Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair

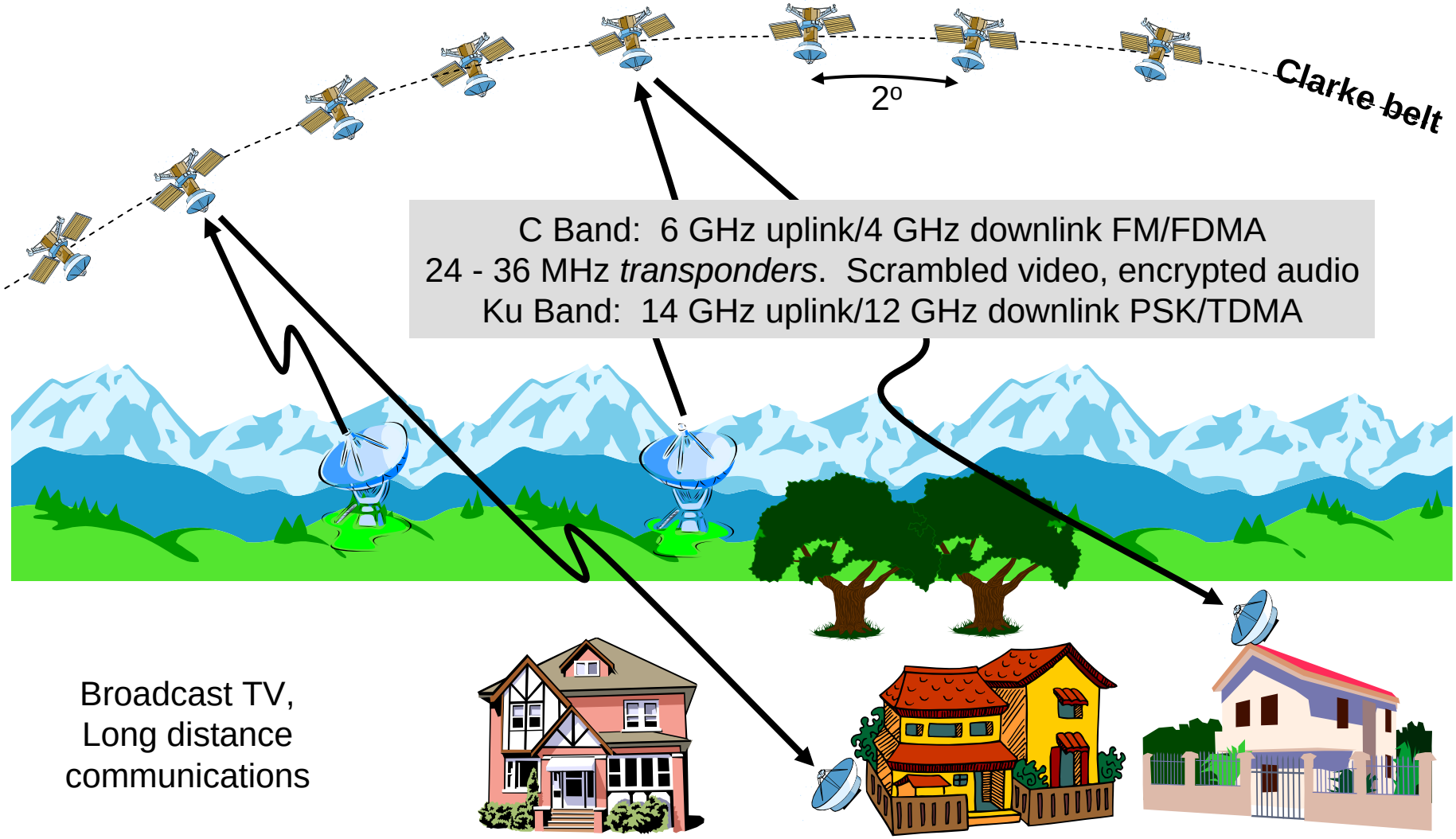
bmcnair@stevens.edu

Week 8 - Wrapup

Case Study 4

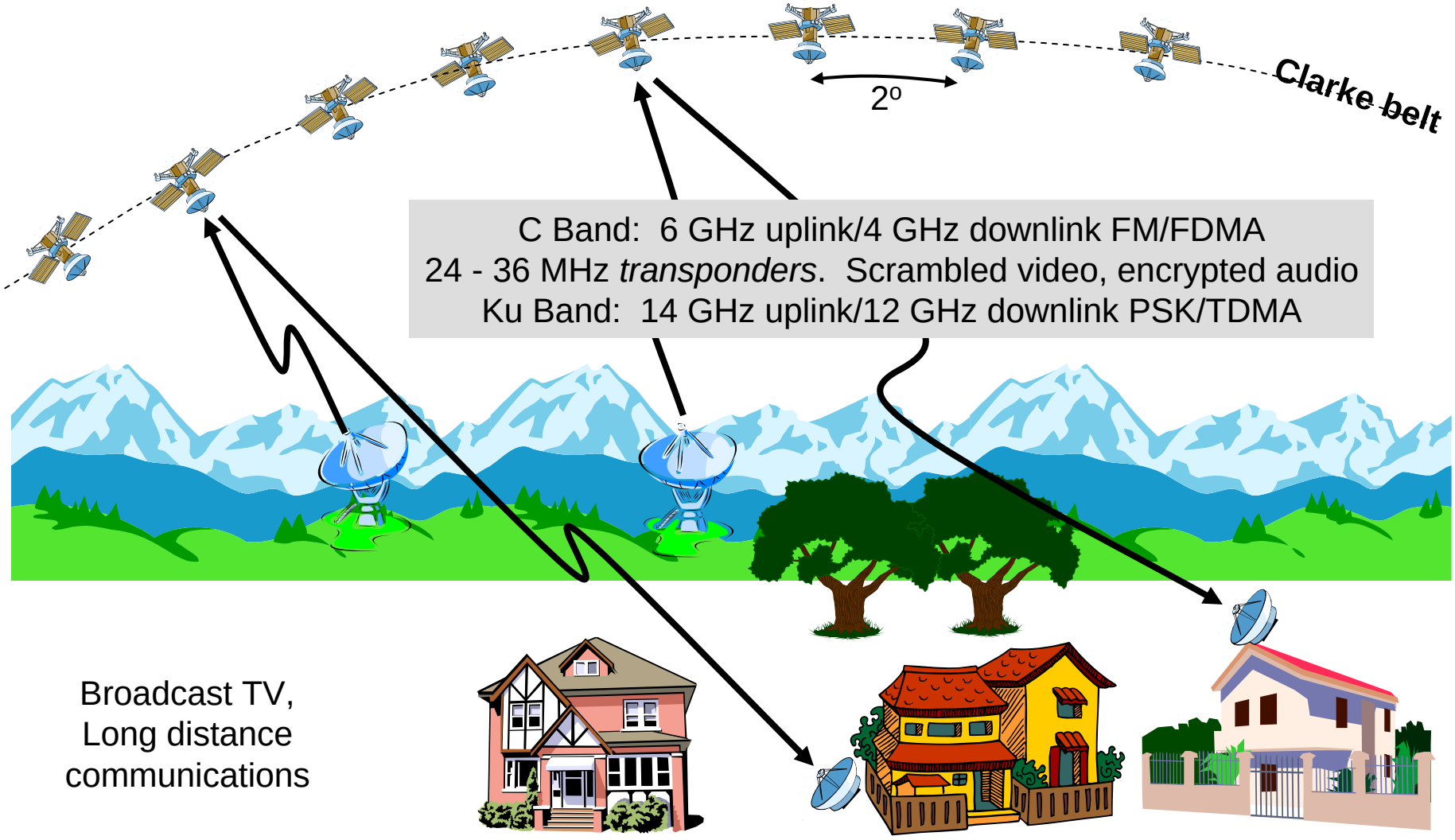
Summary and observations

Case 4 – Satellite Communications Systems



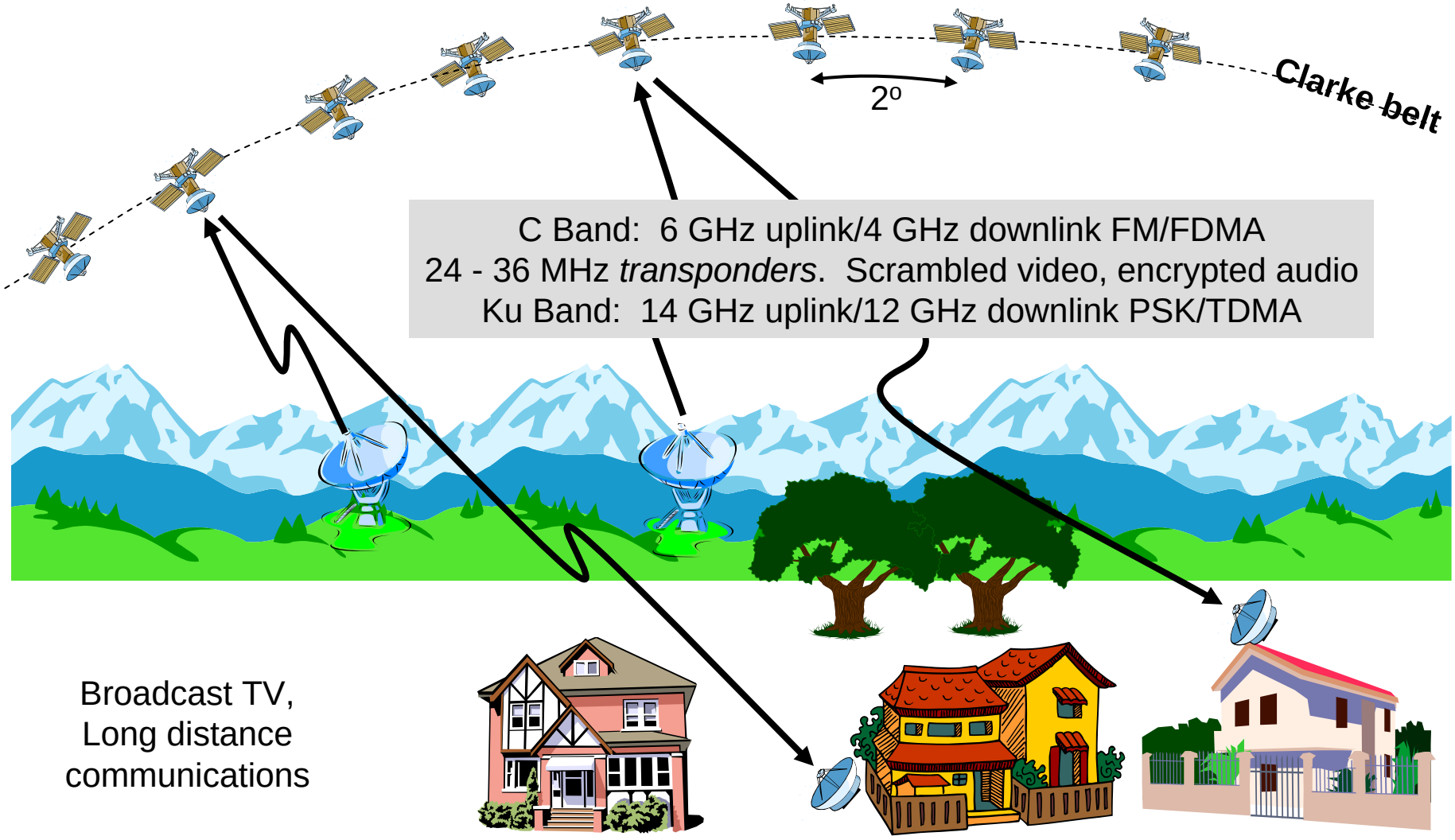
Broadcast TV,
Long distance
communications

Case 4 – Satellite Communications Systems



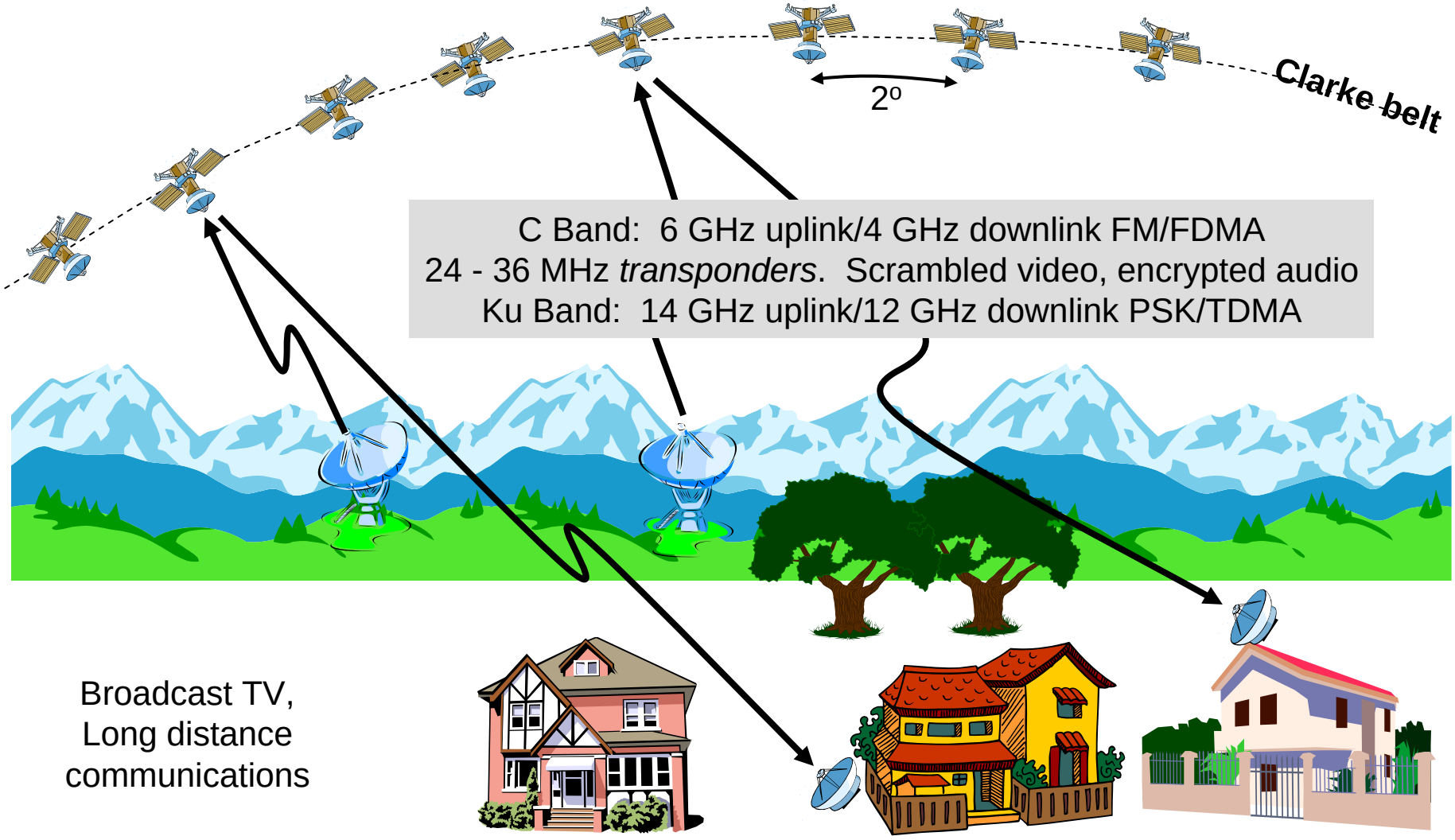
Broadcast TV,
Long distance
communications

Case 4 – Satellite Communications Systems



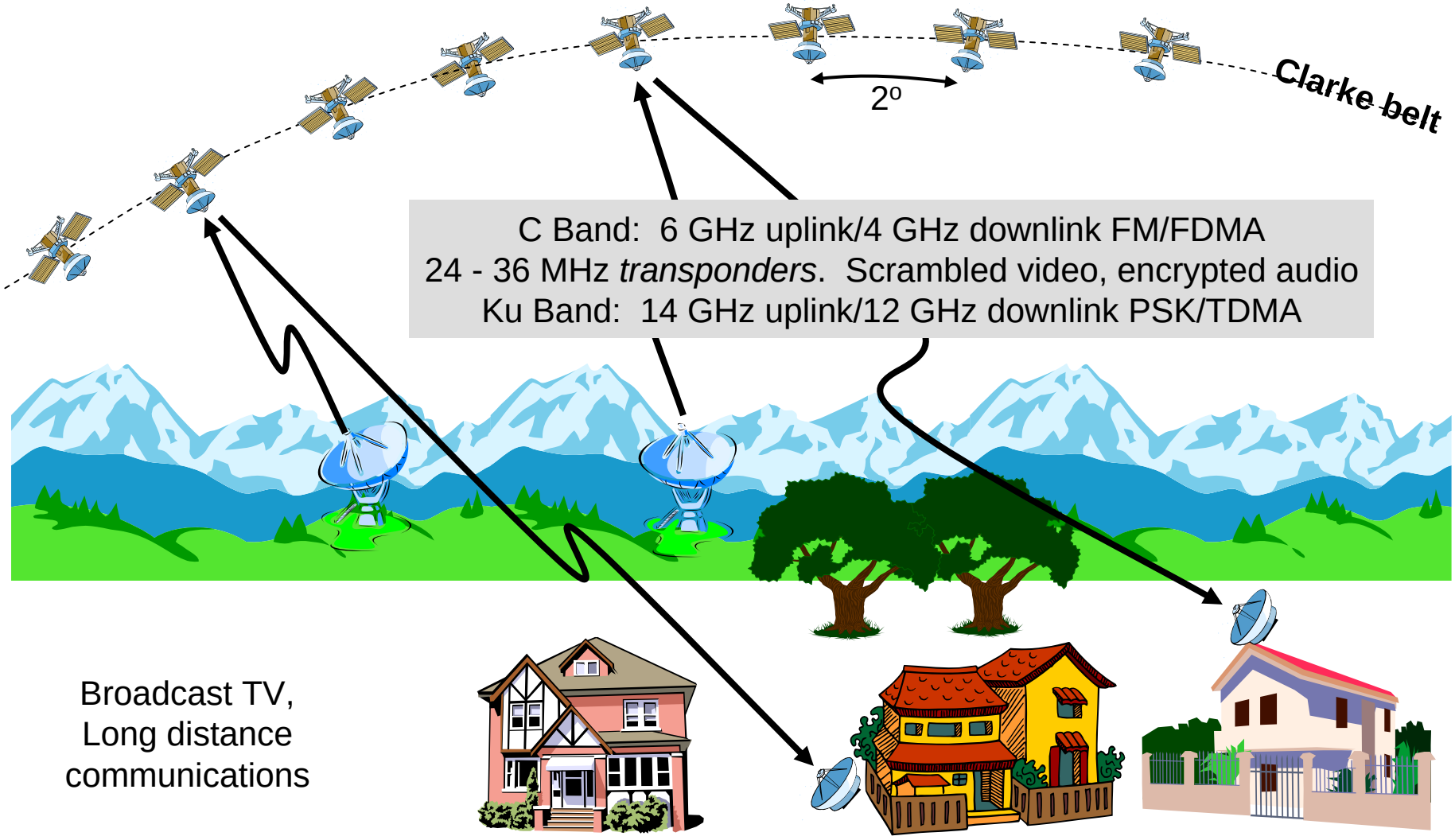
Broadcast TV,
Long distance
communications

Case 4 – Satellite Communications Systems

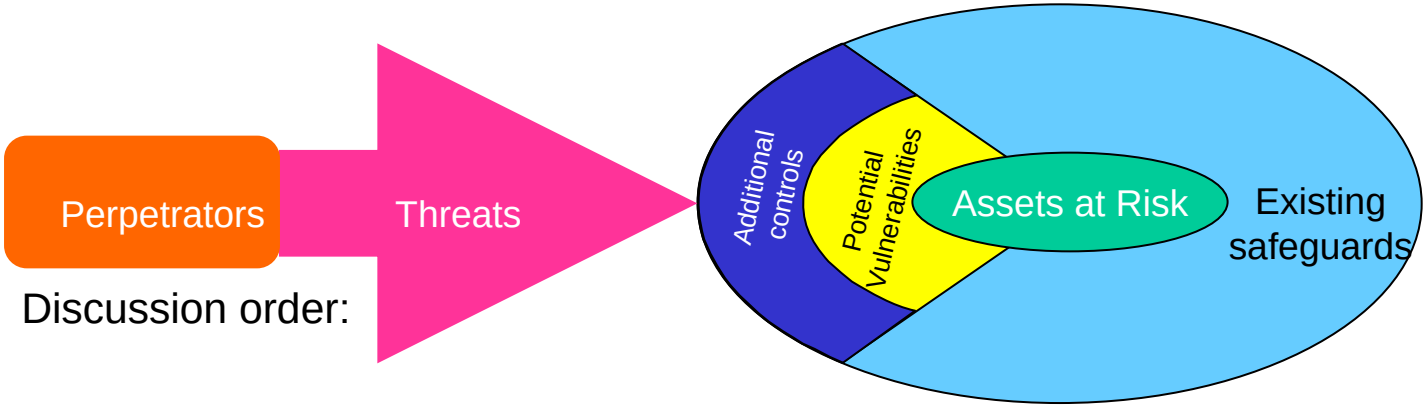


Broadcast TV,
Long distance
communications

Case 4 – Satellite Communications Systems

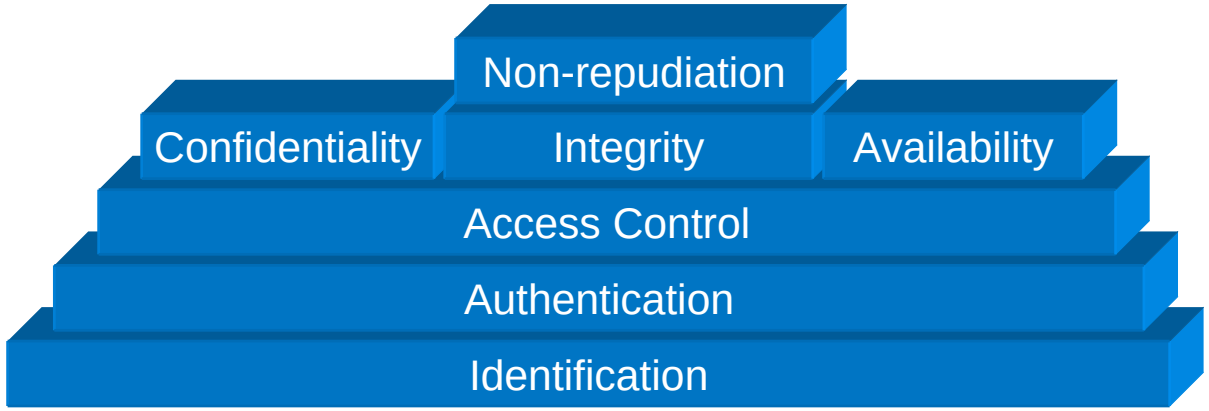


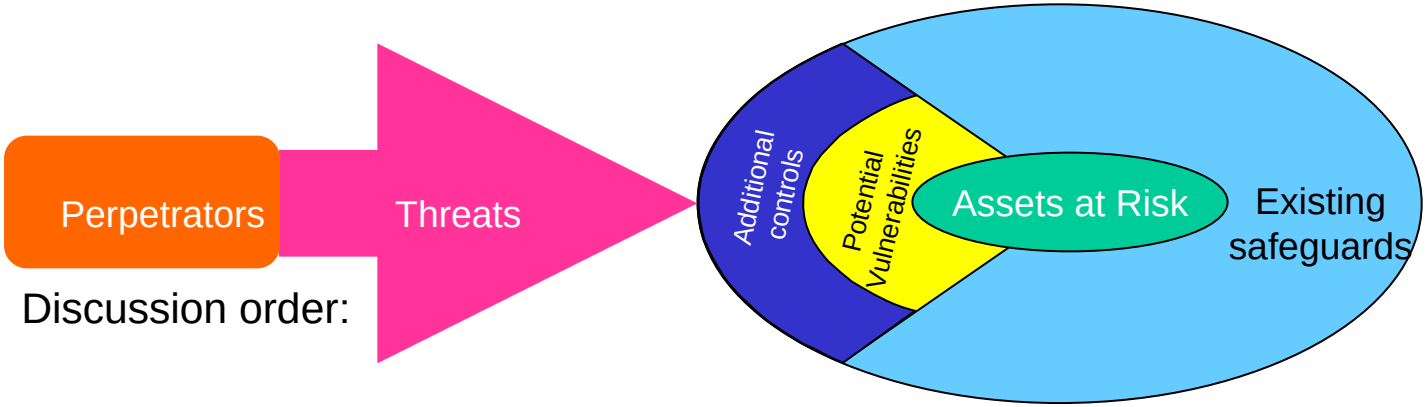
Broadcast TV,
Long distance
communications



Discussion order:

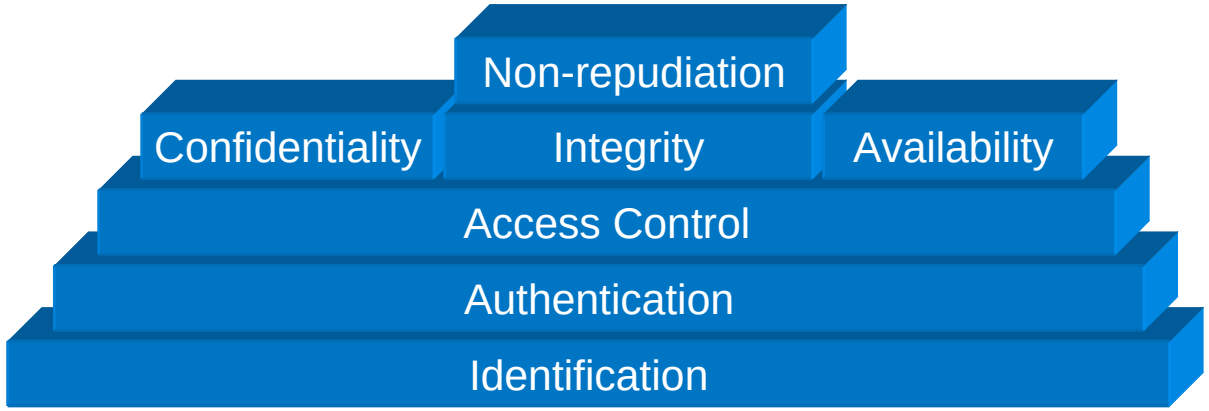
- Assets
- Perpetrators
- Threats
- Existing Safeguards
- Potential Vulnerabilities
- Additional Security Controls





Discussion order:

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



Assets

Equipment
- Dish
- satellite

Information
RF spectrum
Orbital position
Protocol used
Frequency
Ground station
Bandwidth
Technical information about satellite or design, including encryption
Power
Satellite fuel
Satellite station-keeping management system(s)

Perpetrators

Foreign government
People trying to steal data, entertainment programs
Teen-age hackers
Other providers
Listeners in other countries who want to be able to receive programming
Resellers of stolen/pirate devices
Distributors of hacking technology
Underground TV stations
Nature
Meteors, asteroids

Threats

Physical destruction of uplink ground station
Orbital projectiles
Jamming
Hacker gets into satellite control system and unparks satellite, wasting fuel
Land-satellite projectiles
Guided energy weapons
Destruction of any part of system, including cables, can render system unusable
Jam downlink from aerial platform (e.g., balloon)
Intercept information
Special interest group (e.g., PETA) takes over uplink to broadcast their propaganda/announcements
Exploit sensitive information about system
Steal transponder bandwidth with spread-spectrum signal

Existing Safeguards

Encryption of programming
Encryption of control link
Control protocols are unpublished
Uplink beamwidth is small
Terrestrial propagation at 6 GHz is limited
Ground station in remote/RF quite areas
Broad satellite earth coverage to disseminate information
Satellite health monitoring systems
(limited) Satellite mobility
Uplink power control -> equitable sharing
(satellite handsets) – communications diversity
physical separation of satellites

Vulnerabilities

Electrical/mechanical failure of satellite
Human error
Mismatched “service orders” (e.g., meters/feet error with Martian lander)
Inadequate physical security
- Ground stations
- Servers
- Network management systems

Movability of receiving dish (repositionable)
Path obstructions
Untraceability of control function or utilization of capacity (anywhere in satellite footpring)
Broad coverage area -> large security perimeter
General immobility of satellite
Encryption for entertainment services is weak
Method of distribution of viewing permission weak
Wind, heavy rain -> signal disruption