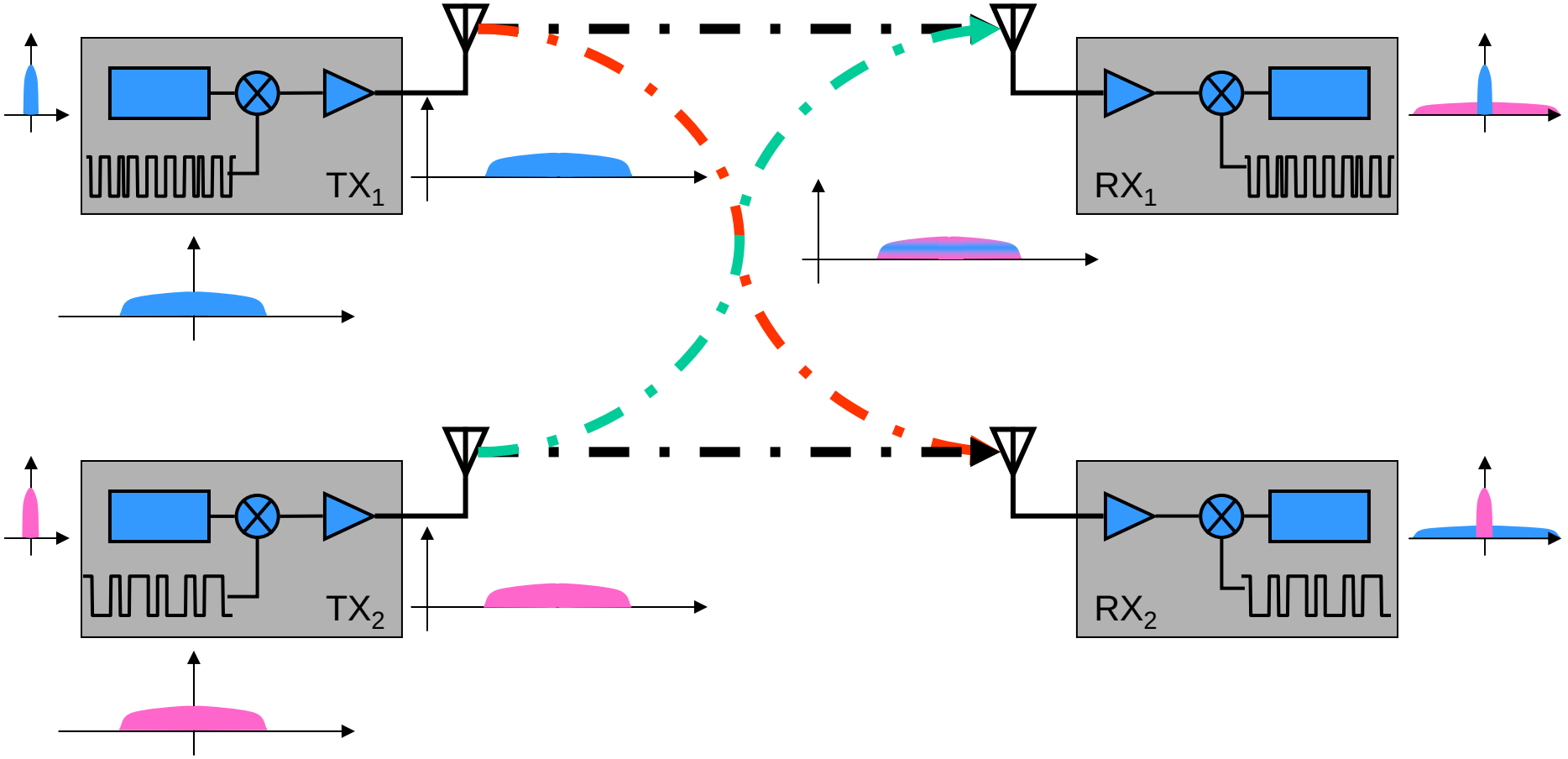


RF Spectrum



See http://www.ntia.doc.gov/osmhome/allochrt.pdf for full details (1996)
Or http://www.jsc.mil/images/speccht.jpg for the military view

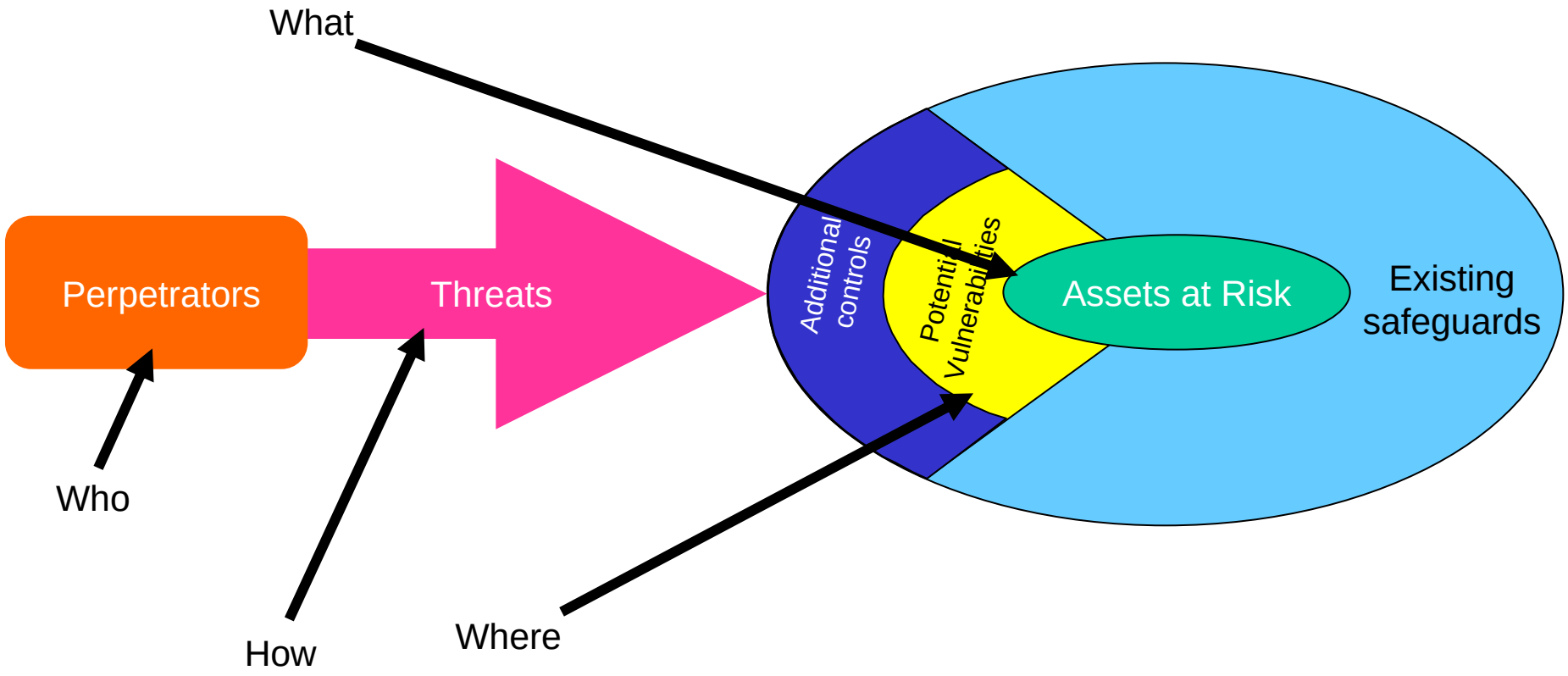
CDMA Spreading and Despreading



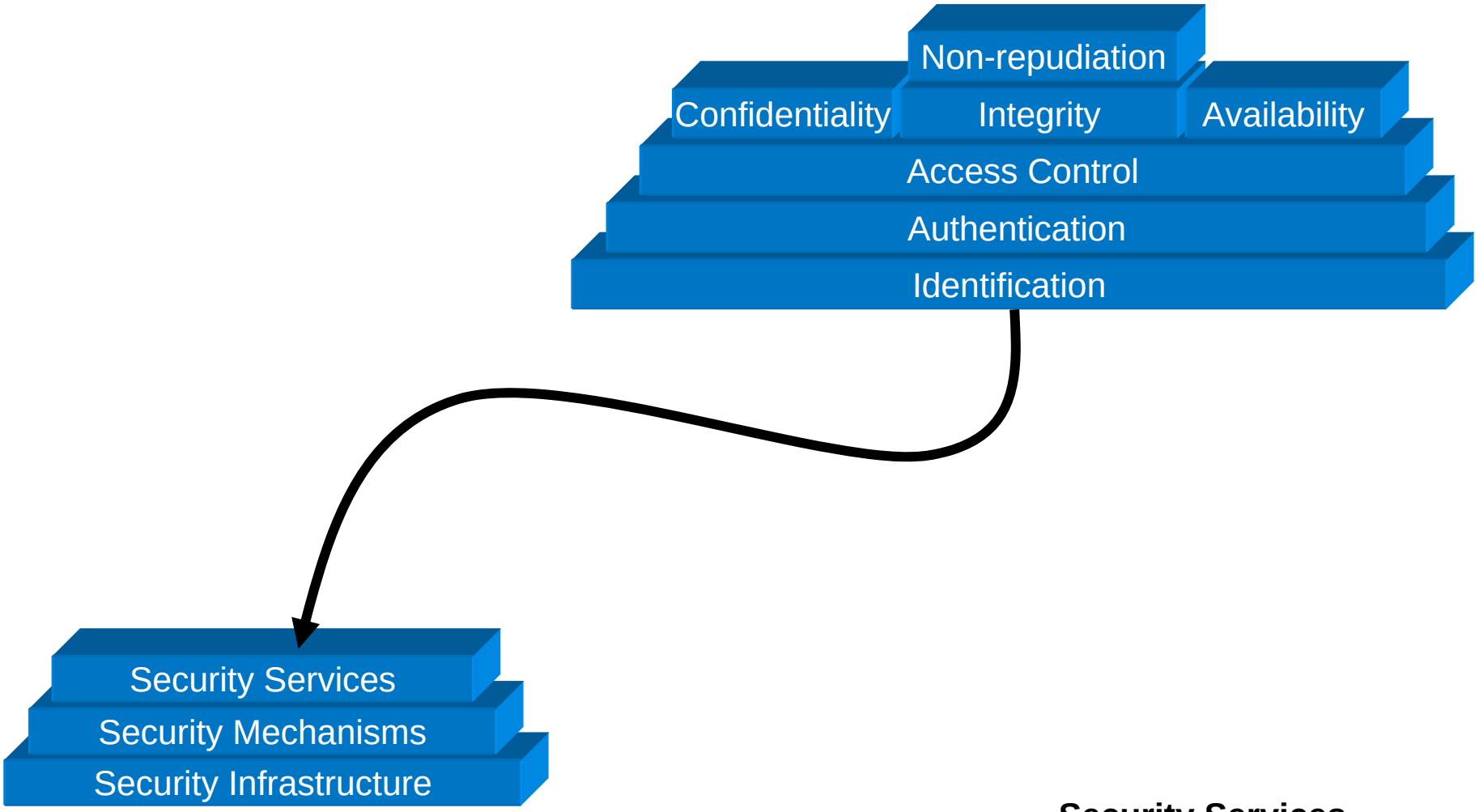
Spreading factor ~ (RF Bandwidth)/(Baseband bandwidth)

How Much Security Is Enough?

A security assessment model

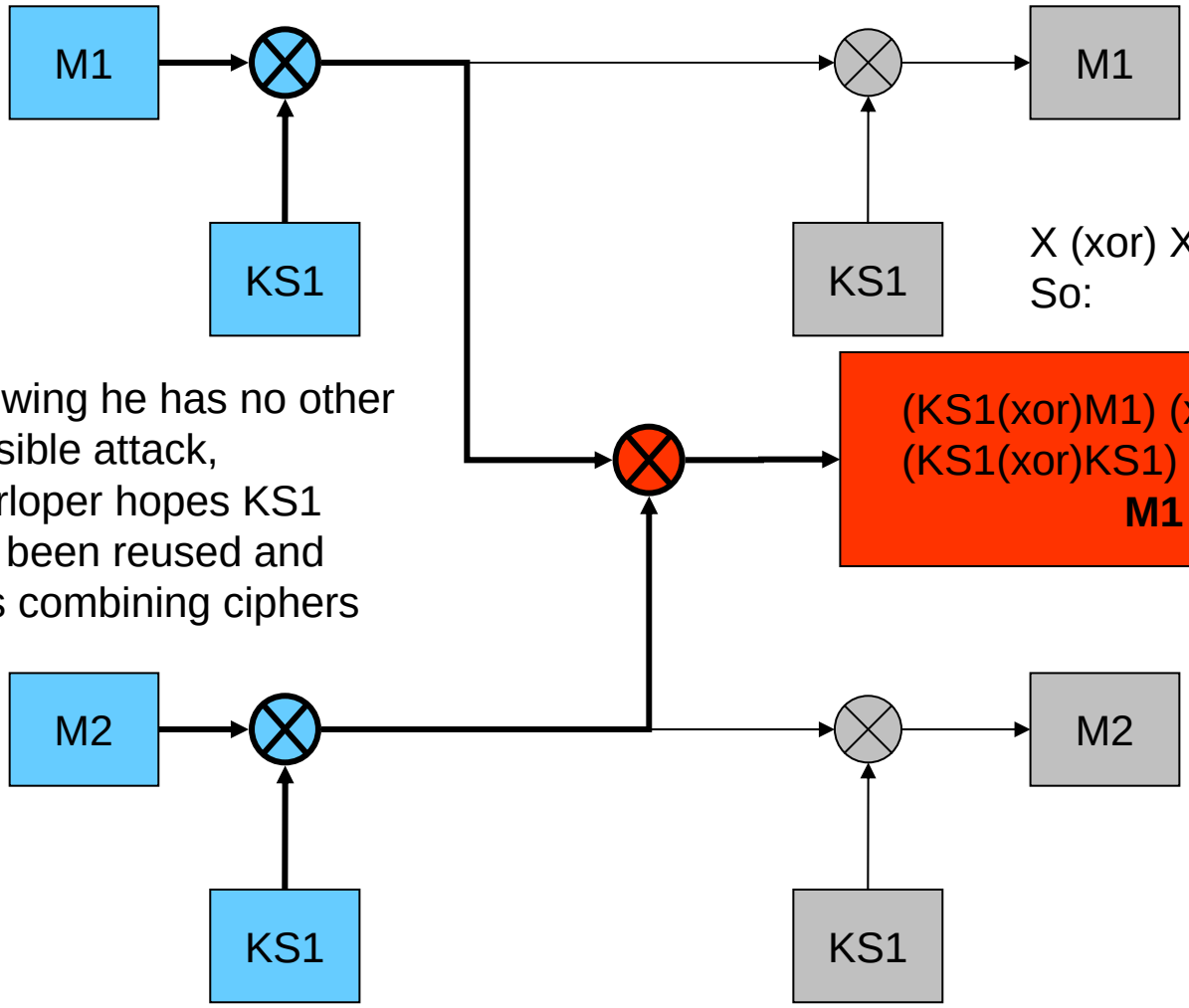


One Structured Way of Viewing Security



Security Services

One-bit-pad Key Reuse



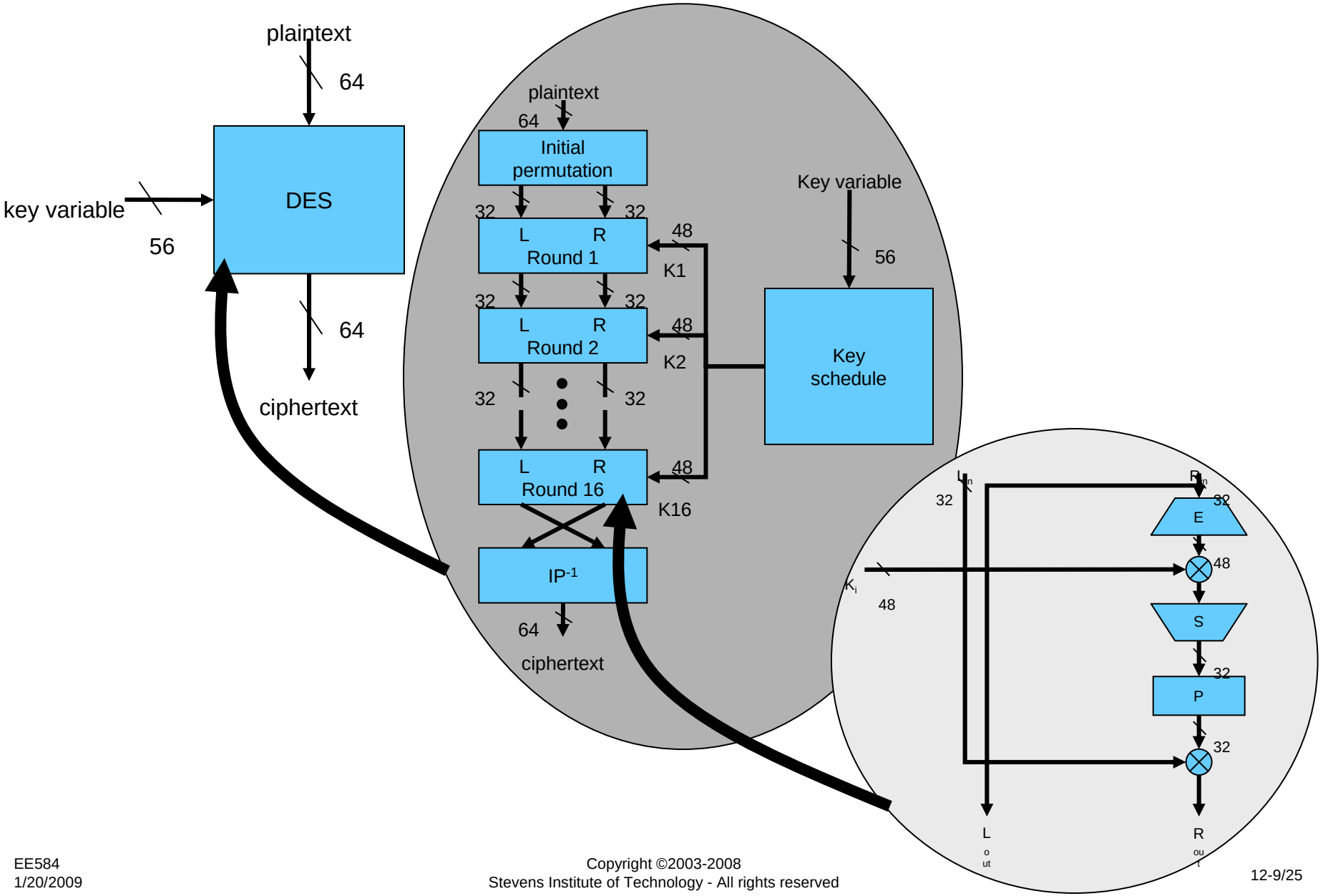
X (xor) X = 0, and Y (xor) 0 = Y,
So:

(KS1(xor)M1) (xor) (KS1 (xor) M2) =
(KS1(xor)KS1) (xor) (M1 (xor) M2) =
M1 (xor) M2

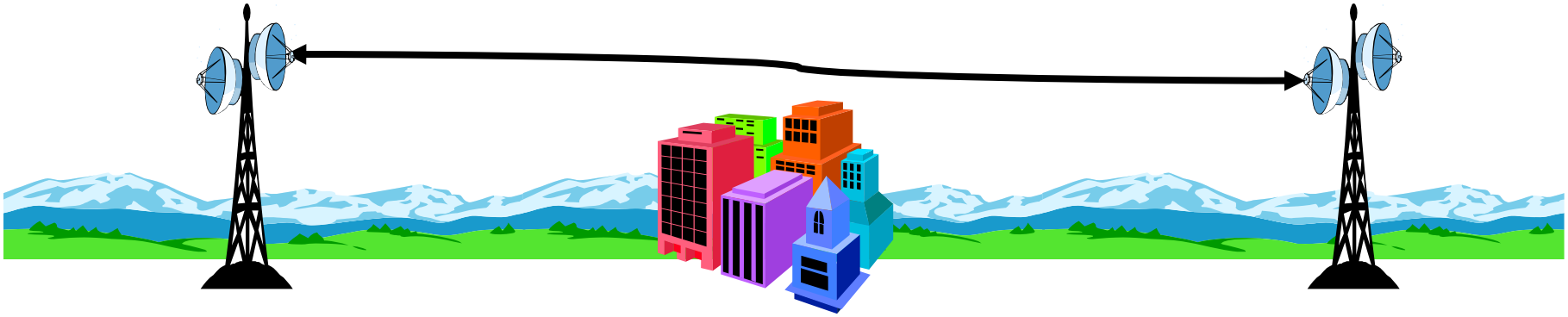
Knowing he has no other possible attack, interloper hopes KS1 has been reused and tries combining ciphers

This is the polyalphabetic encryption of M1 using M2 as a key stream!!

DES as an Example of Encryption Algorithm

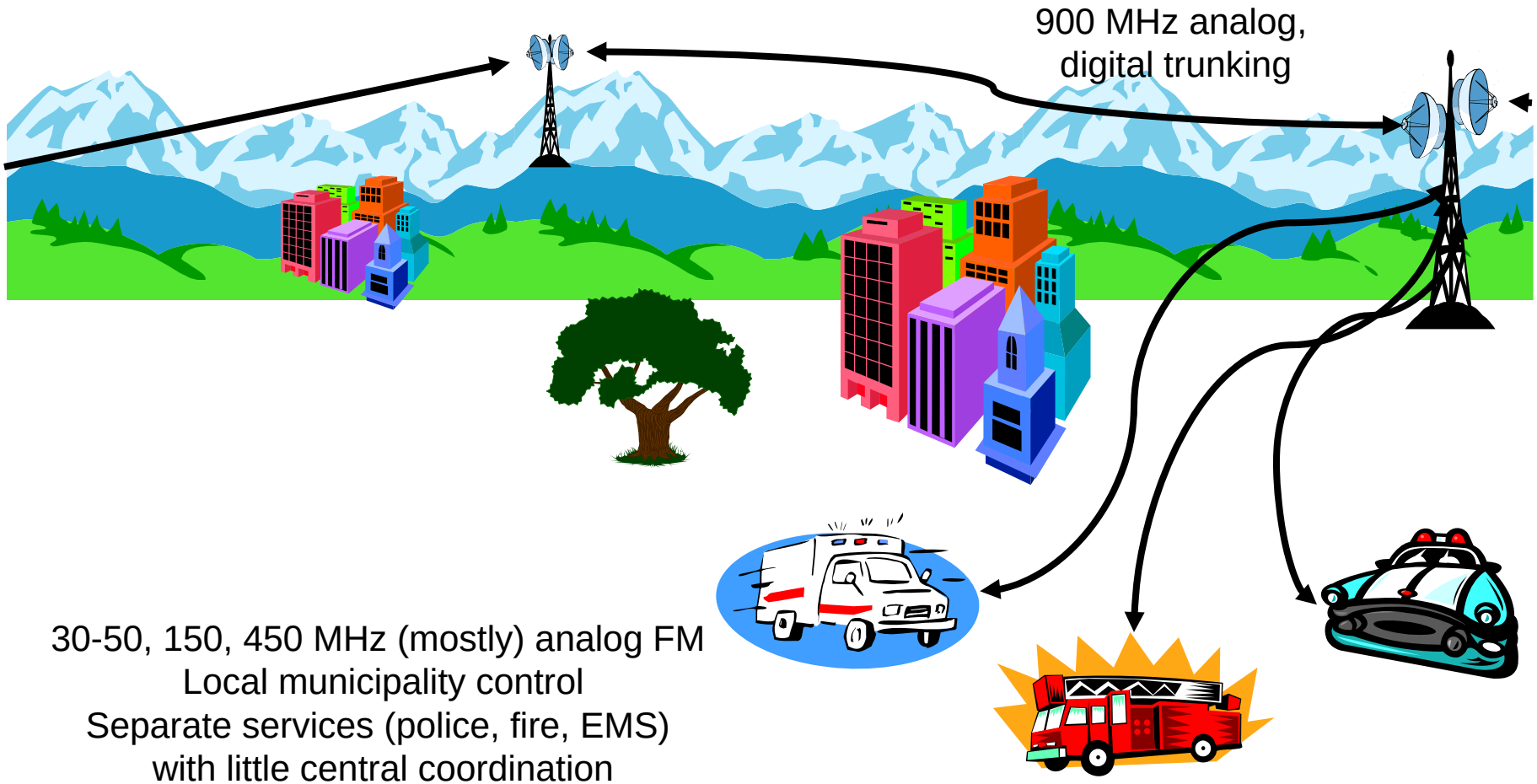


Case 1
Terrestrial Microwave RF Telephone Relay System



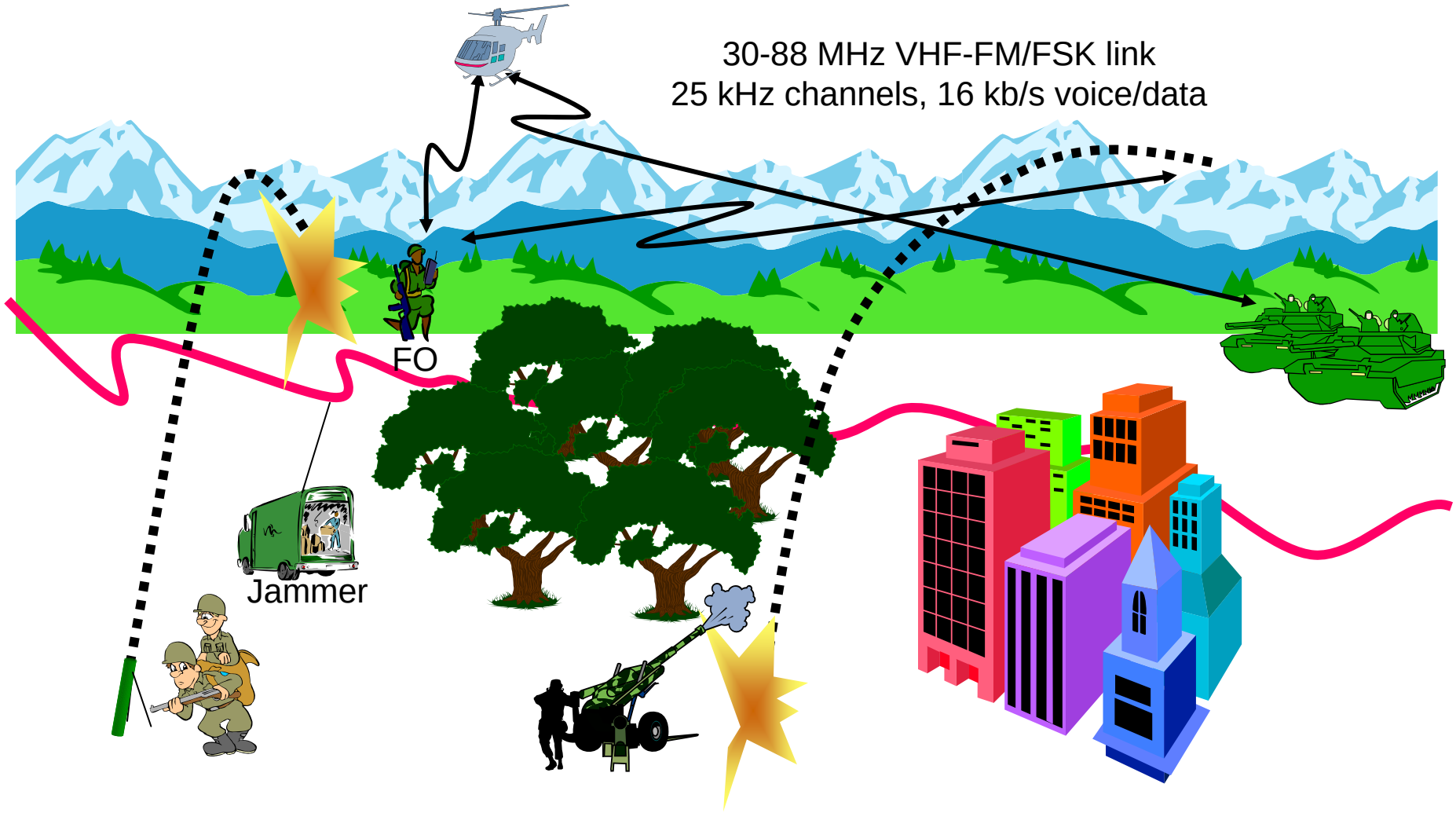
4 GHz
Analog SSB FDMA
Multichannel Voice traffic
CCS signaling
Washington, DC area

Case 2 – Public Safety Wireless Networks

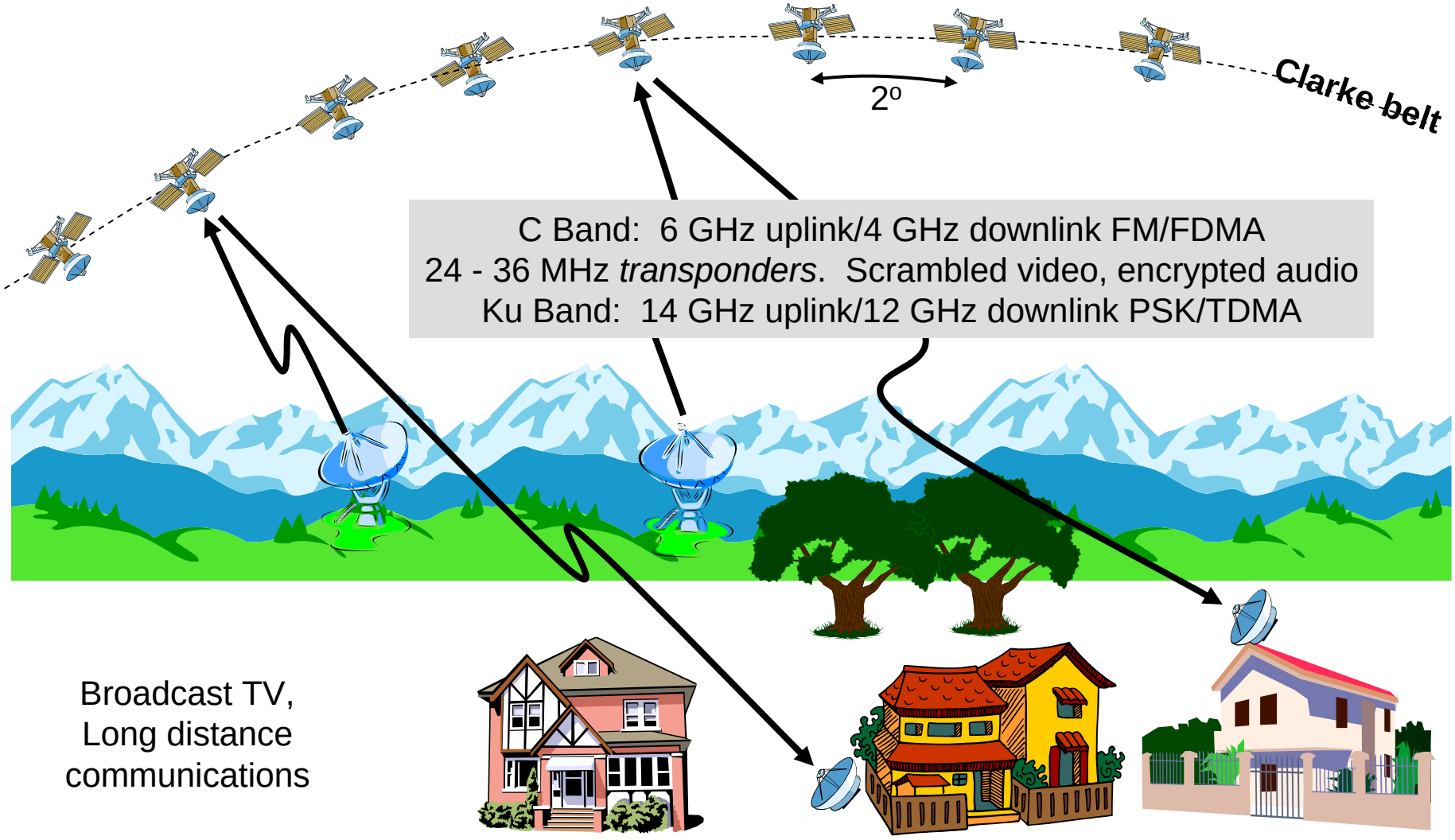


30-50, 150, 450 MHz (mostly) analog FM
Local municipality control
Separate services (police, fire, EMS)
with little central coordination
Some point-to-point; heavy use of RF repeaters

Case 3 – Military Tactical Radio Systems

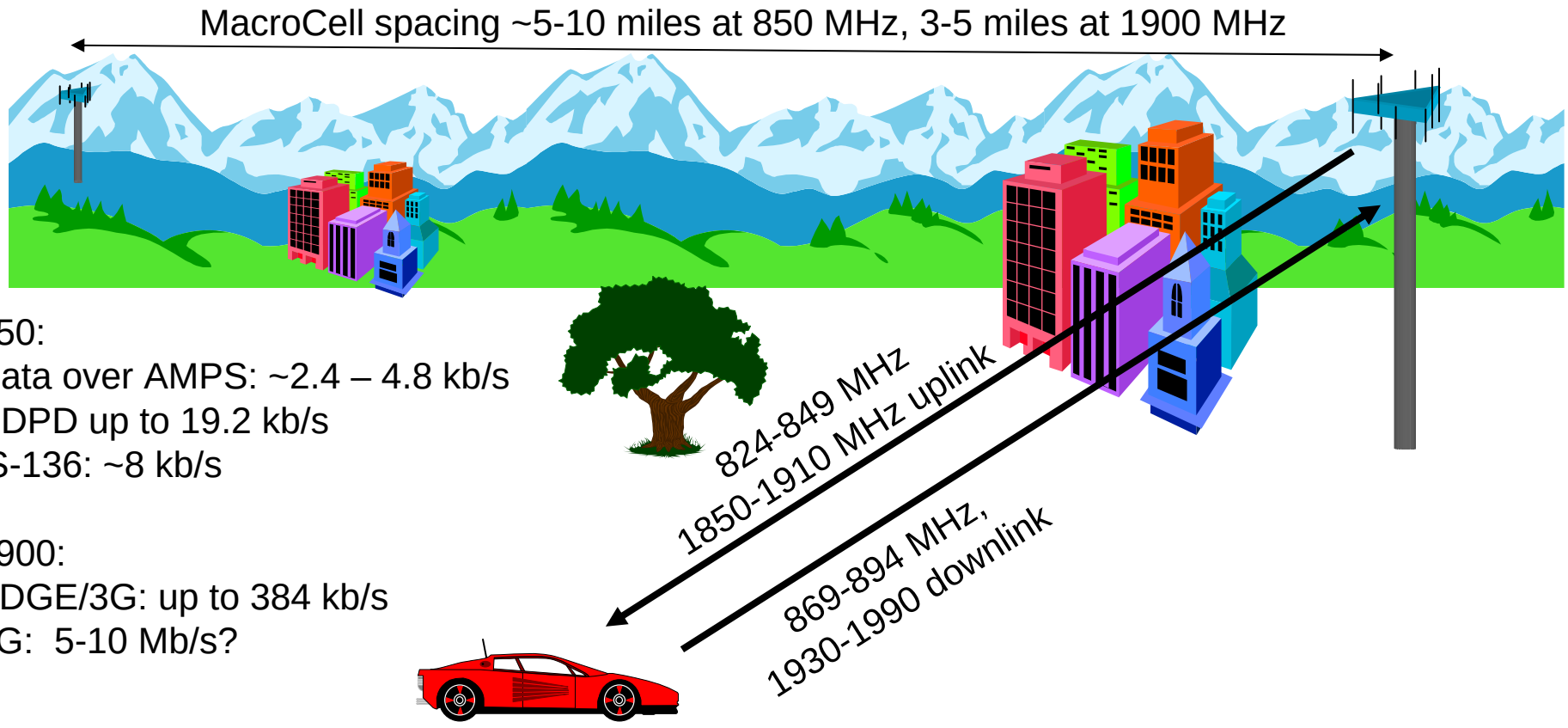


Case 4 – Satellite Communications Systems



Broadcast TV,
Long distance
communications

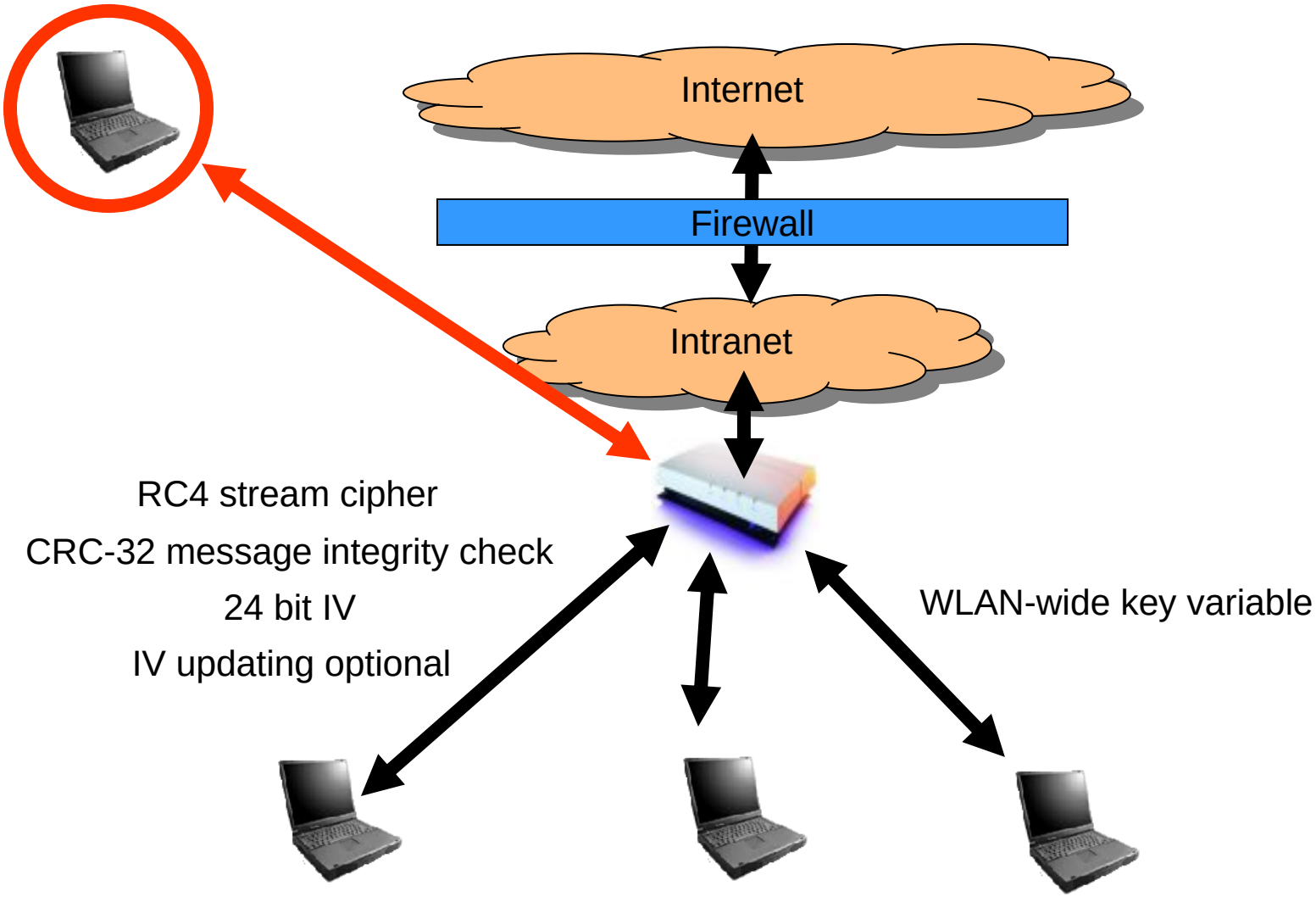
Case 5 – Wide Area Wireless Data Services
CDPD, 3G, EDGE, etc.



850:
Data over AMPS: ~2.4 – 4.8 kb/s
CDPD up to 19.2 kb/s
IS-136: ~8 kb/s

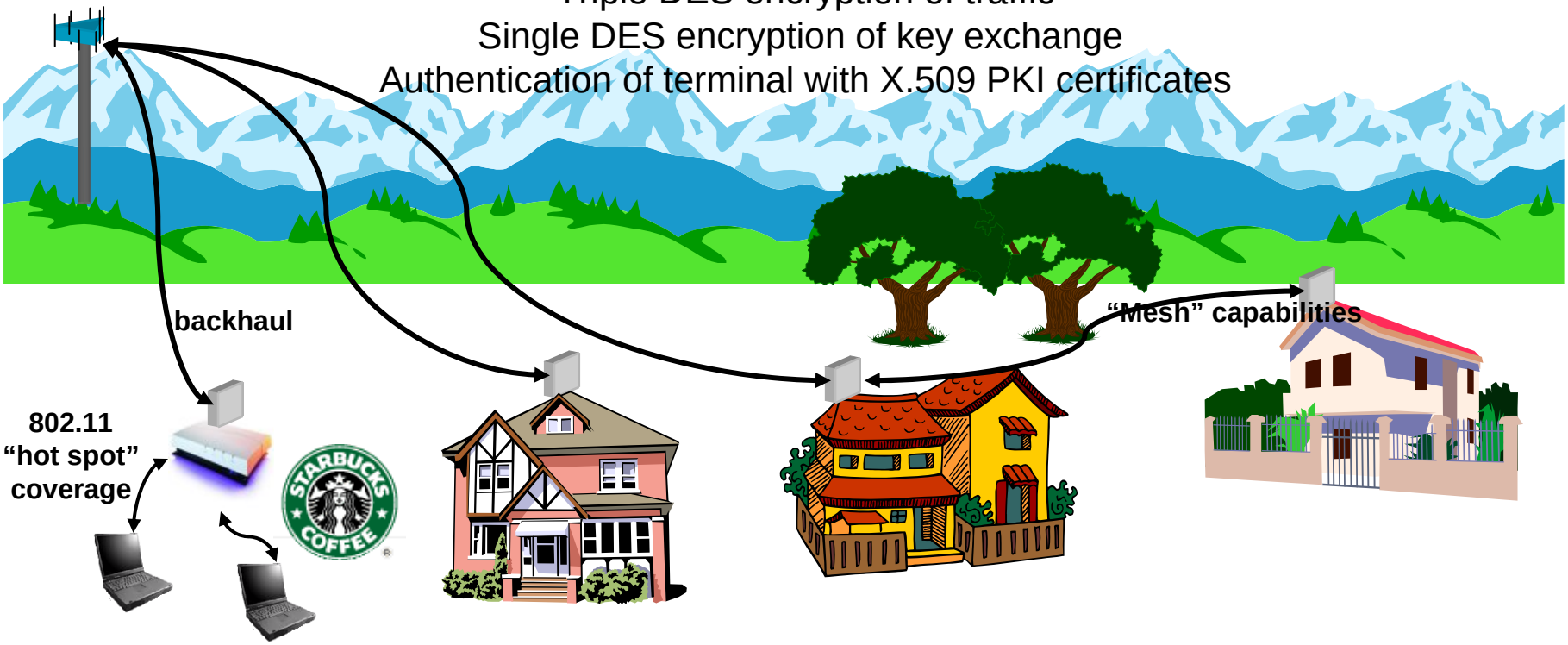
1900:
EDGE/3G: up to 384 kb/s
4G: 5-10 Mb/s?

Case 6 – Wireless LANs
802.11a, b, g

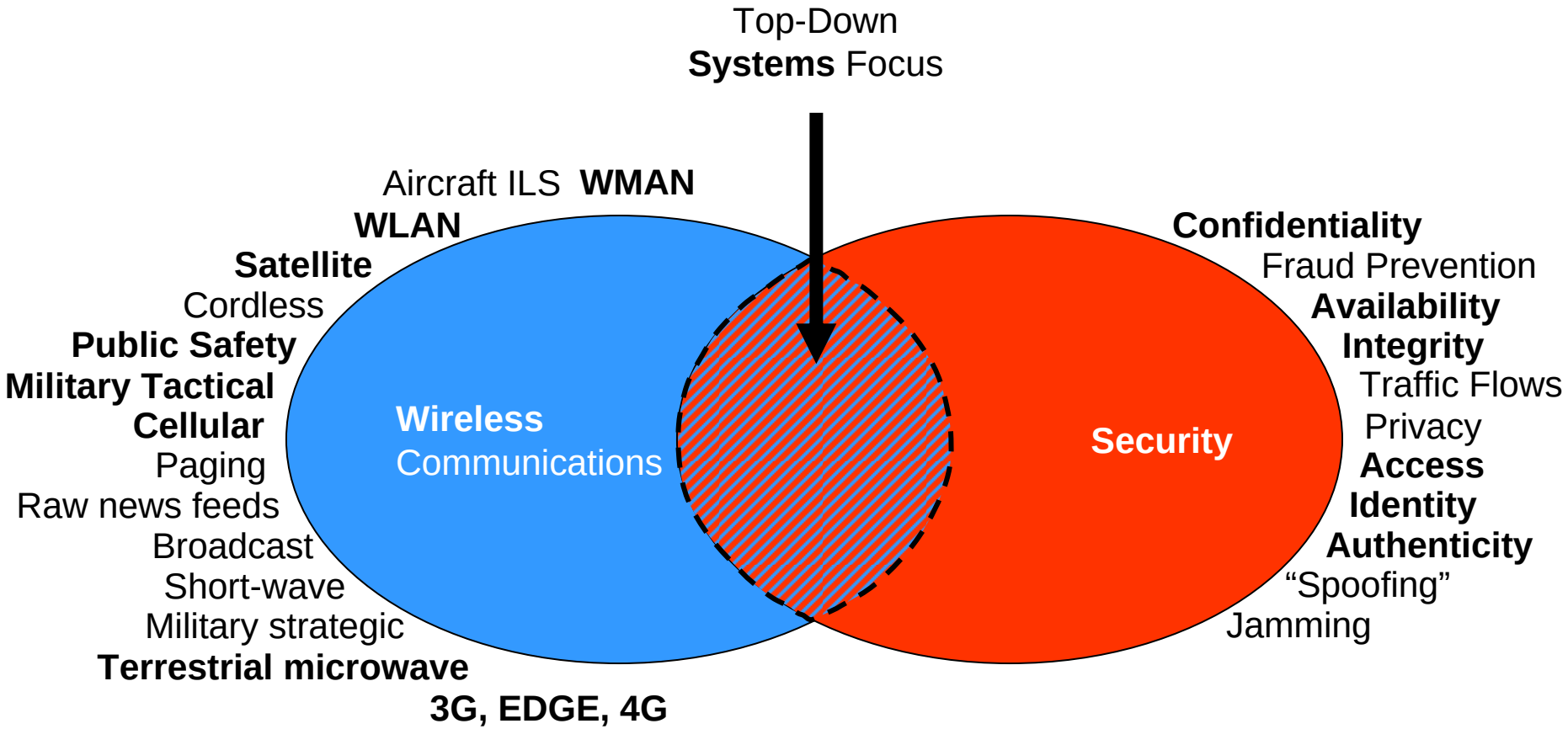


Case 7 –
Wireless Metropolitan Area Networks (W-MANs)
802.16

802.16a: 2-11 GHz 256/2048 carrier OFDM,
802.16.1: 10 – 66 GHz LOS
120 Mb/s capacity
T1+ user data, multiple voice channels, Wireless Local Loop
Triple DES encryption of traffic
Single DES encryption of key exchange
Authentication of terminal with X.509 PKI certificates



The Intersection of Wireless and Security



Key Points

- Security:
  - is best designed in, rather than added on
  - issues must be examined in the broadest context
  - cannot be taken for granted

- The interaction between complex systems is a fertile growth medium for security issues
- Obfuscation doesn't help
  - Where does mold tend to grow in homes?

- Wireless systems are generally:
  - New designs (not much field experience)
  - Complex (interactions between varied technologies)
  - Designed with short development cycles
  - Closed systems at introduction

- Broadcast nature of most wireless systems creates issues that wired systems don't share:
  - Ease of monitoring
  - Potential for jamming
  - Attack from anywhere – difficulty in controlling access to airwaves

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

- A fool is someone who does not learn from their mistakes

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

- A fool is someone who does not learn from their mistakes
- A genius is someone who learns from *other's mistakes*

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

- A fool is someone who does not learn from their mistakes
- A genius is someone who learns from *other's mistakes*

- Effective quality processes do not expect perfection

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

- A fool is someone who does not learn from their mistakes
- A genius is someone who learns from *other's mistakes*

- Effective quality processes do not expect perfection
- They do expect continuous process improvement

A Few Operative Definitions

- Quality is meeting or exceeding customers' expectations
- Security is meeting or exceeding customers' expectations *in the presence of the actions of an adversary*

- A fool is someone who does not learn from their mistakes
- A genius is someone who learns from *other's mistakes*

- Effective quality processes do not expect perfection
- They do expect continuous process improvement

An effective security process would be one that
- continually ***anticipates*** threats,
- ***prioritizes*** the most credible threats, and
- ***adapts*** to meet those threats ***before*** they degrade the system