Hacking a Bird in the Sky 2.0

Exploiting Satellite Trust Relationship

Jim Geovedi
jim.geovedi@bellua.com

Raditya Iryandi
raditya.iryandi@bellua.com

Anthony Zboralski
anthony.zboralski@bellua.com

Disclaimer

This presentation is intended to demonstrate the inherent security, design and configuration flaws in publicly accessible satellite communication networks and promote the use of safer satellite communication systems. Viewers and readers are responsible for their own actions and strongly encourage to behave themselves.

Slanguage Dictionary

- **Bird**: a variety term for satellite; "The proposed channel would be carried by an Asian **bird** to be launched next spring."

Satellite

- A satellite is **any object that orbits another object** (which known as its primary).

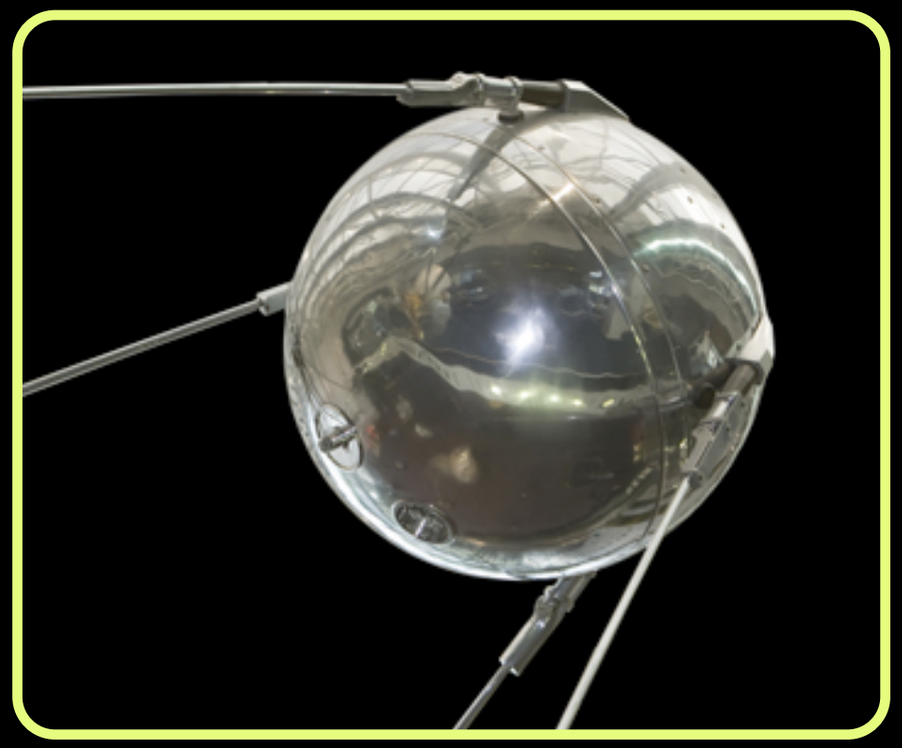
Artificial Satellite

- It was the English sci-fi writer Arthur C. Clarke who conceived **the possibility of artificial communication satellites** in 1945. Clarke examined the logistics of satellite launch, possible orbits and other aspects.

Arthur C. Clarke, science fiction author, meeting with fans, at his home office in Colombo, Sri Lanka.
source: http://en.wikipedia.org/wiki/Arthur_C._Clarke

Artificial Satellite

- The first artificial satellite was **Sputnik 1** launched by Soviet Union on 4 October 1957.



In 1957, the Soviet Union launched Sputnik, a basketball-size capsule that became the Earth's first man-made satellite. Sputnik's radio signals were a "raspberry" from the Soviets, fumed one U.S. pundit. The next year, the United States created NASA, and the space race was under way.
source: http://magma.nationalgeographic.com/ngm/2007-10/space-travel/space-travel-photography.html

Satellite Internet Services

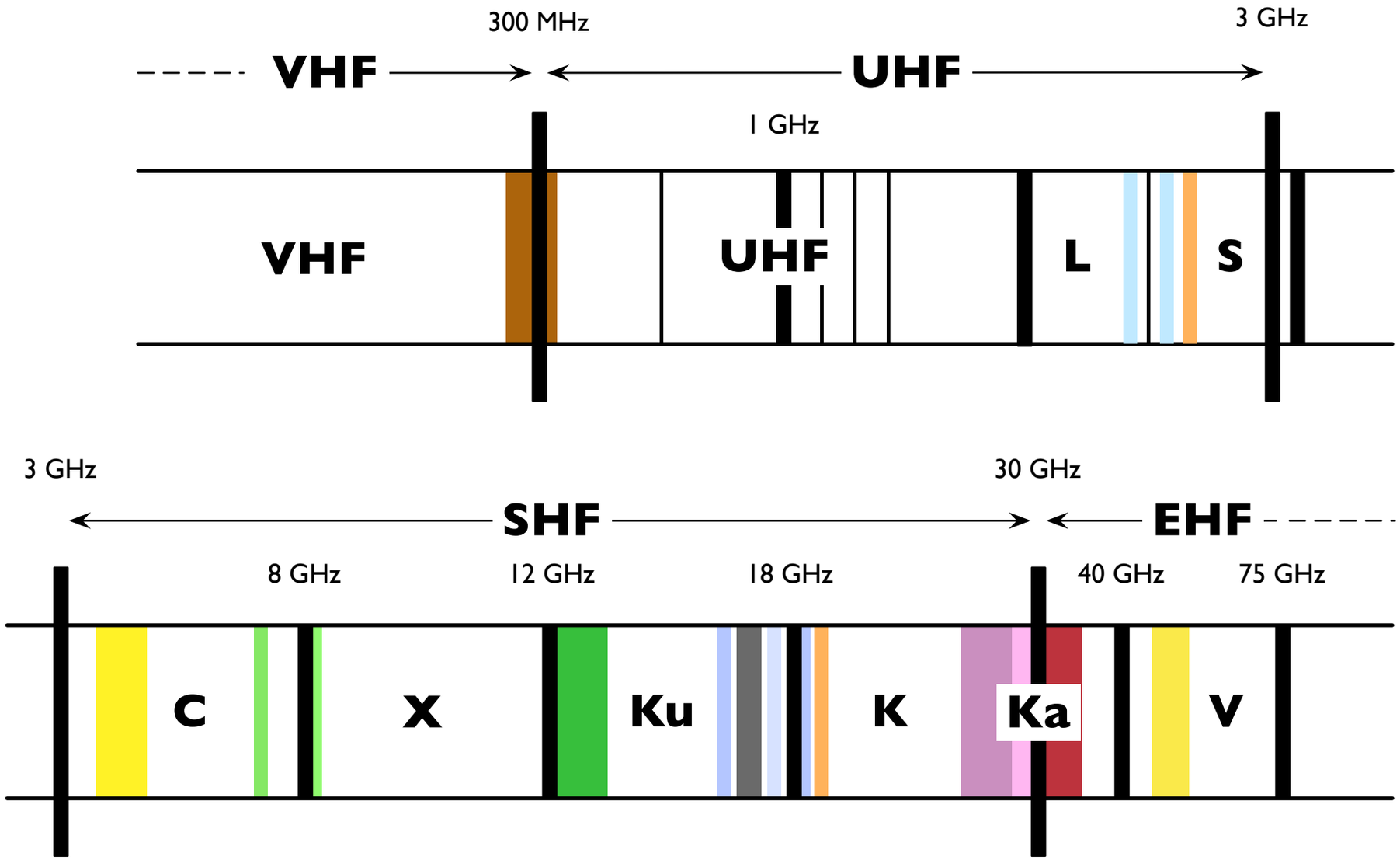
- **One-way multicast:** used for IP multicast-based data, audio and video distribution.
  - Most Internet protocols will not work correctly over one-way access, since they require a return channel.
- **One-way with terrestrial return:** used with traditional dial-up access to the Internet, but downloads are sent via satellite at a speed near that of broadband Internet access.
- **Two-way satellite access:** allows upload and download data communications.

Very Small Aperture Terminal

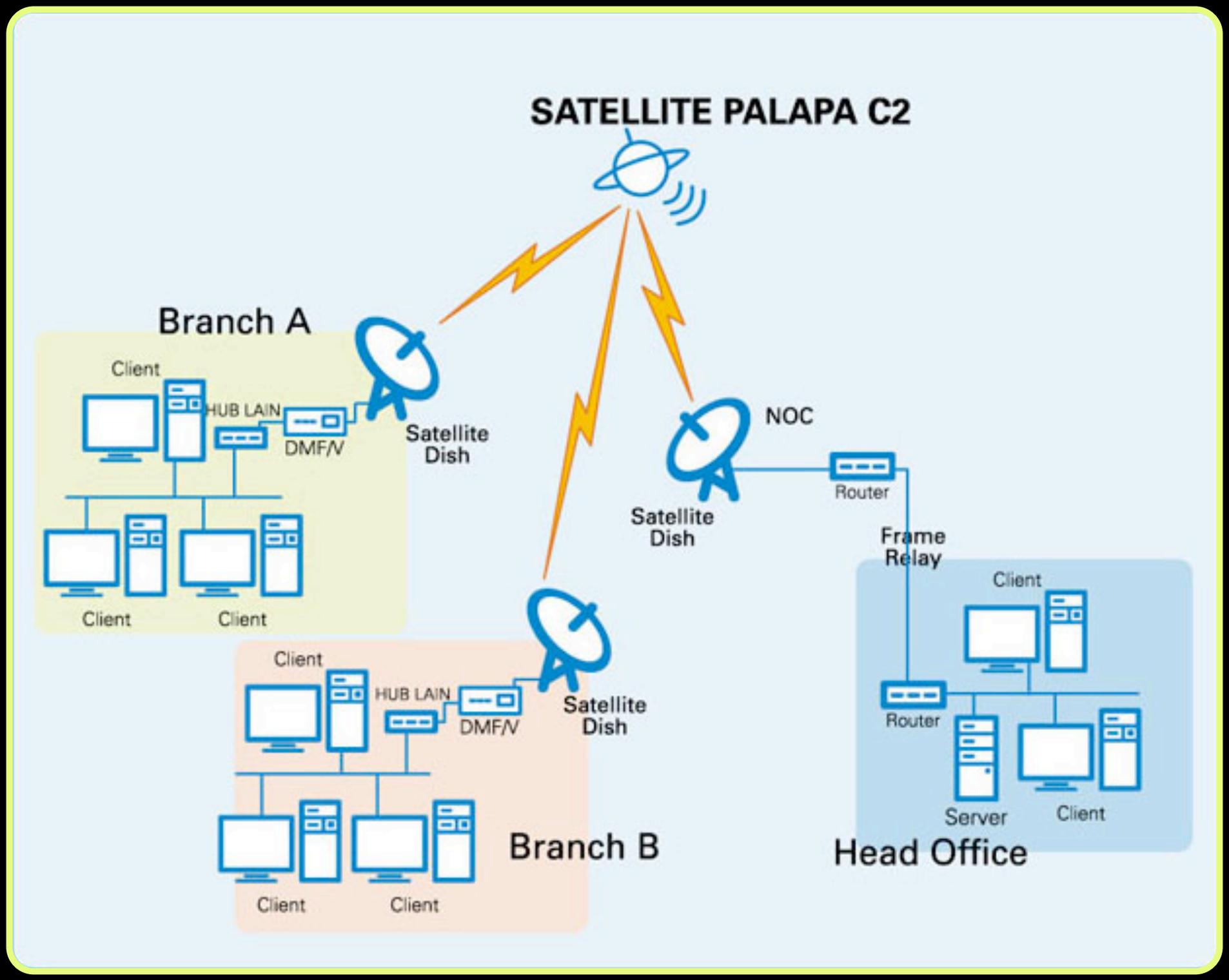
- A one or two-way terminal used in a star, mesh or point to point network with. Antenna size is restricted to being less than or equal to 3.8 m at Ku band and 7.8 m at C band.
- It consists of a large high performance hub earth station (with an antenna of up to 9 m in diameter) and a large number of smaller, lower performance terminals. These small terminals can be receive only, transmit only or transmit/receive.

A 2.5m parabolic dish antenna for bidirectional high-speed satellite Internet.
source: http://en.wikipedia.org/wiki/VSAT

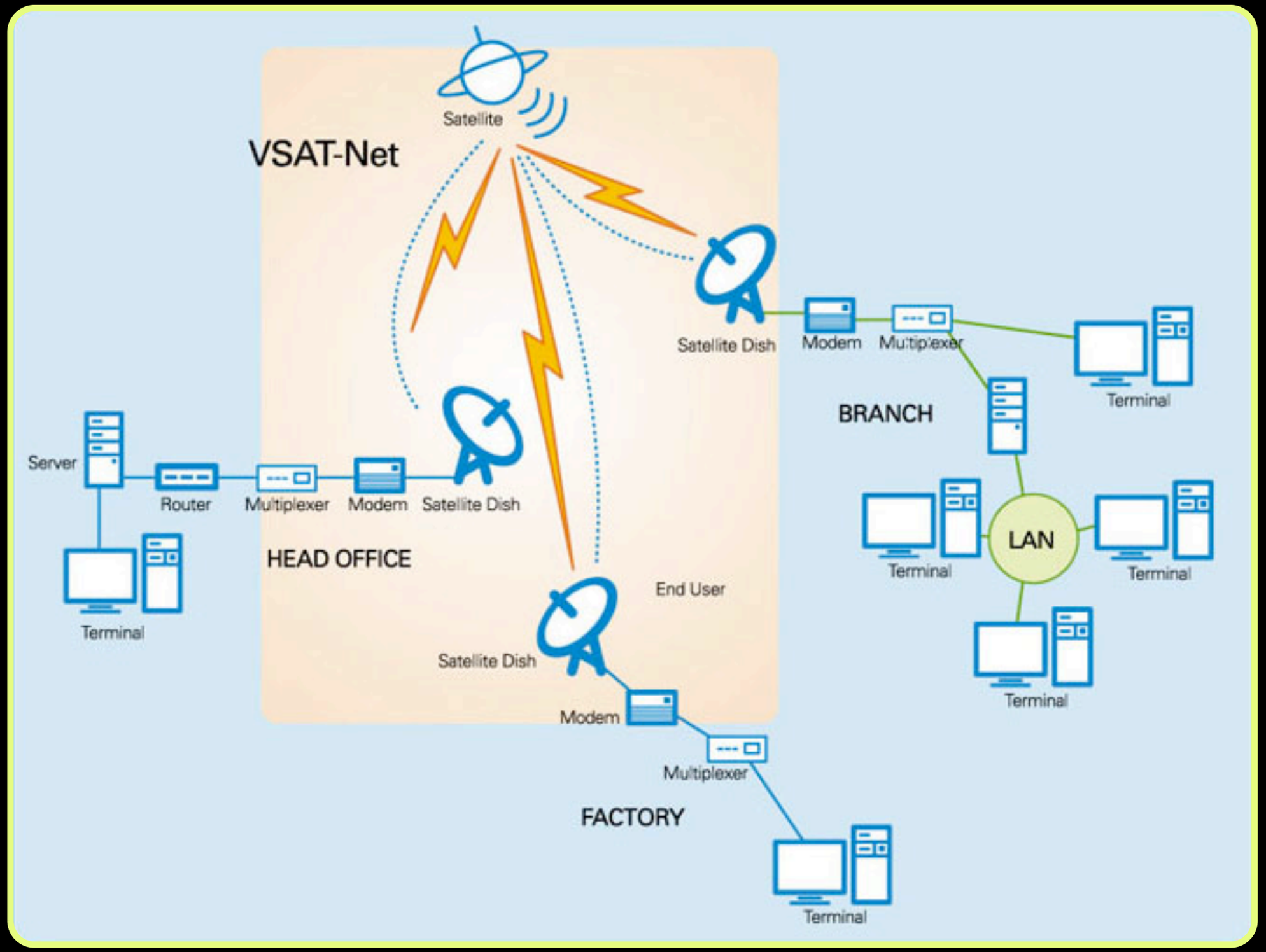
Frequency Band Designations



source: http://www.satcom-services.com/sat_freq.htm



Data communication service using satellite access media with Time Division Multiplex (TDM) / Time Division Multiple Access (TDMA) technology based on Internet-protocol.
source: http://www.lintasarta.net/PRODUKLAYANAN/Satelit/VsatIP/tabid/85/Default.aspx



Data communication service using satellite access media with Single Channel per Carrier (SCPC) connecting point-to-point and point-to-multipoint.
source: http://www.lintasarta.net/PRODUKLAYANAN/Satelit/VsatLink/tabid/86/Default.aspx

Attacks against Satellite Systems

- Hypothetical Attacks
  - Denial of services (uplink/downlink jamming, overpower uplink), orbital positioning attacks (raging transponder spoofing, direct commanding, command replay, insertion after confirmation but prior to execution)
- Practical Attacks

Hacking a Bird in the Sky: Exploiting Satellite Trust Relationship

Hack In The Box Security Conference 2008

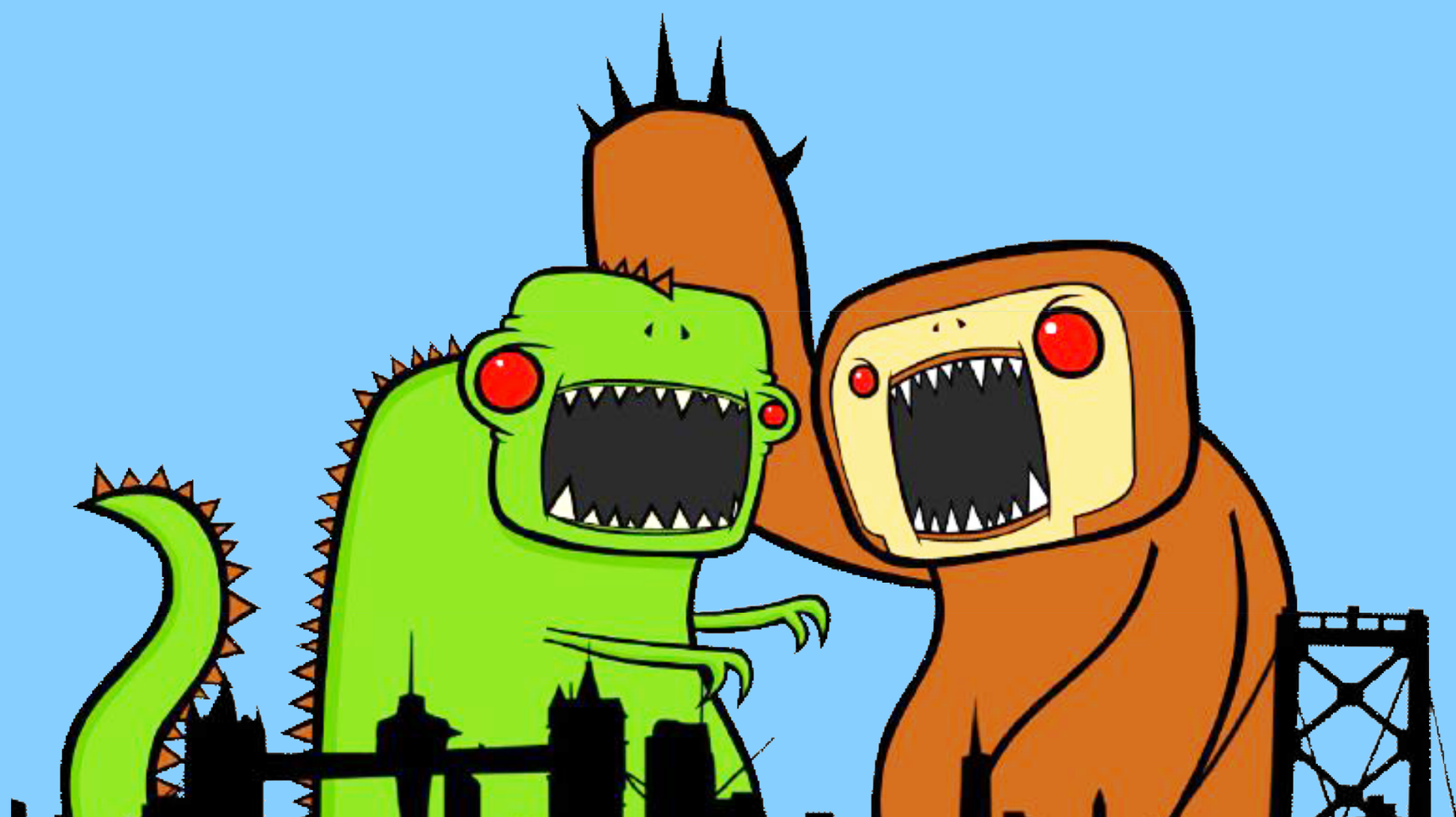
Abusing Satellite Systems

"Satellite Piggyjacking"

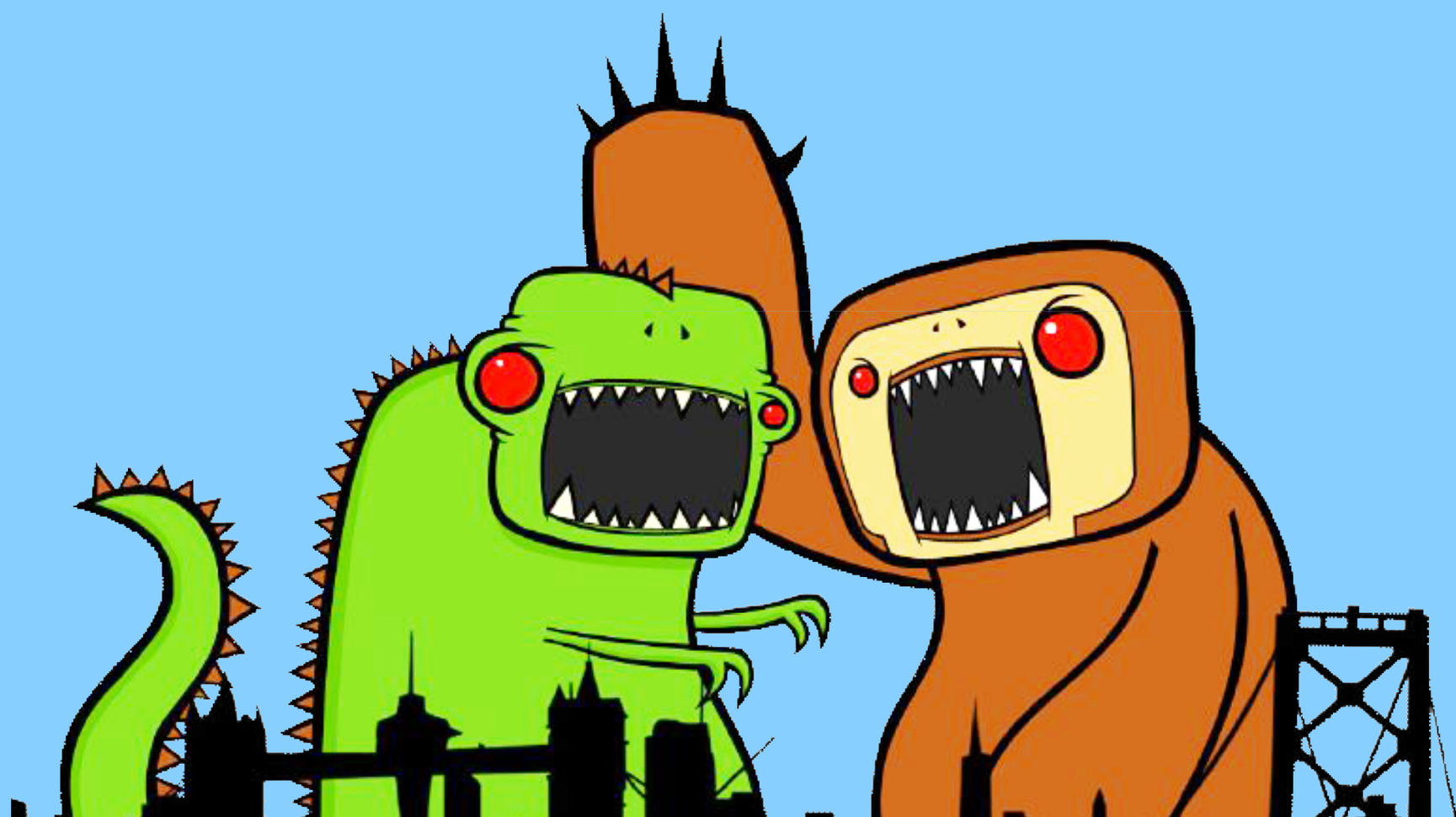
(Exploiting Satellite Trust Relationship on VSAT Network)

Hacking a Bird in the Sky: Exploiting Satellite Trust Relationship

Hack In The Box Security Conference 2008

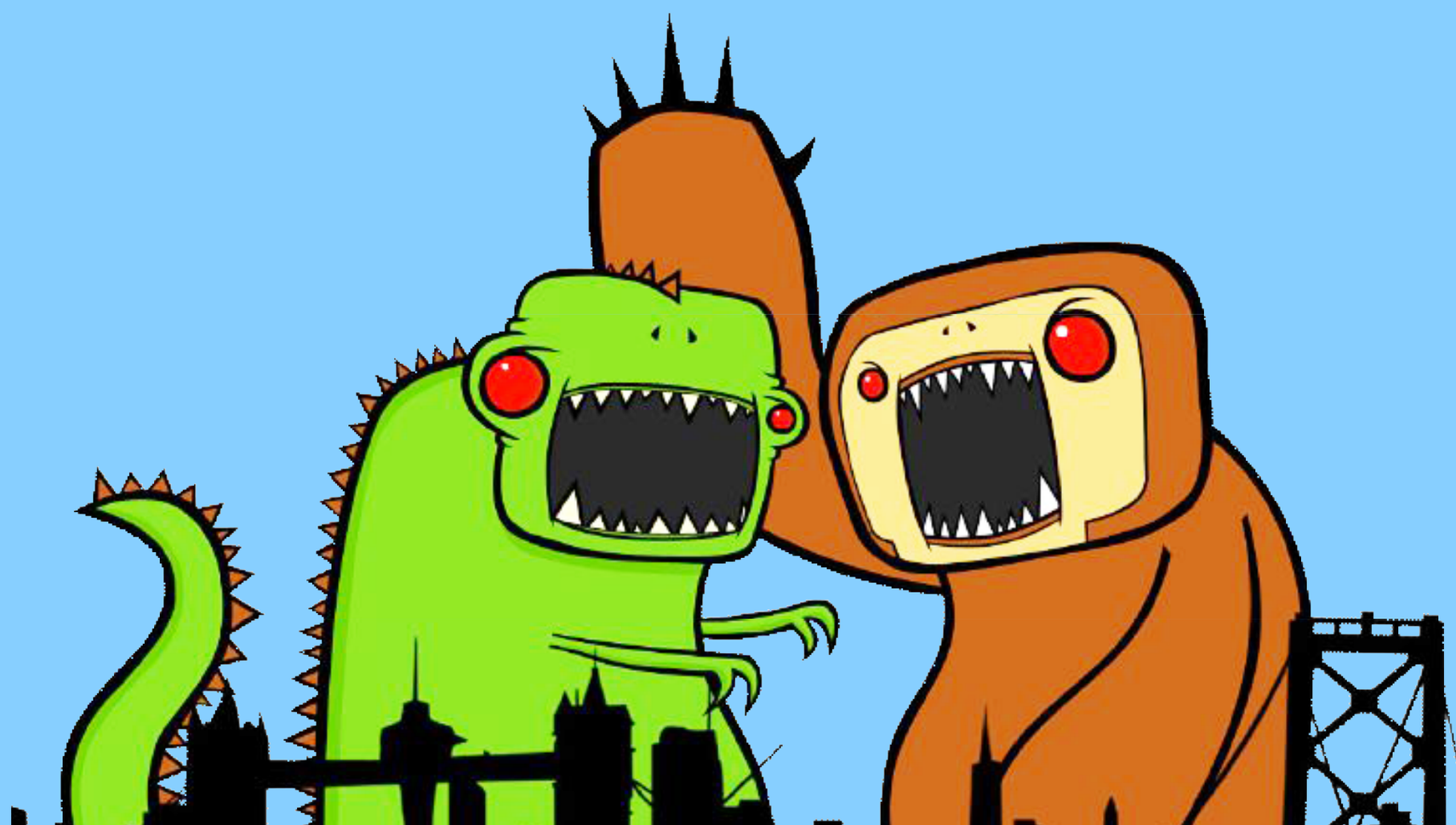


Satellite Piggyjacking



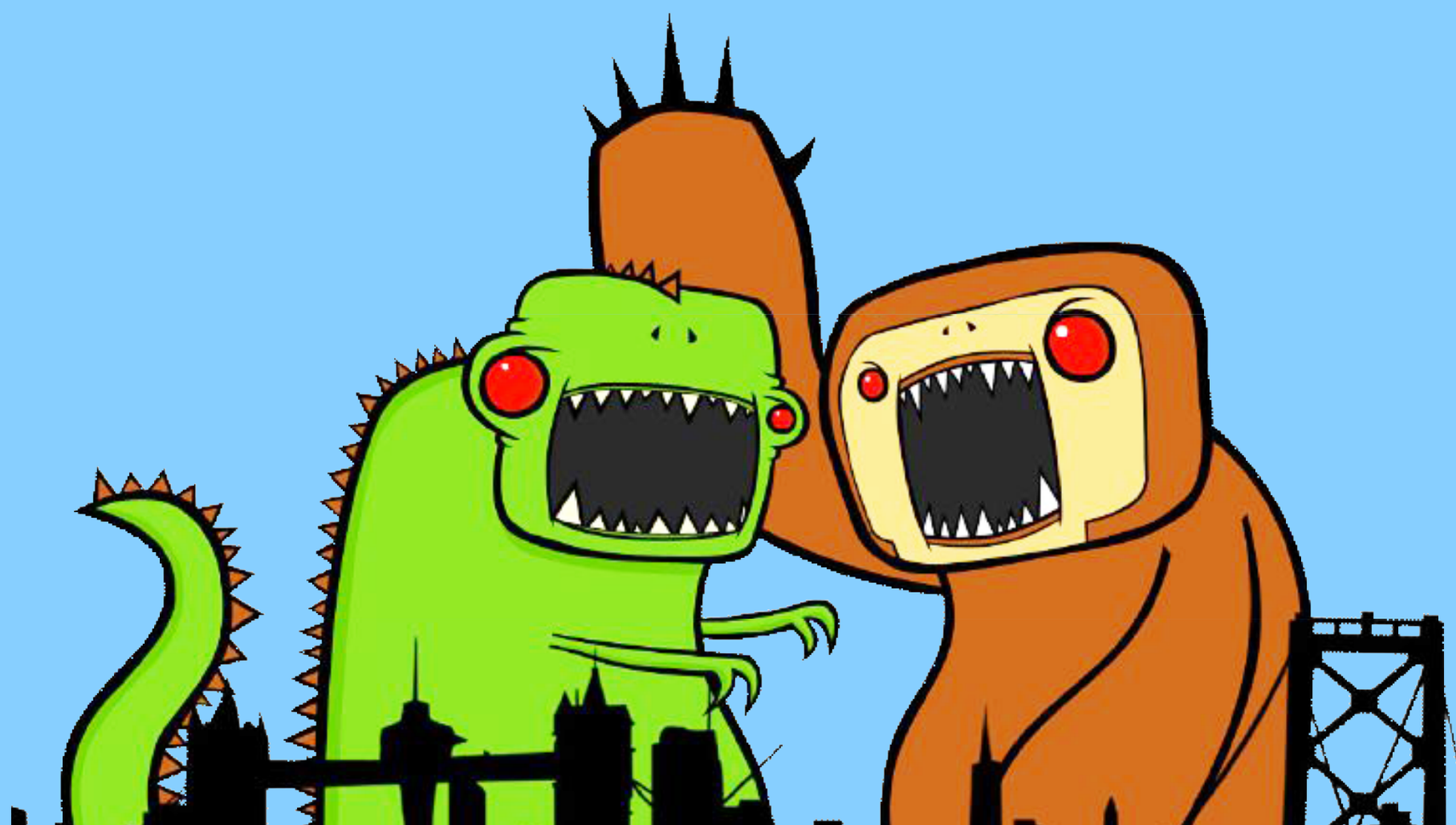
Satellite Piggyjacking

- Selecting target



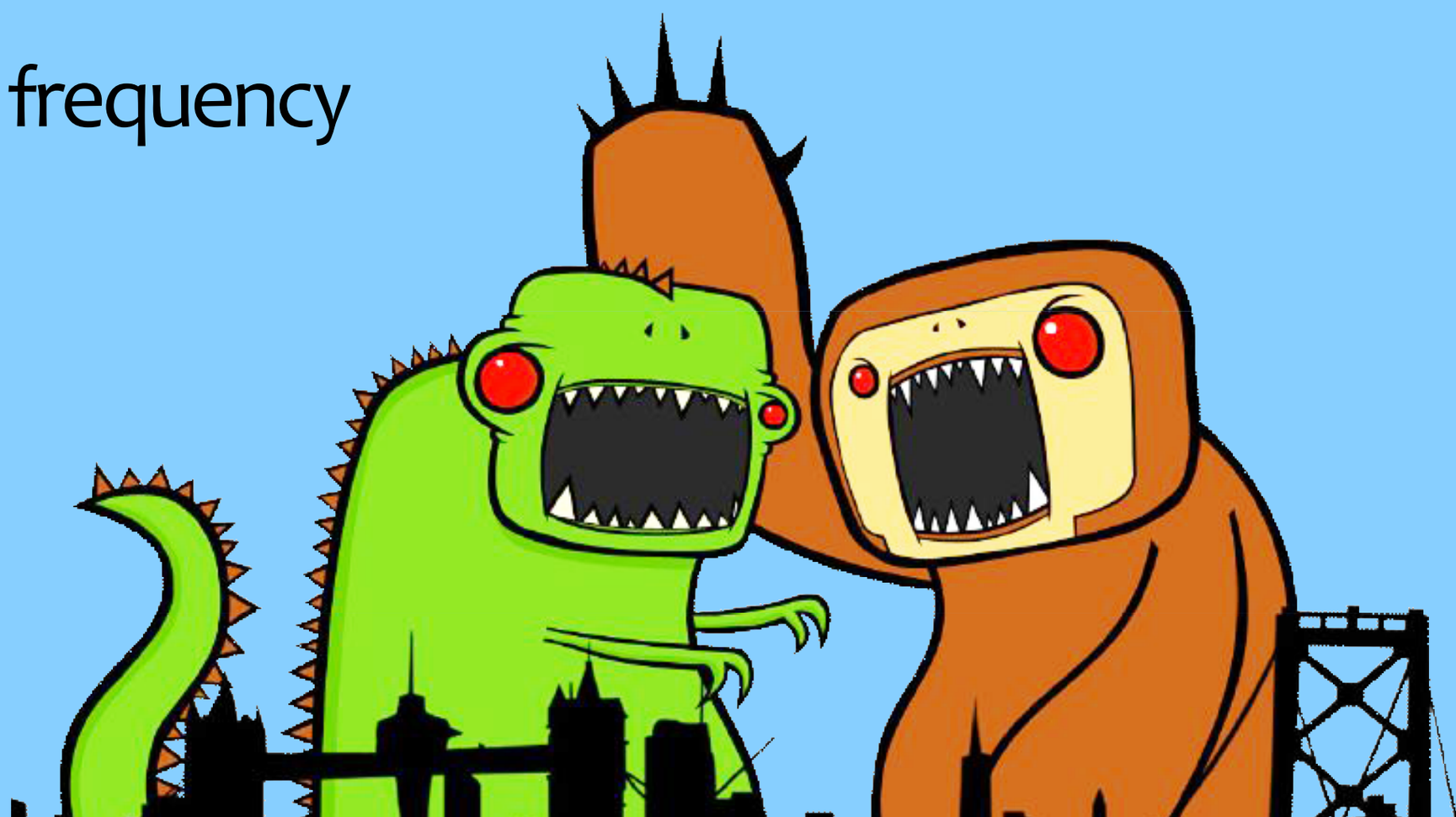
Satellite Piggyjacking

- Selecting target
- Pointing antenna



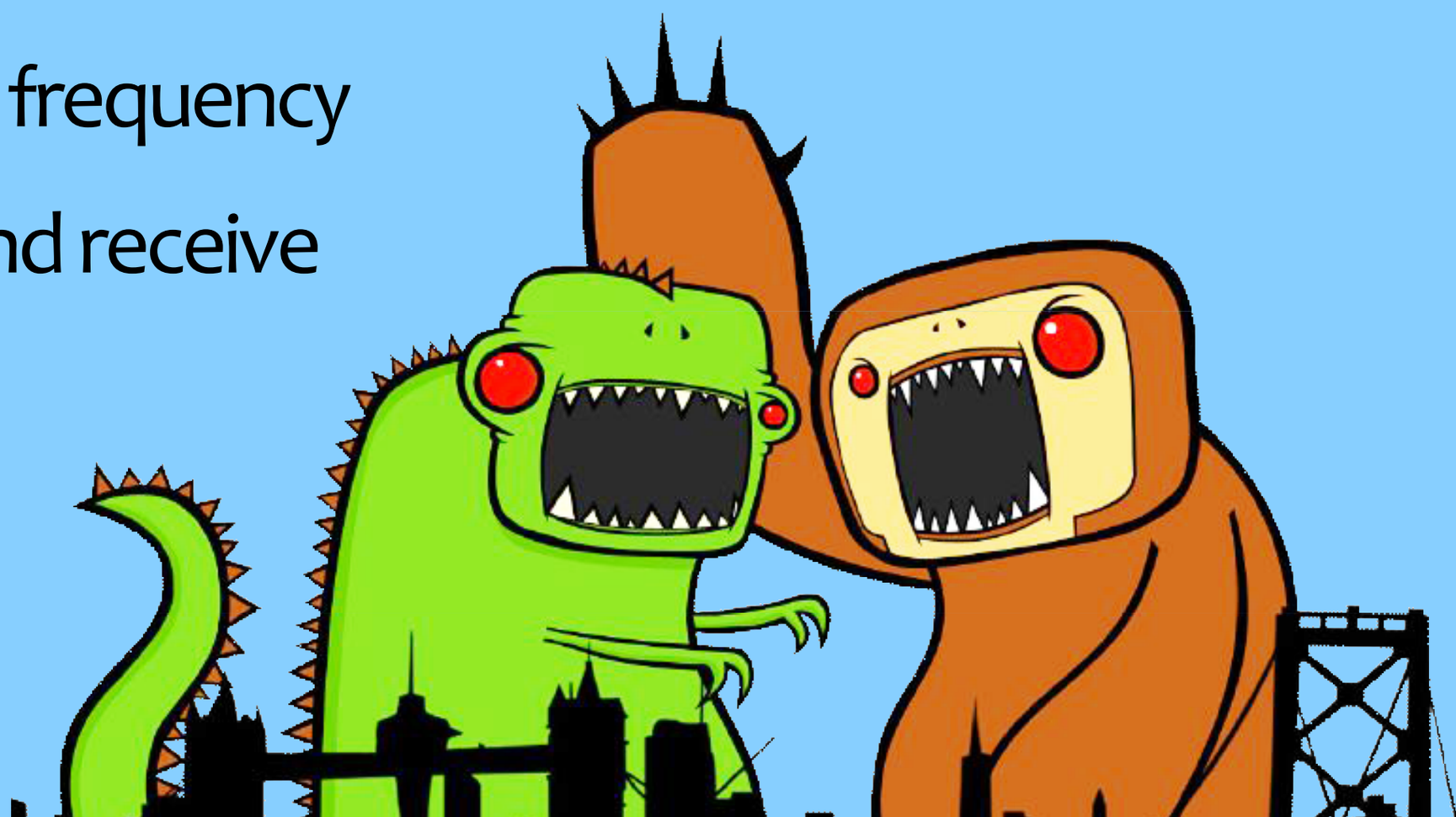
Satellite Piggyjacking

- Selecting target
- Pointing antenna
- Find "free" frequency



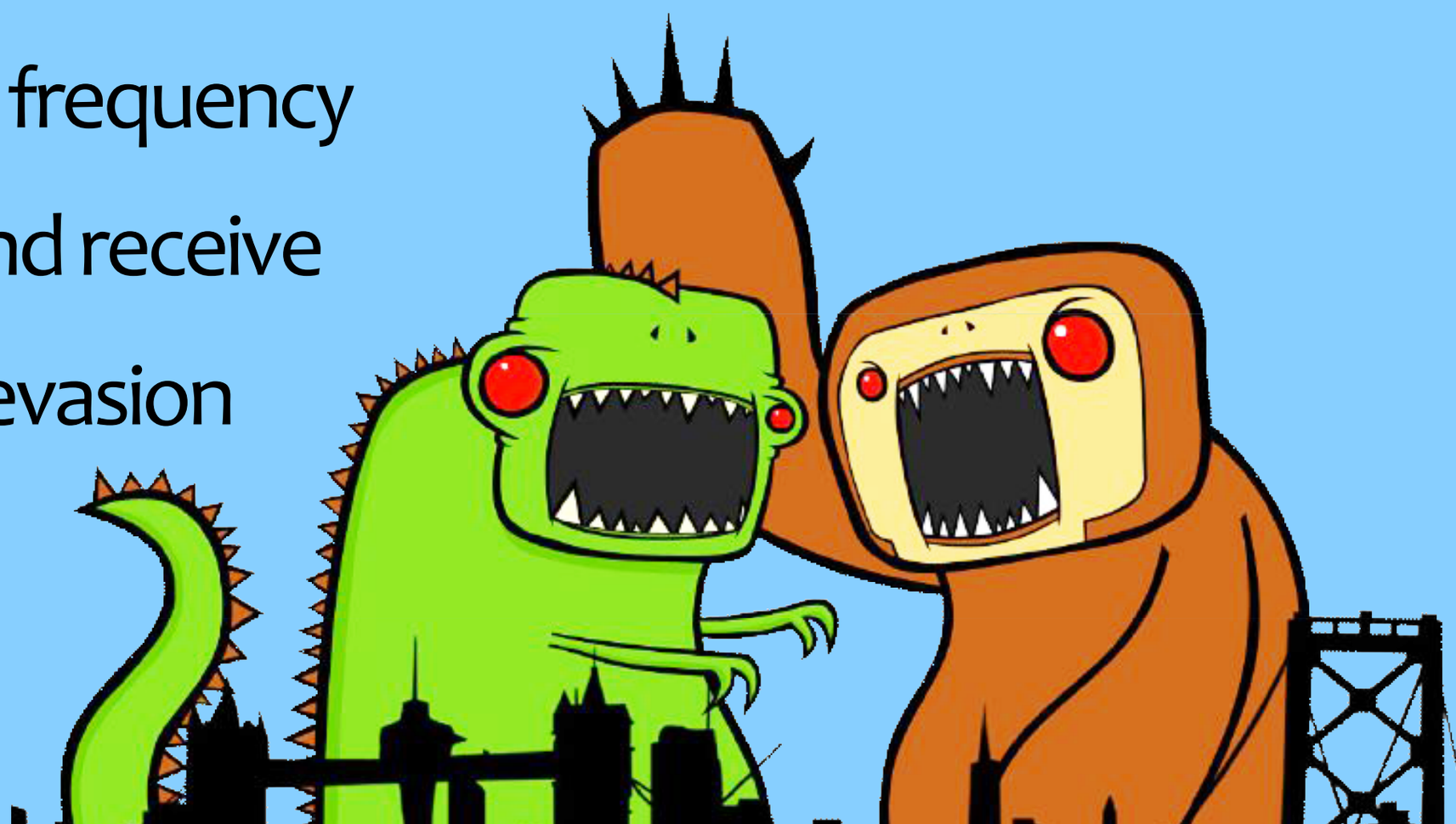
Satellite Piggyjacking

- Selecting target
- Pointing antenna
- Find "free" frequency
- Transmit and receive



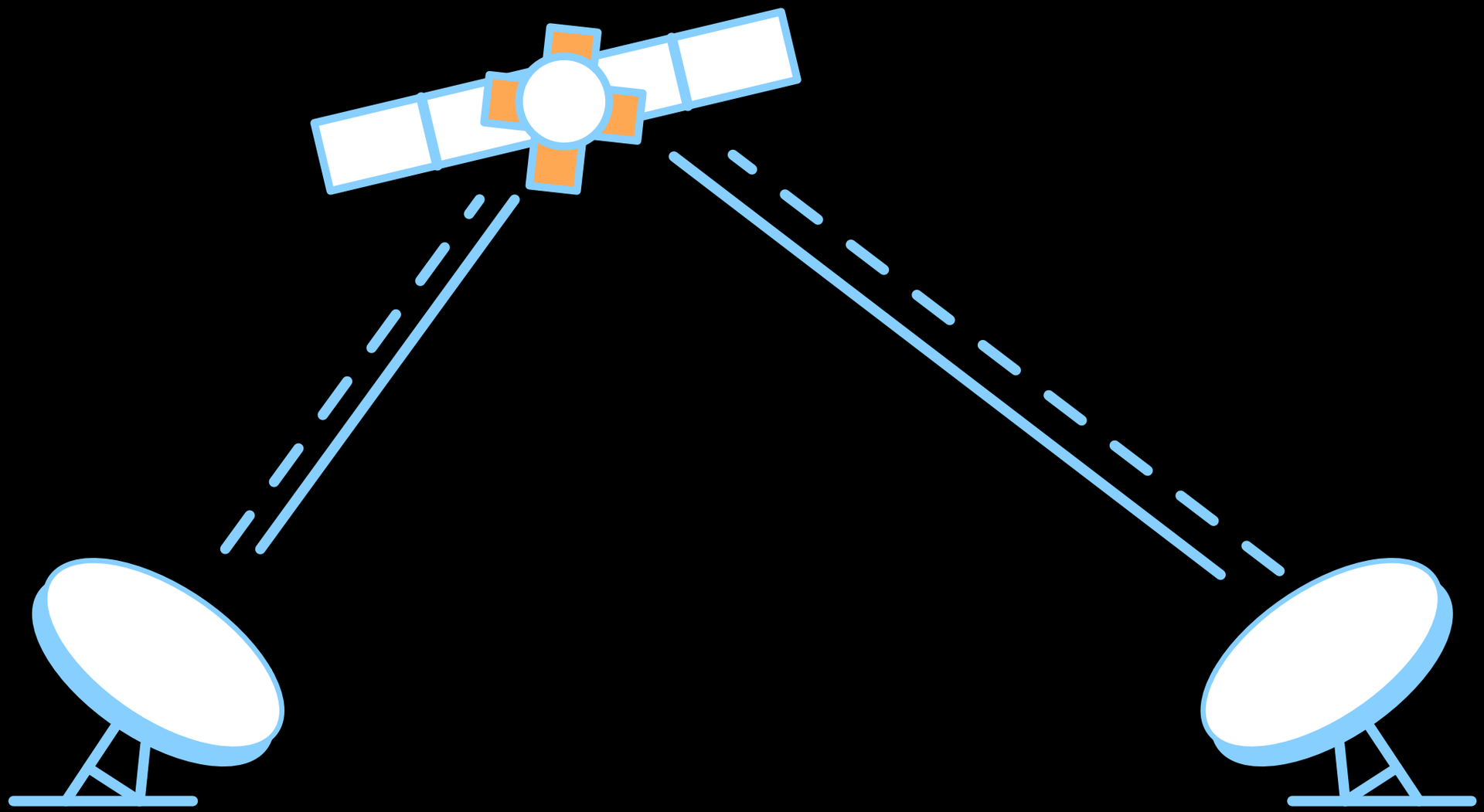
Satellite Piggyjacking

- Selecting target
- Pointing antenna
- Find "free" frequency
- Transmit and receive
- Detection evasion

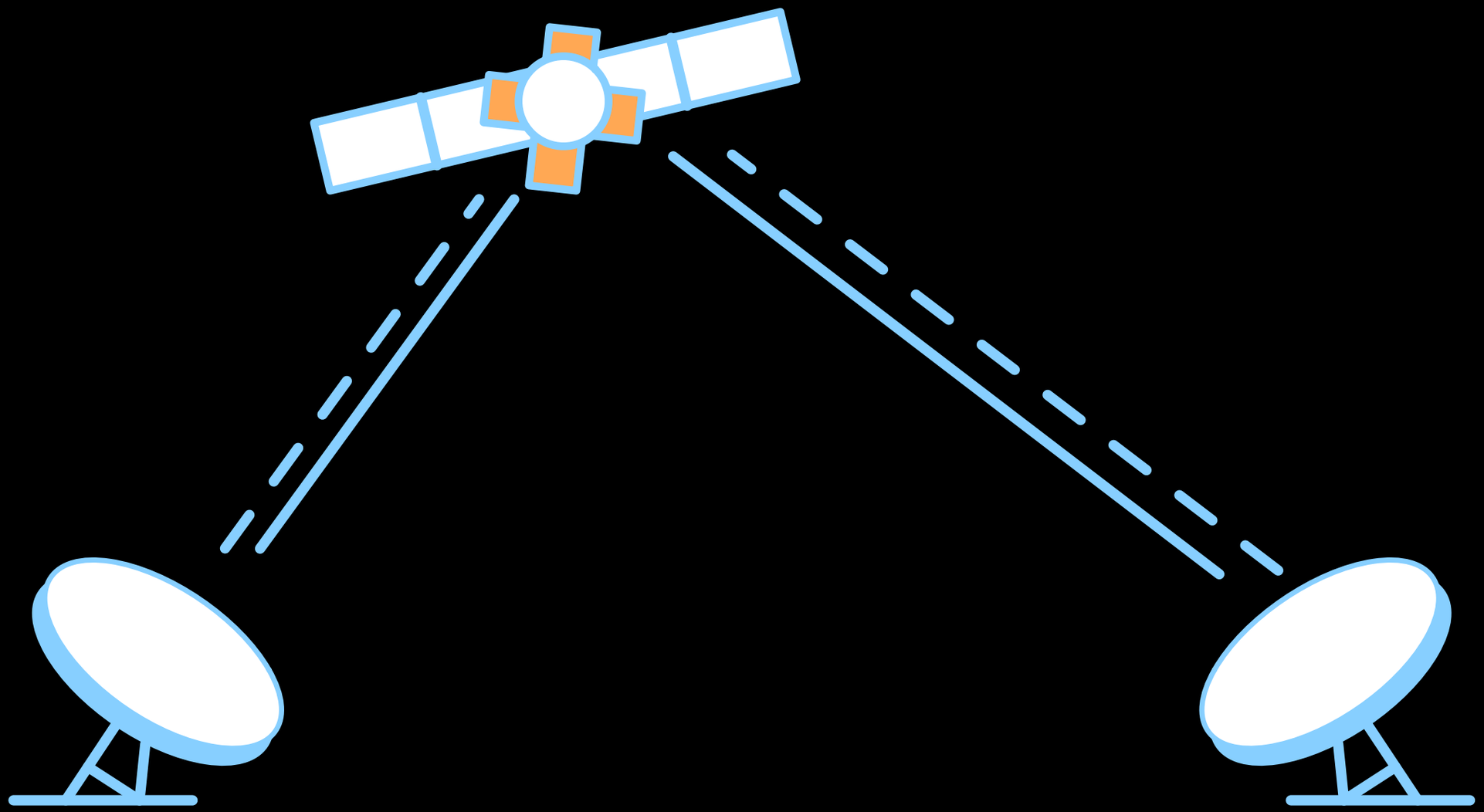


Demo

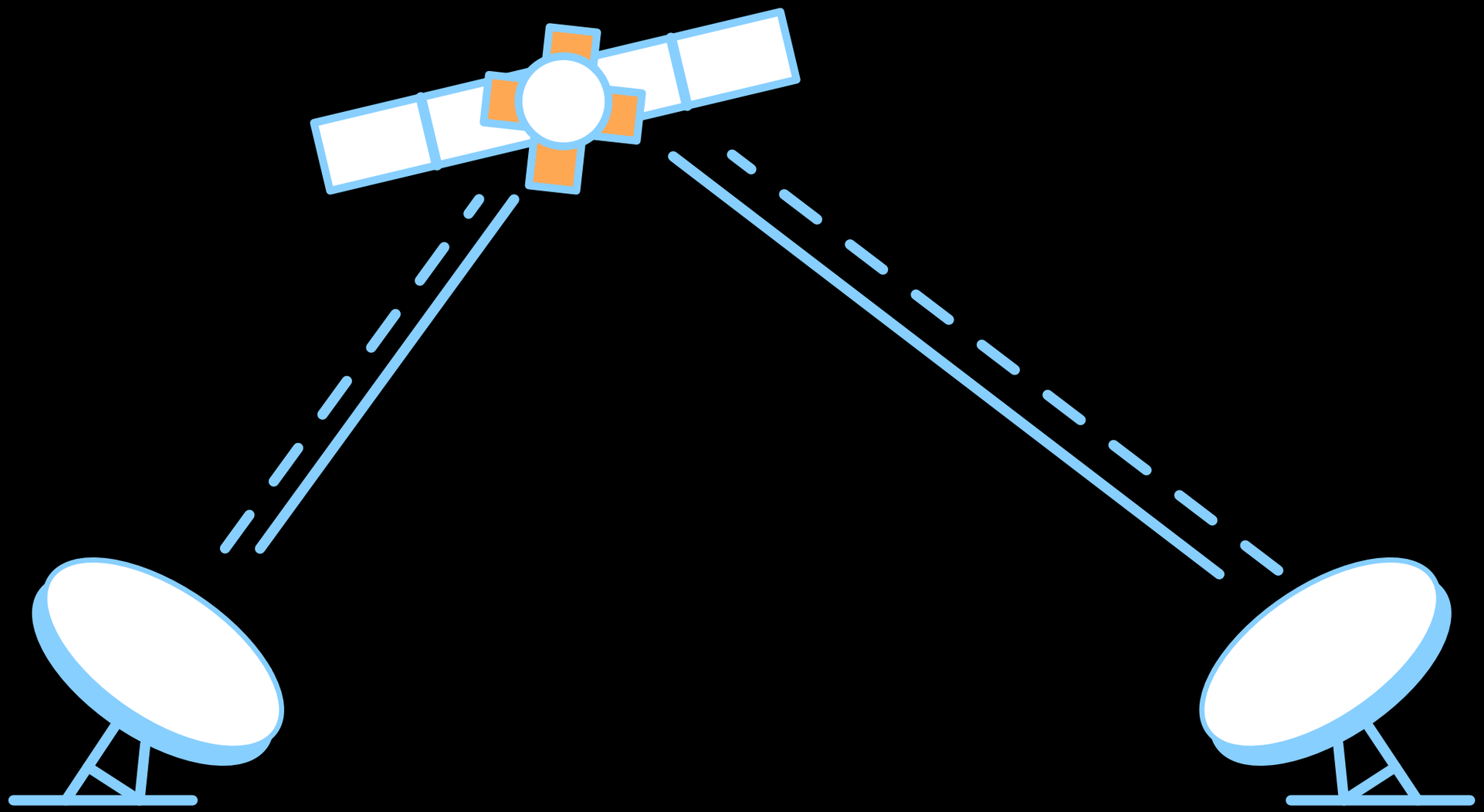
Rogue Carrier Detection Evasion

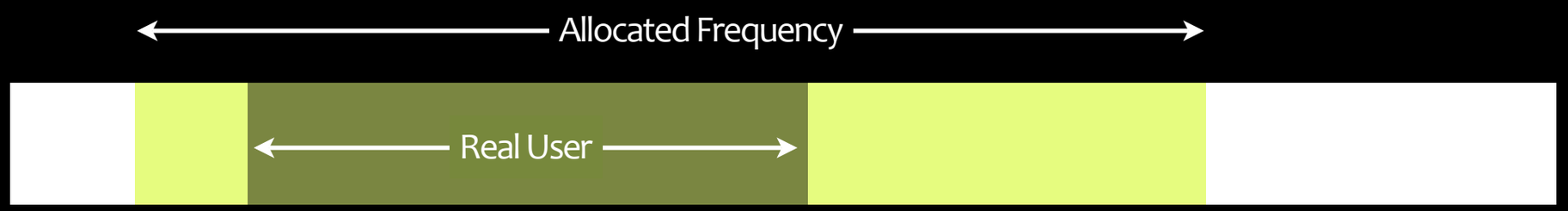


Rogue Carrier Detection Evasion

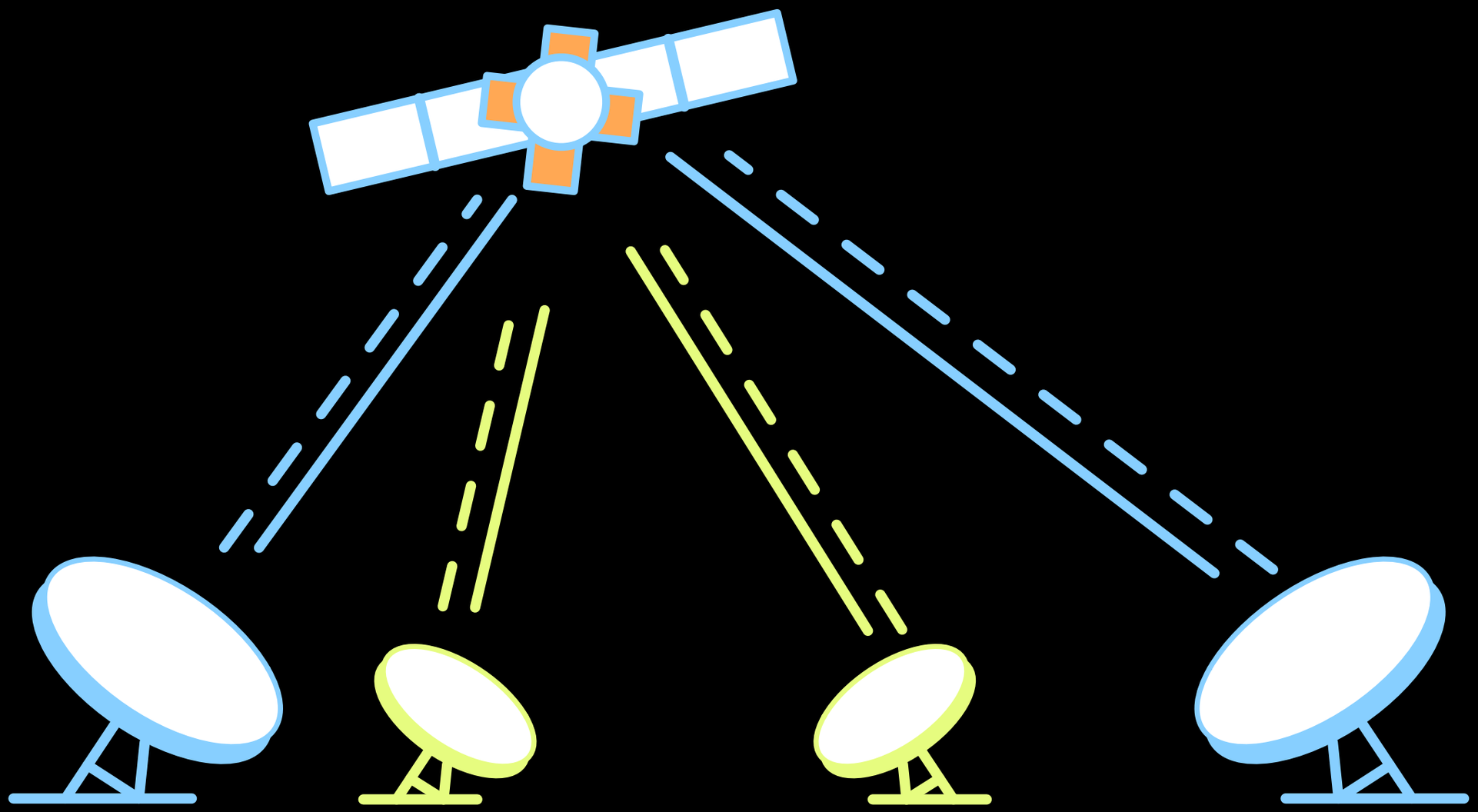


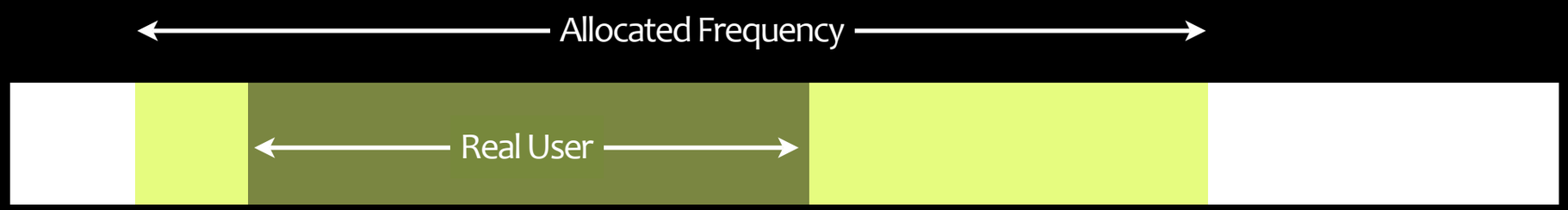
Rogue Carrier Detection Evasion



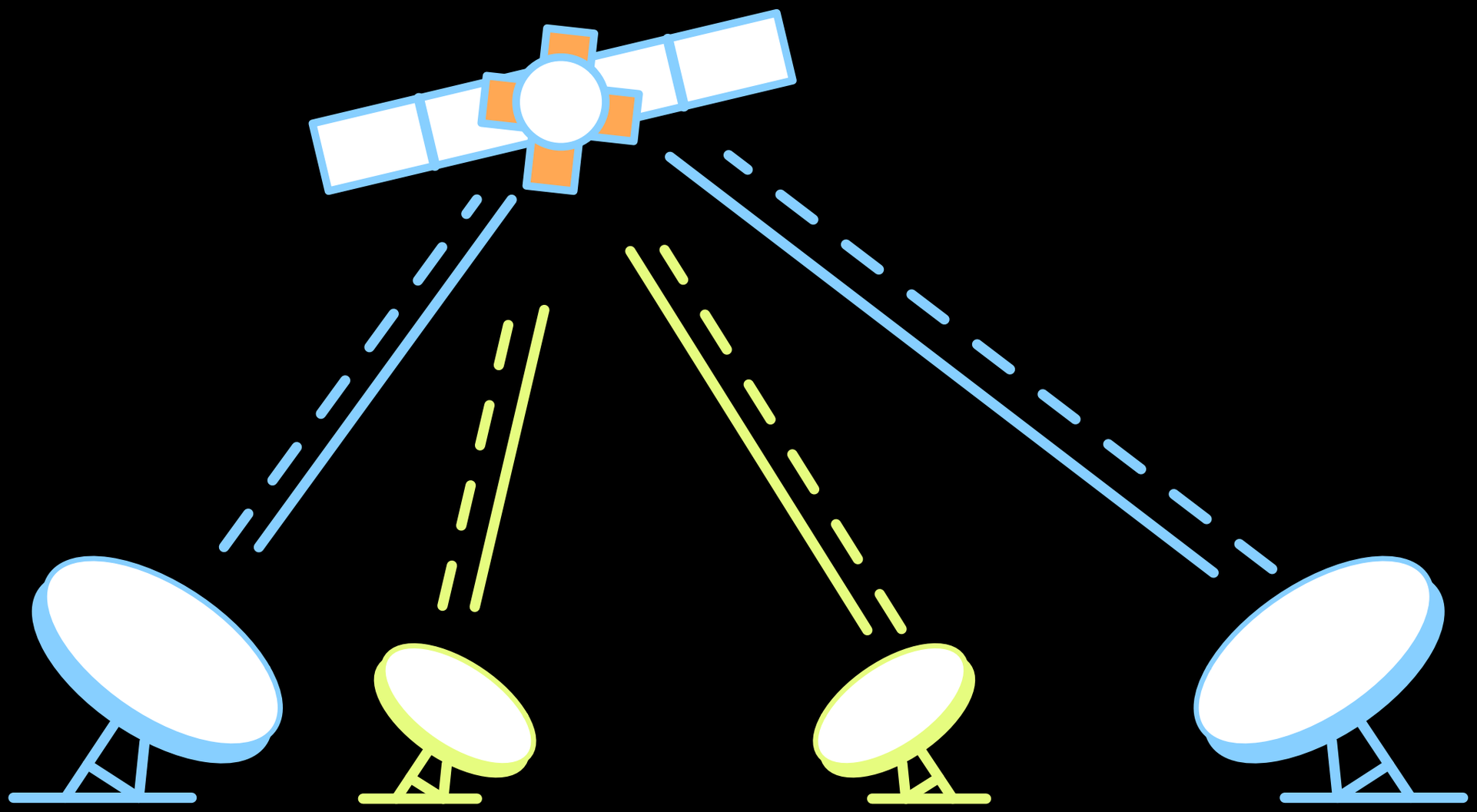


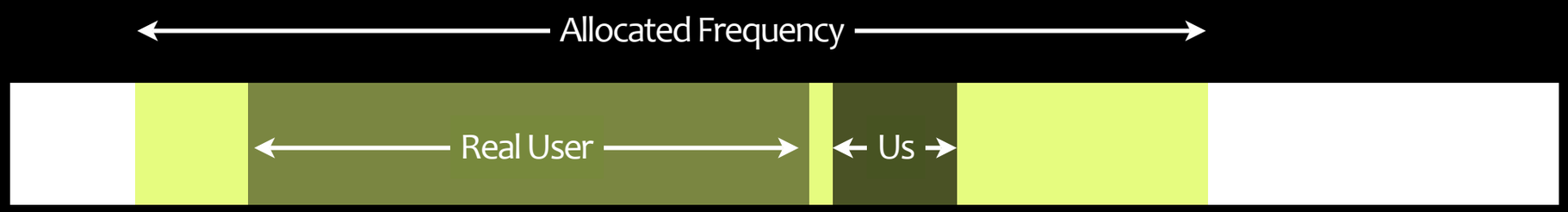
Rogue Carrier Detection Evasion



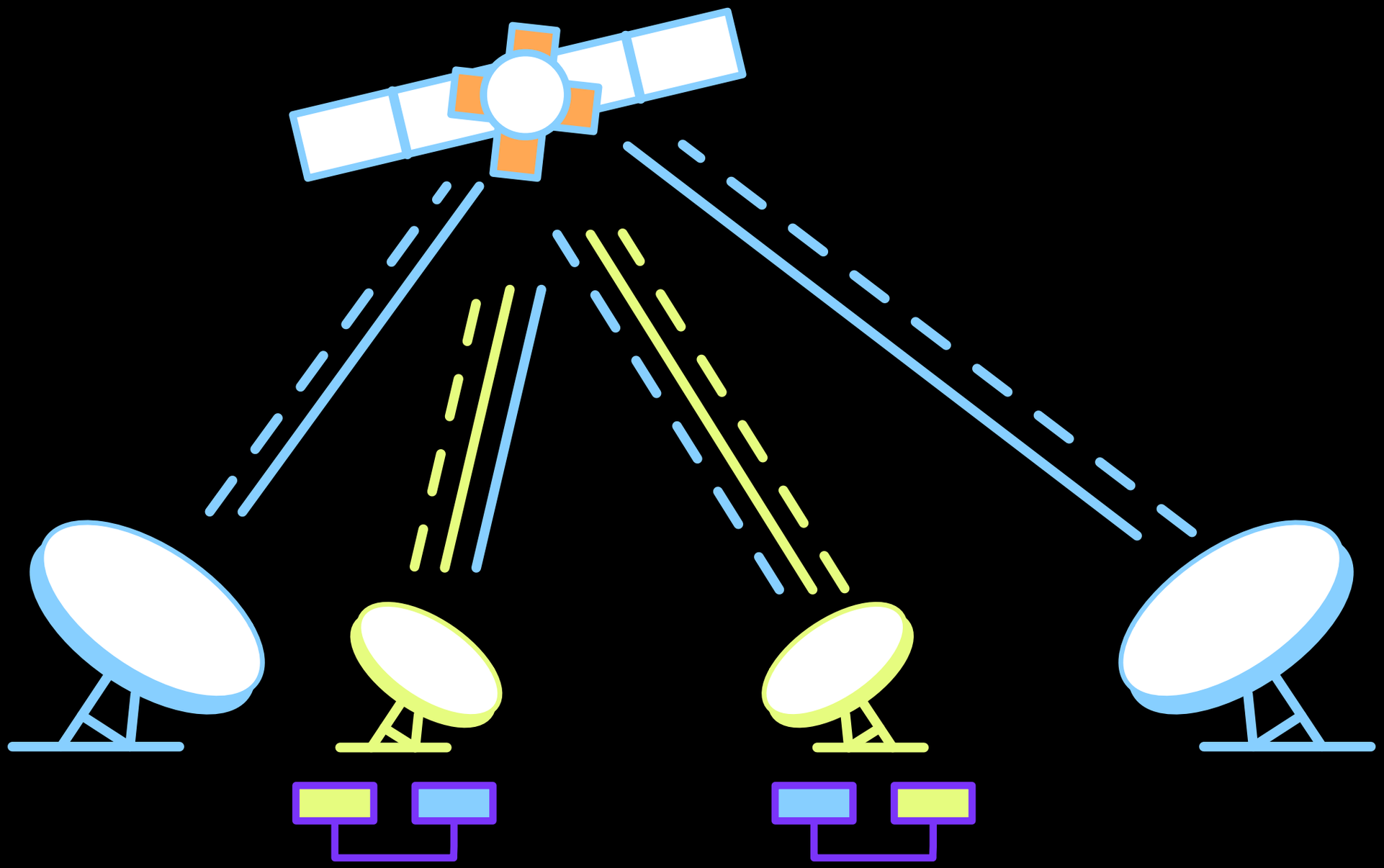


Rogue Carrier Detection Evasion

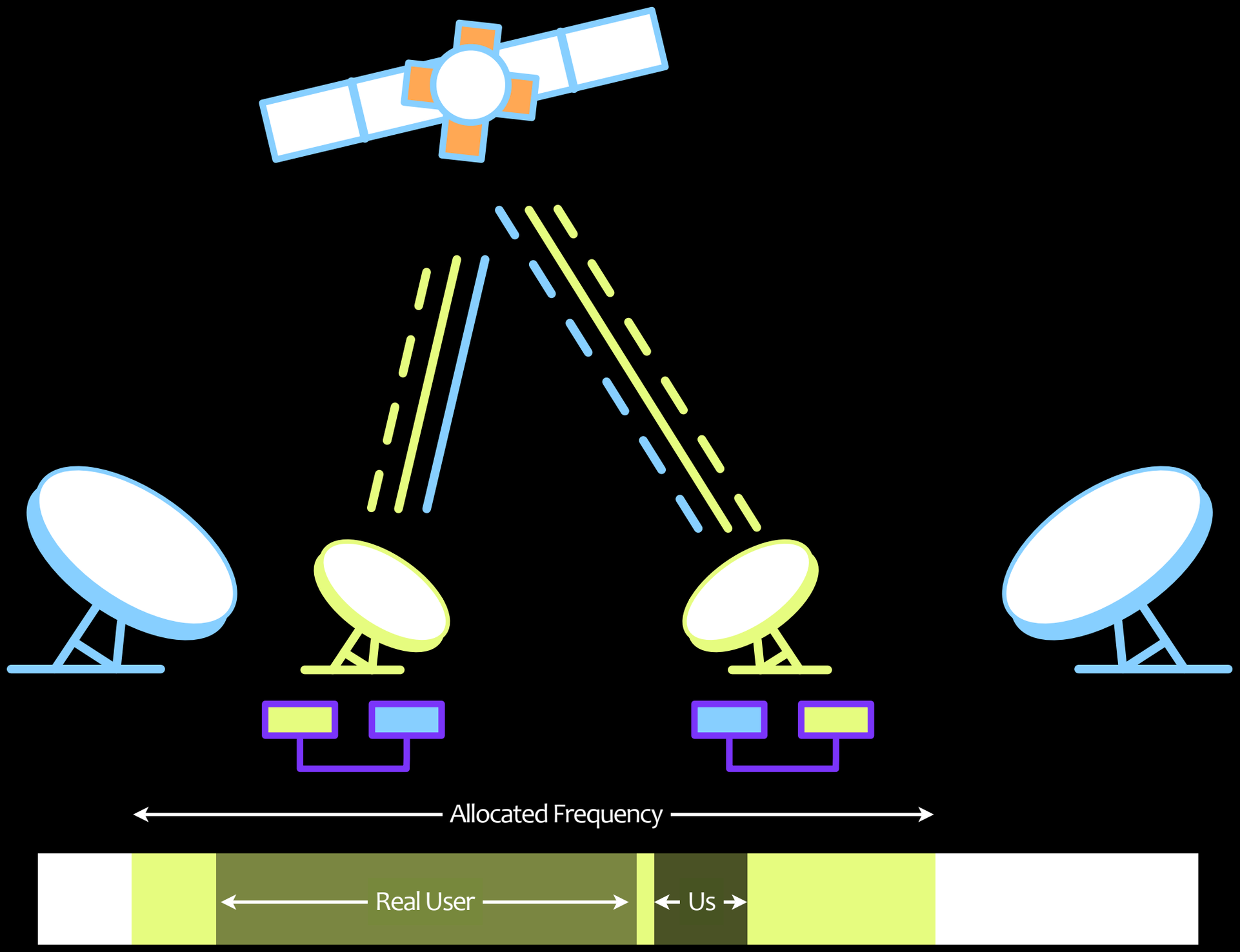




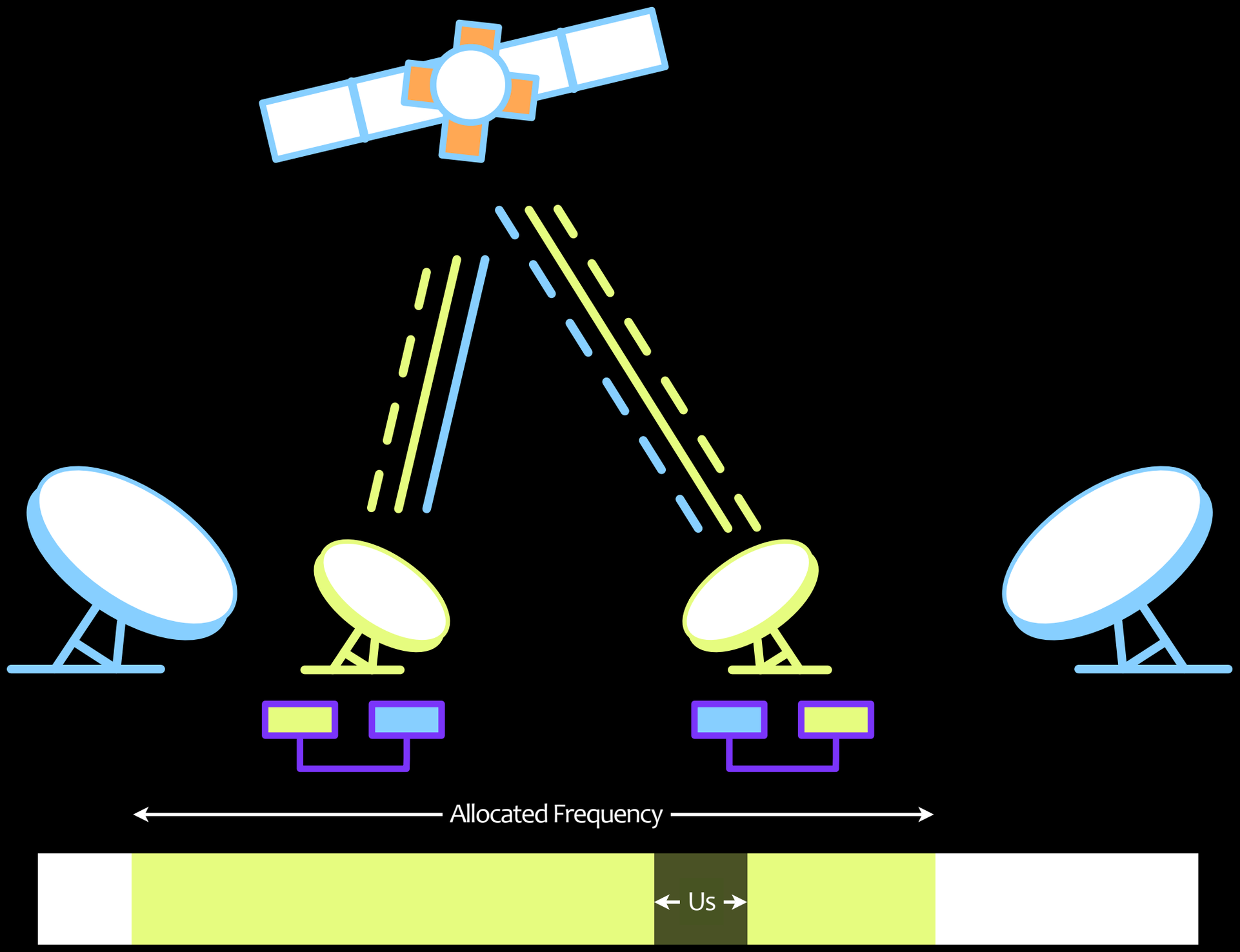
Rogue Carrier Detection Evasion



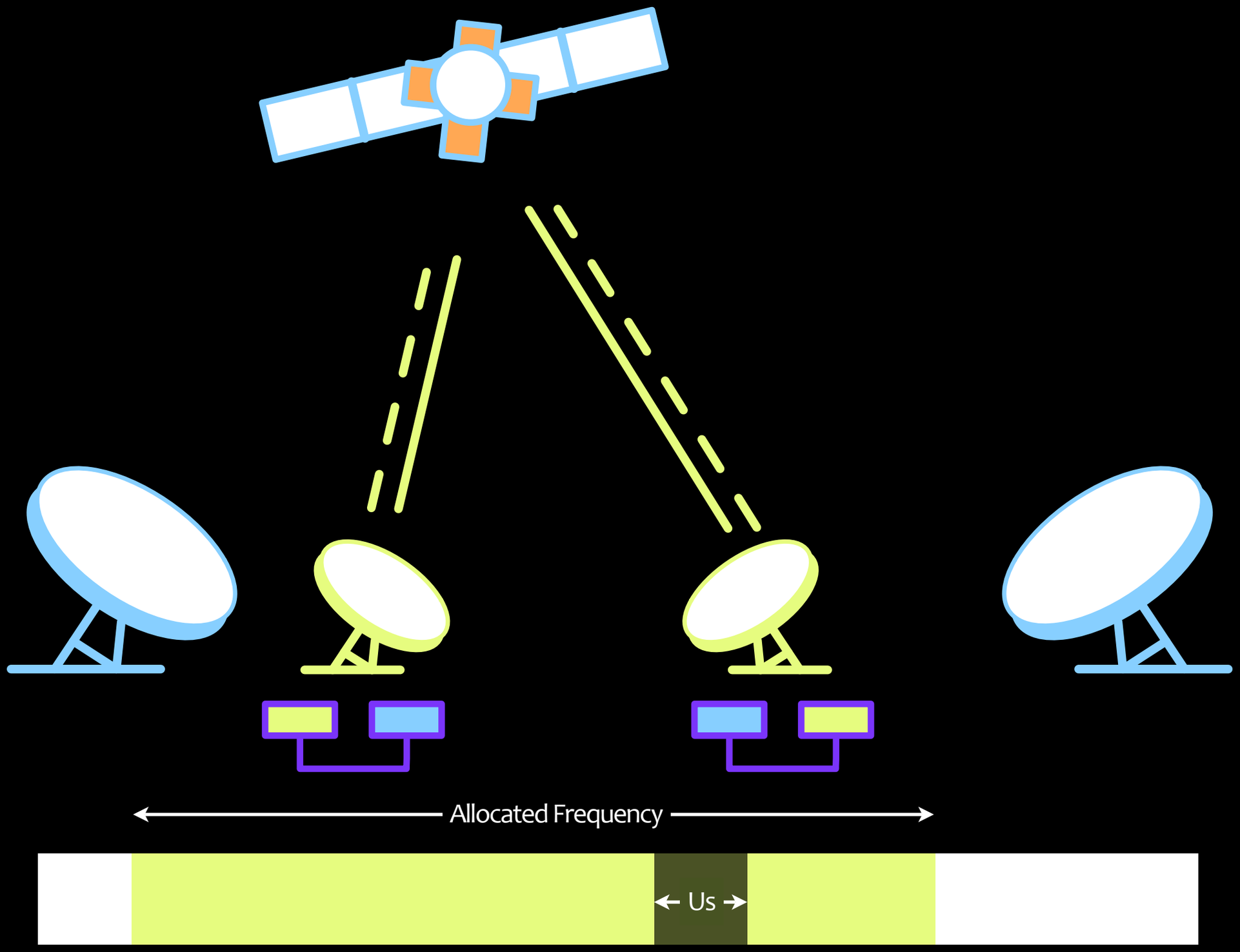
Rogue Carrier Detection Evasion



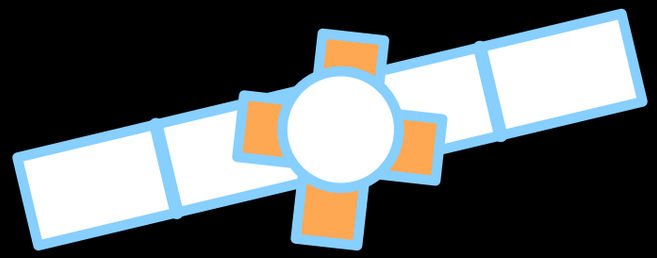
Rogue Carrier Detection Evasion

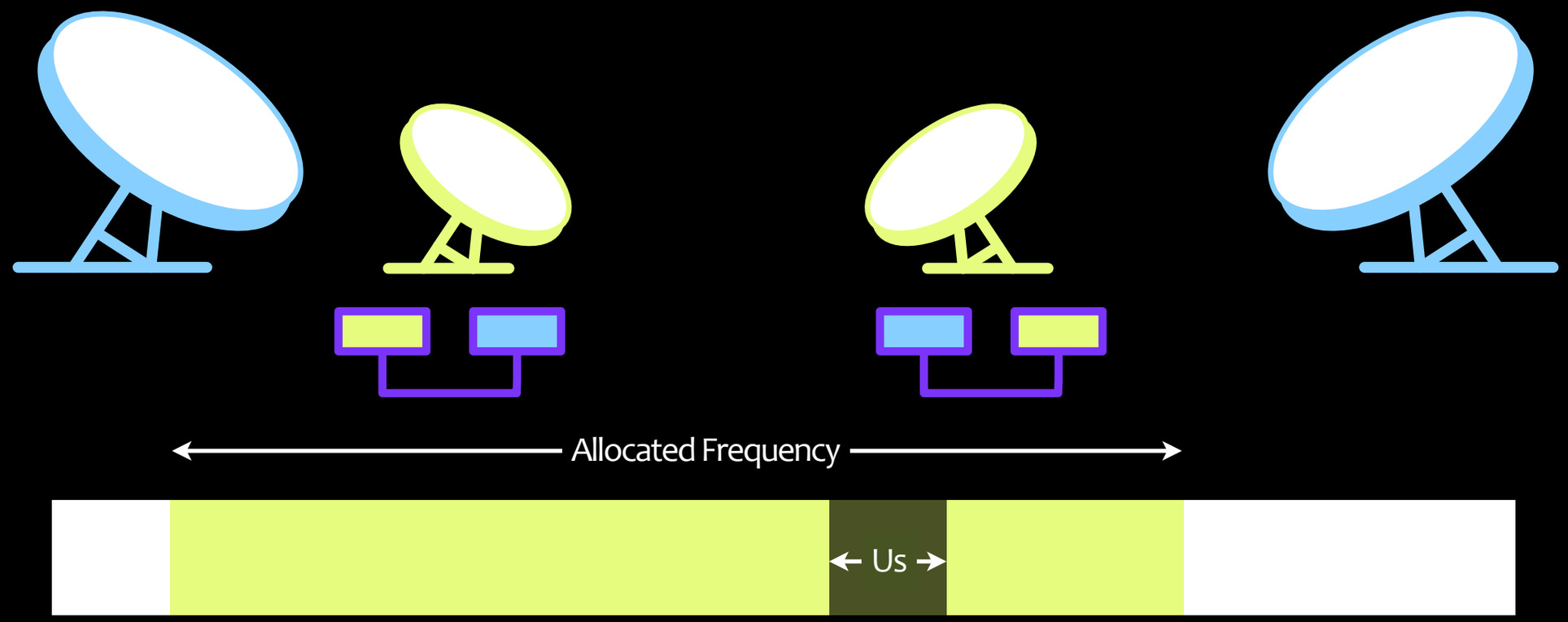


Rogue Carrier Detection Evasion

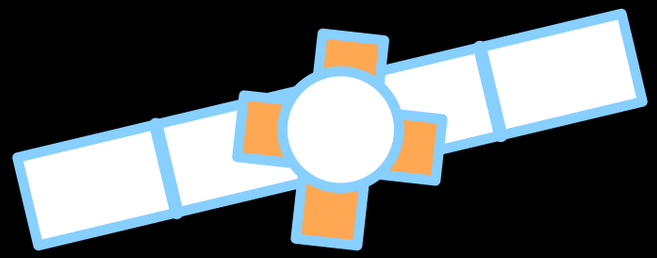


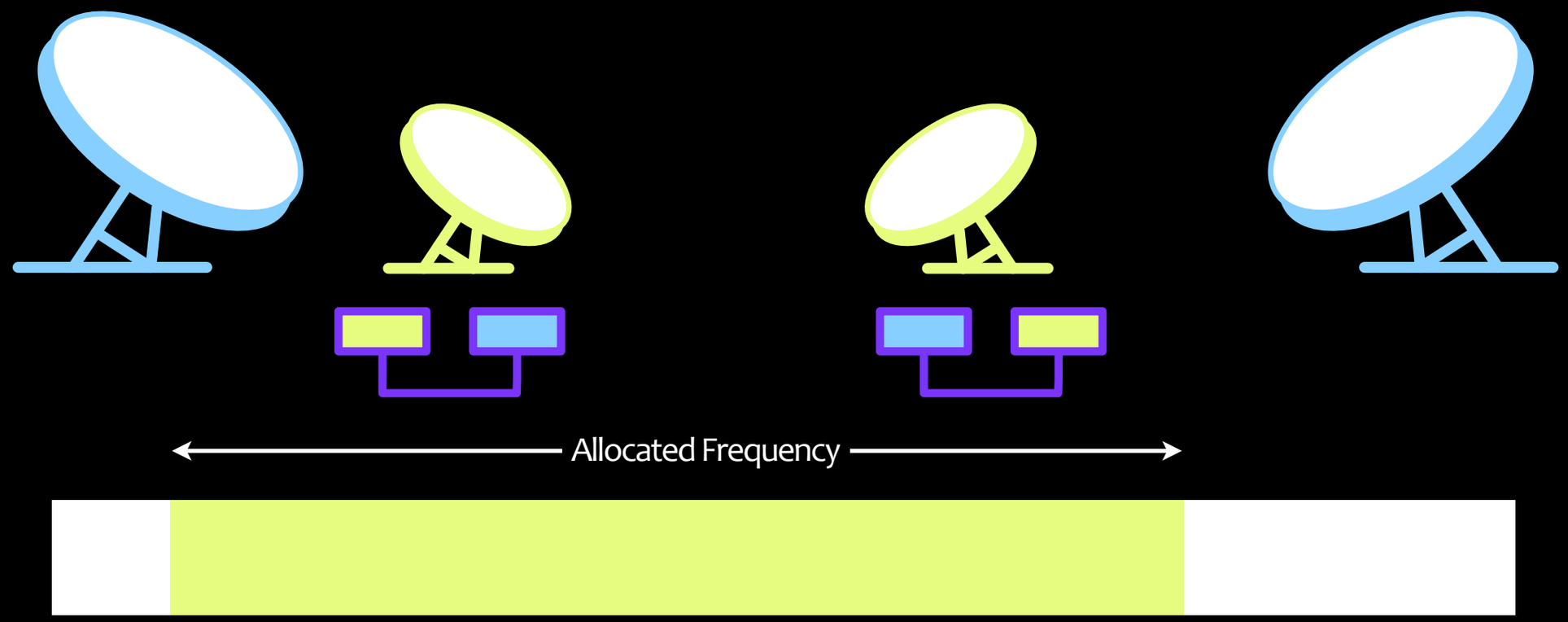
Rogue Carrier Detection Evasion





Rogue Carrier Detection Evasion





Detection Issues

- Require at least another satellite and satellite operator to detect rogue carrier (similar to GPS mechanism).
  - Satellite operator alliance co-operation.
  - Specialised company detecting rogue carrier.
- Hard to detect if rogue carrier has ability to switch frequency automatically prior detection.

The End

- Last year, we managed to present how to compromise data link layer.
- Today, we present how to compromise network layer.

The End

- Last year, we managed to present how to compromise data link layer.
- Today, we present how to compromise network layer.

Data Link + Network = ?