RESILIENT COMMUNICATIONS AVAILABILITY

Inverting the Confidentiality, Integrity, and Availability Paradigm

Presented by

STEVE CHAN

IARIA CYBER 2020

TABLE OF CONTENT

INTRODUCTION

"Although signal boosters can improve cell phone coverage, malfunctioning, poorly designed, or improperly installed signal boosters can interfere with wireless networks and cause interference to a range of calls, including emergency and 911 calls."

Federal Communications Commission (FCC)

The market demand for boosters has increased dramatically. However, not all of these signal boosters comply with FCC standards.

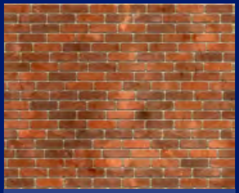
This paper will examine the notions of reliability and resiliency for communications networks amidst some known cyber electromagnetic spectrum phenomena, which can readily segue to a cyber kill chain.

COMMUNICATIONS COVERAGE

Mountain

Hills

Concrete


Brick

Valleys

Trees

Metal

Glass

Wood

Plaster

Drywall

Plywood

Weather

Cellular Coverage

Cellular signals are radio waves, and as with all types of radio frequency waves, they are readily susceptible to Radio Frequency Interference (RFI). **RFI can be caused by** outside environs, the transition from an outside to an inside environs, internal interference, and weather also has a tremendous impact.

A cellular signal booster (a.k.a. amplifier or repeater) can assist matters by amplifying the weak signal.

Non-Cellular Coverage

Non- cellular wi-fi is a method for devices to connect wirelessly to the internet via radio frequency waves. Similar to cellular, **wi-fi is also susceptible to interference**, such as from other wi-fi networks and other usages within the utilized bands.

wi-fi can be faster than 3G 4G

↓

REGULATORY COMPLIANCE AND ADHERENCE

REGULATORY COMPLIANCE AND ADHERENCE

Signal boosters are subject to the wireless licensee's presumptive authorization

Bi-Directional Amplifiers (BDAs) shall have oscillation prevention circuitry and a spectrum analyzer

Signal boosters may only be operated on a channelized basis on the proscribed frequencies utilized by the wireless licensee

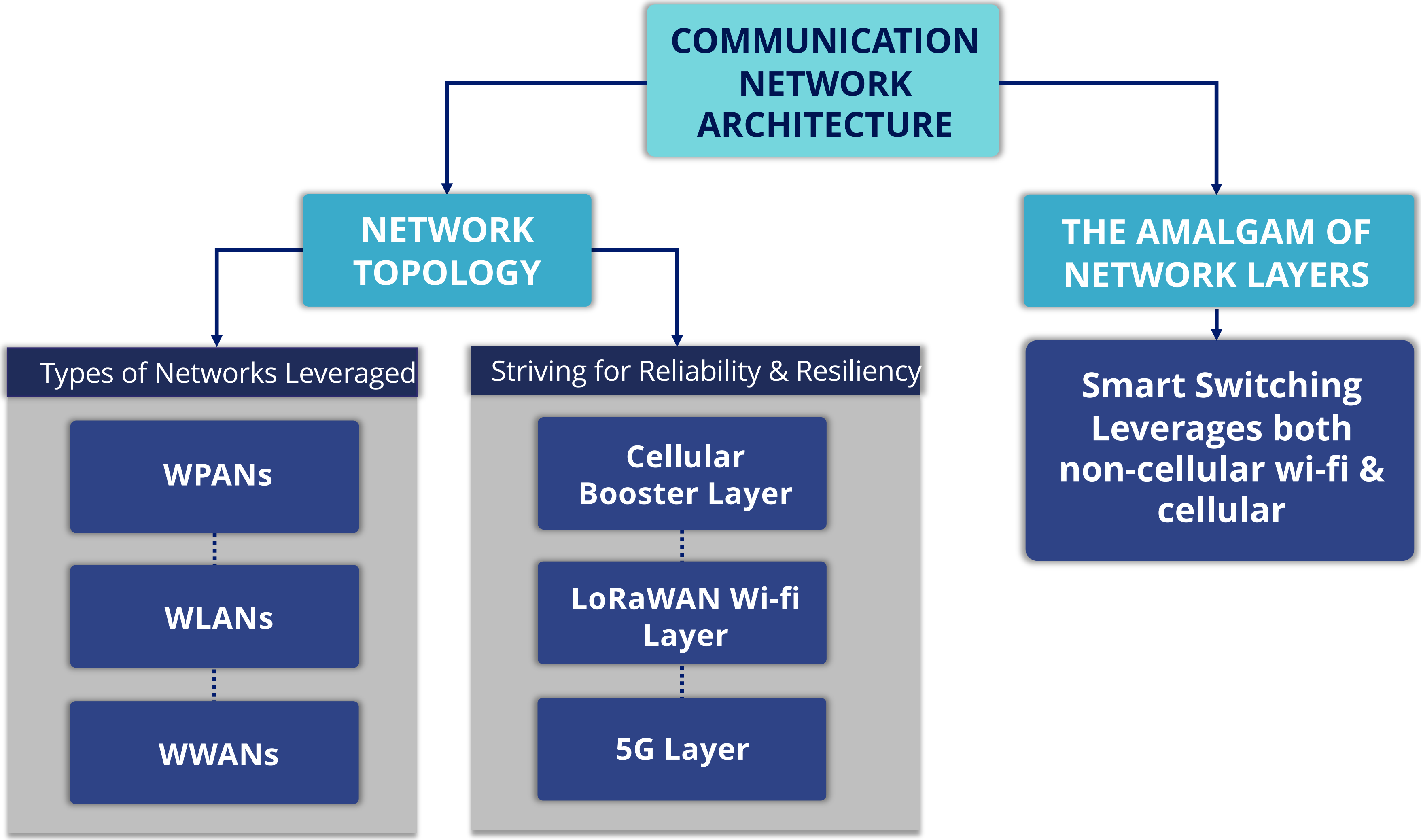
Signal boosters shall have FCC or other radio licensing authority and be suitable for safety installation

Signal boosters are designed with oscillation detection and will terminate transmission when oscillation occurs

Signal boosters are subject to the FCC's equipment and industry certification process, and approval by the individual licensee

*IFC refers to the International Code Council's (ICC) 2018 International Fire Code (IFC)

COMMUNICATIONS ARCHITECTURES


COMMUNICATION NETWORK ARCHITECTURE
NETWORK TOPOLOGY
THE AMALGAM OF NETWORK LAYERS
Types of Networks Leveraged
WPANs
WLANs
WWANs
Striving for Reliability & Resiliency
Cellular Booster Layer
LoRaWAN Wi-fi Layer
5G Layer
Smart Switching Leverages both non-cellular wi-fi & cellular

PREDELICTION TOWARDS AVAILABILITY

PREDELICTION TOWARDS AVAILABILITY

2004

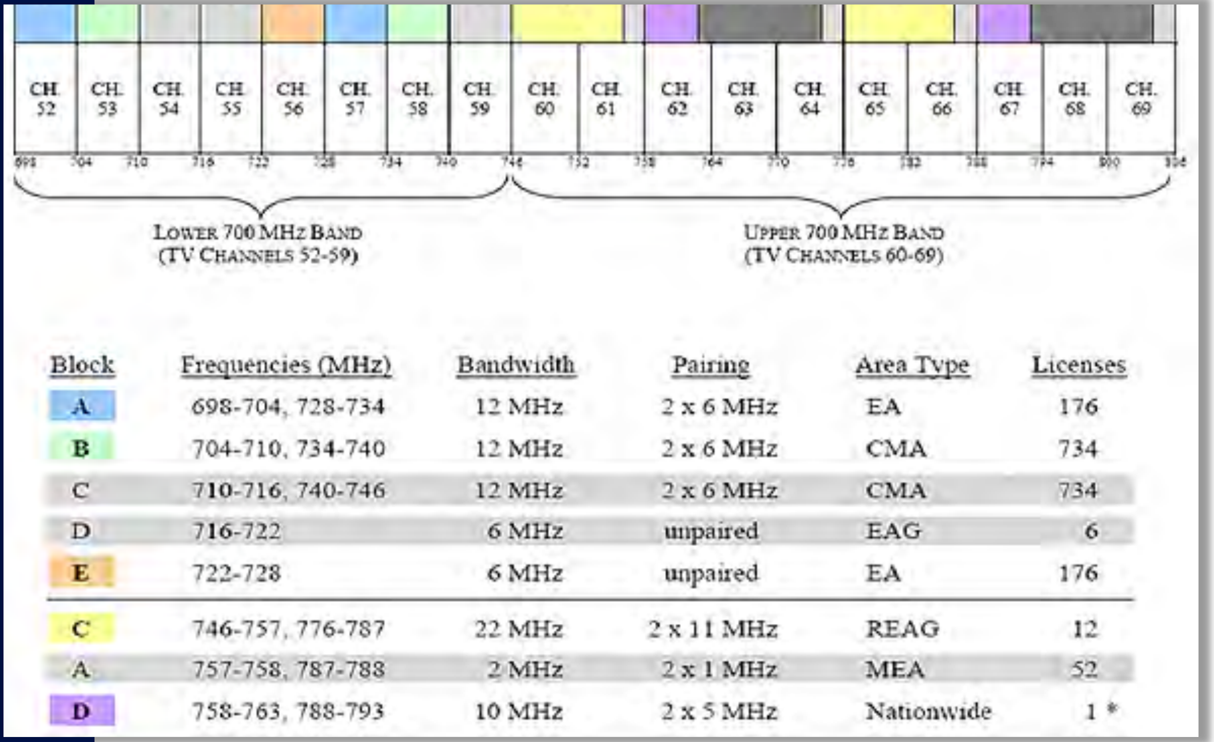
Land Mobile Radios (LMRs) have been the most reliable and secure method of voice communication.

2008

The FCC auctioned licenses for segments of the 700 MHz Band for commercial purposes.

2012

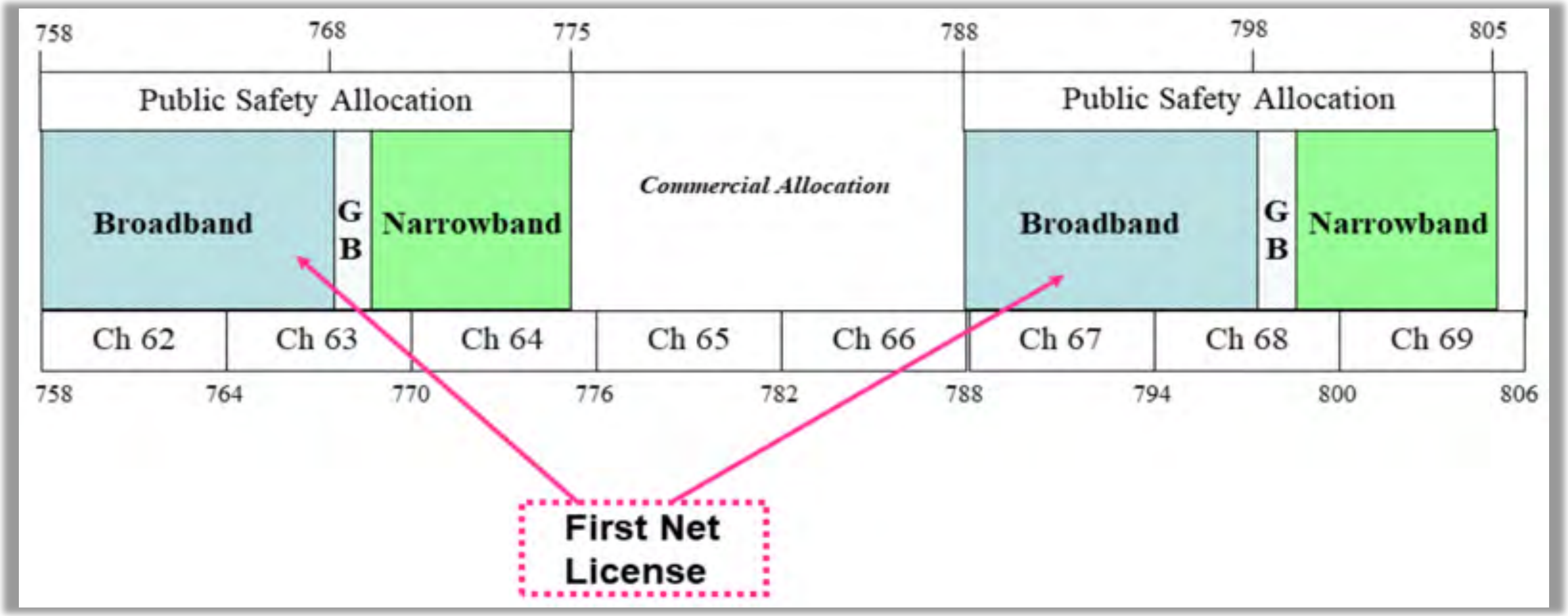
The U.S. Congress directed the FCC allocated the D-Block (758-763 MHz/788-793 MHz) for a public safety nationwide broadband network.


CH. 52
CH. 53
CH. 54
CH. 55
CH. 56
CH. 57
CH. 58
CH. 59
CH. 60
CH. 61
CH. 62
CH. 63
CH. 64
CH. 65
CH. 66
CH. 67
CH. 68
CH. 69
698
704
710
716
722
728
734
740
746
752
758
764
770
776
782
788
794
800
806
LOWER 700 MHZ BAND
(TV CHANNELS 52-59)
UPPER 700 MHZ BAND
(TV CHANNELS 60-69)

Block	Frequencies (MHz)	Bandwidth	Pairing	Area Type	Licenses
A	698-704, 728-734	12 MHz	2 x 6 MHz	EA	176
B	704-710, 734-740	12 MHz	2 x 6 MHz	CMA	734
C	710-716, 740-746	12 MHz	2 x 6 MHz	CMA	734
D	716-722	6 MHz	unpaired	EAG	6
E	722-728	6 MHz	unpaired	EA	176
C	746-757, 776-787	22 MHz	2 x 11 MHz	REAG	12
A	757-758, 787-788	2 MHz	2 x 1 MHz	MEA	52
D	758-763, 788-793	10 MHz	2 x 5 MHz	Nationwide	1 *

2017

First Net formed a public-private partnership with AT&T. AT&T obtained access to the 20 MHz segment of the Band 14 spectrum (758-768 MHz/788-798 MHz)



First Net Licensed Portions of the 700 MHz Spectrum

As the main backbone of AT&T's Long-Term Evolution (LTE) network (which has substantial nationwide coverage) previously consisted of a superset of Band 17 and Band 12 (699-716 MHz/729-746 MHz), AT&T's First Net cellular network soon comprised both Bands 12 and 14.

■ ■ ■ ■ New security vulnerabilities

Institute of Standards and Technology (NIST)

“the preference towards availability and the looming vulnerabilities of having band 14 in so may devices constitutes a large attack surface area.”

If the network is overloaded with public-safety use, it would not be available for citizen 911 calls or alerting by citizens.

KNOWN CYBER VULNERABILITIES

Next Generation 911 (NG911)

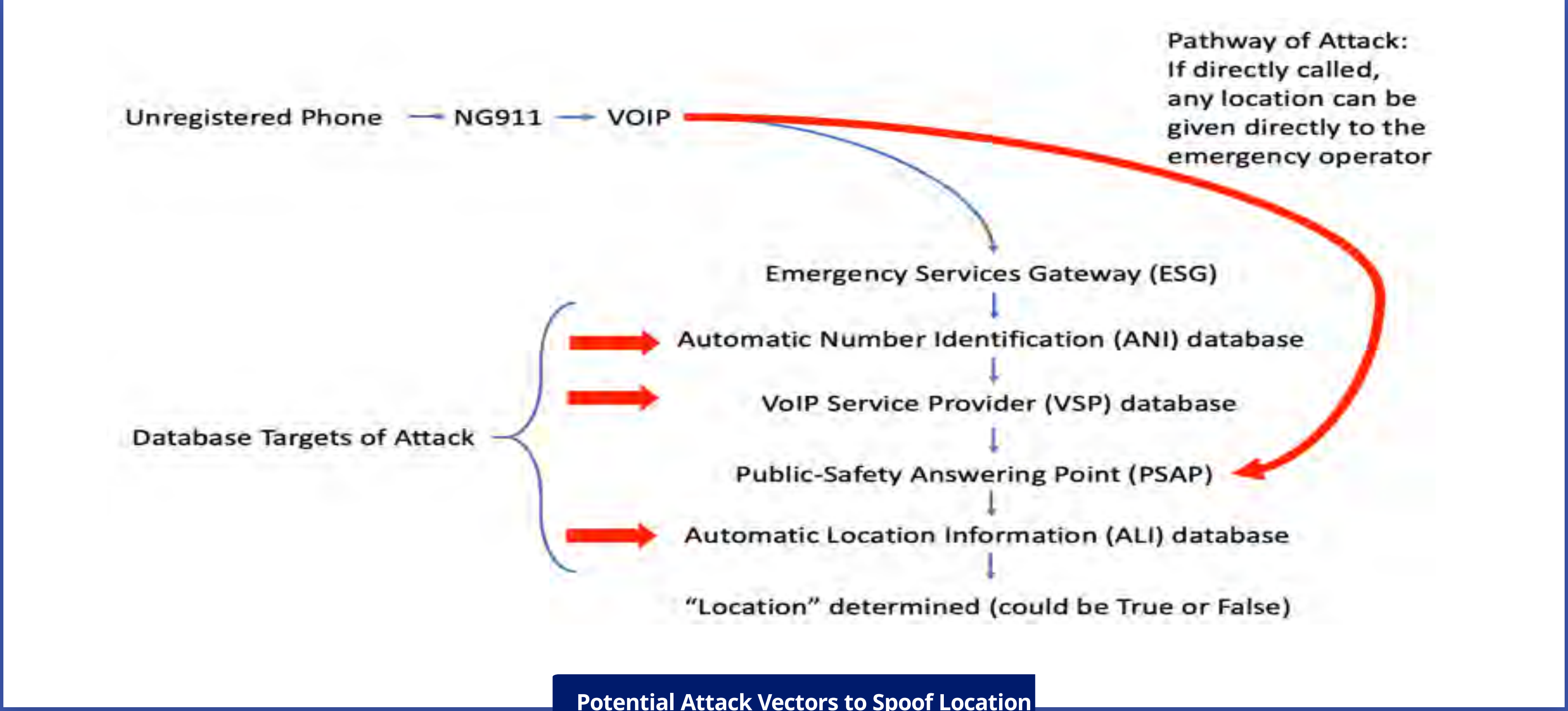
Carriers have transitioned from circuit-switched 911 infrastructure to Voice over Internet Protocol (VoIP) infrastructure, which is referred to NG911.

- ✓ Mitigate against the DDoS & TDoS problem
- ✓ Increase the capacity and avoid bottlenecks
- ✓ Load balancing among Public-Safety Access Points (PSAPs) improves reliability
- ✓ Callers can also transmit text, images, video and other data to the PSAPs.

Known Cyber Vulnerabilities

Distributed Denial of Service (DDoS) or Telephony Denial of Services (TDoS) attacks could affect 911 call systems. With only **6,000 infected phones**, it was possible to effectively **block 911 calls from 20% of the state’s landline callers.**

VoIP Vulnerability



Unregistered Phone → NG911 → VOIP

Pathway of Attack:
If directly called,
any location can be
given directly to the
emergency operator

Emergency Services Gateway (ESG)

Automatic Number Identification (ANI) database

VoIP Service Provider (VSP) database

Public-Safety Answering Point (PSAP)

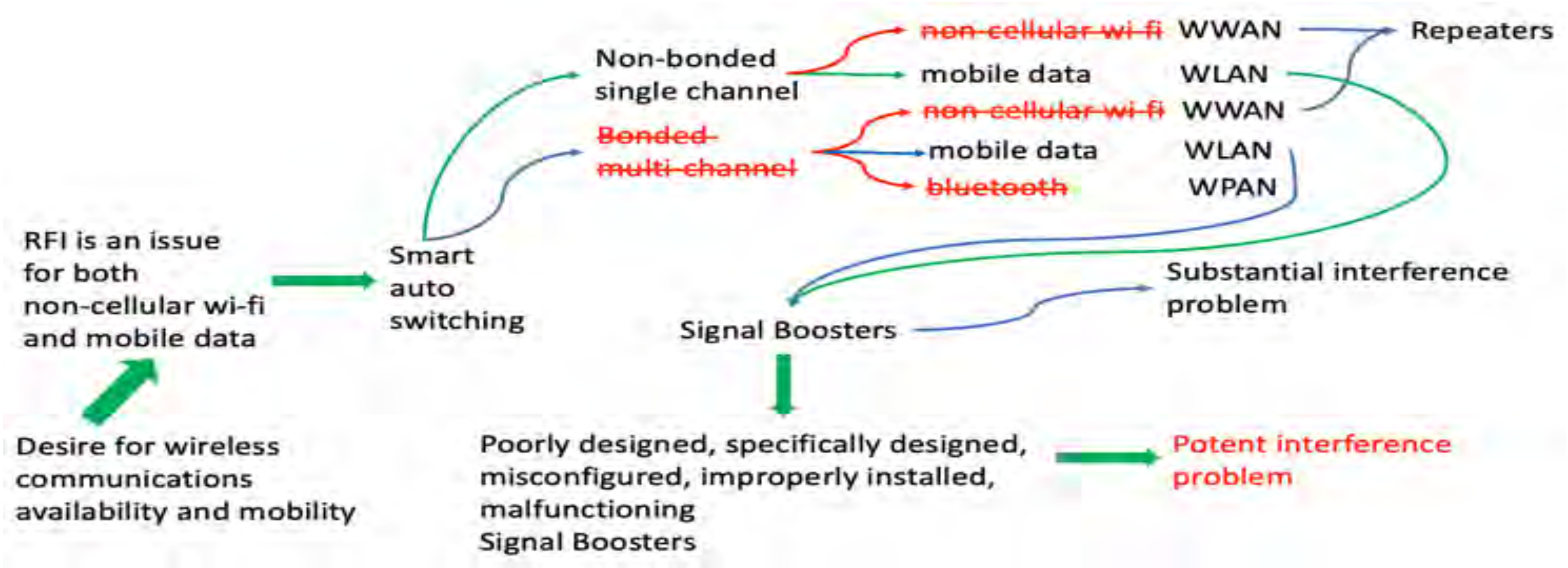
Automatic Location Information (ALI) database

"Location" determined (could be True or False)

Database Targets of Attack

Potential Attack Vectors to Spoof Location

EXPERIMENTATION/ SIMULATION



RFI is an issue for both non-cellular wi-fi and mobile data

Desire for wireless communications availability and mobility

Smart auto switching

Non-bonded single channel

~~Bonded multi-channel~~

~~non-cellular wi-fi~~ WWAN

mobile data WLAN

~~non-cellular wi-fi~~ WWAN

mobile data WLAN

~~bluetooth~~ WPAN

Repeaters

Signal Boosters

Substantial interference problem

Poorly designed, specifically designed, misconfigured, improperly installed, malfunctioning Signal Boosters

Potent interference problem

SIMULATED ON GNU OCTAVE | **Limiting the channels available for use creates a more potent honeypot observational space cyber kill chain**

Simulation Setup

Bluetooth and Wi-fi

Bluetooth Adaptive Frequency-Hopping (AFH) spread spectrum on twenty collocated WPANs. The Bluetooth simulation engaged in changing channels up to 1600 times per second among 79 channels on the 2.4 GHz band. Wi-fi networks on twenty collocated WLANs (on the 2.4 GHz and 5 GHz band).

FirstNet-capable Devices

The specified effective range for the devices were as follows: 200 meters from a hub for cellphones, 400 meters from a hub for tablets, and 900 meters from a hub for laptops.

HUB

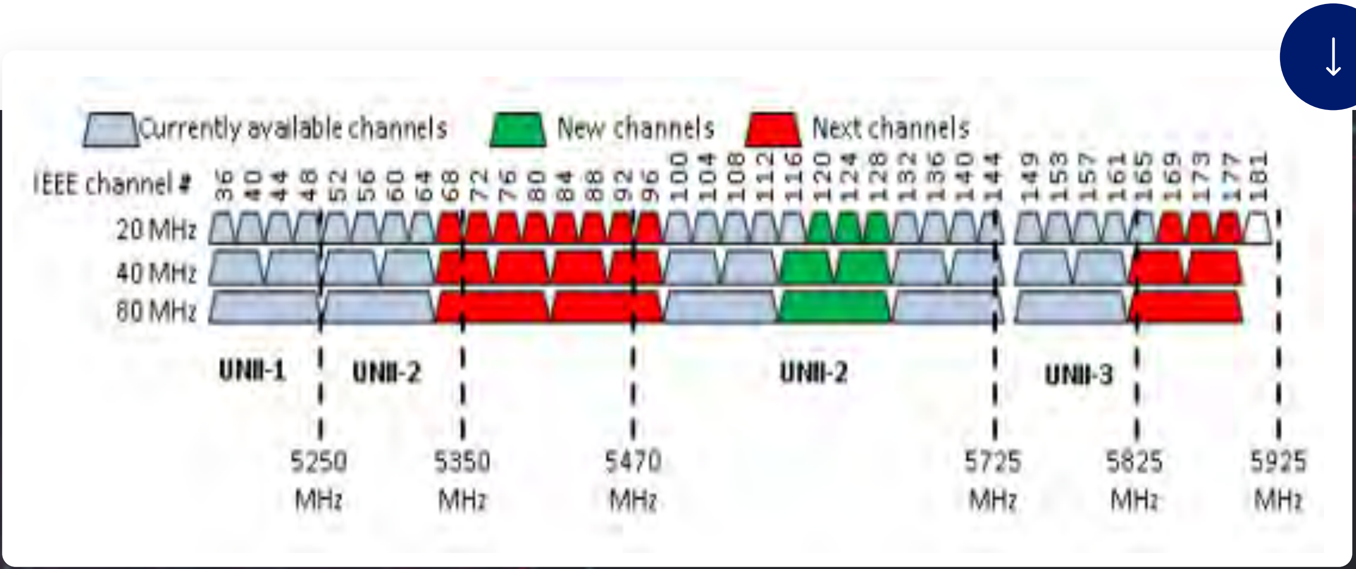
The effective range between a hub to another hub (i.e., remote hub) was established as 3 km. At 1.5 km, the bandwidth was 10 Million bits per second (Mbps); at 3 km, the bandwidth is < 5 Mbps.

The urban/rural Demarcation

The urban/rural demarcation was set at 1.5 km. As the “urban” area was congested with Bluetooth traffic, the wi-fi avoided the 2.4 GHz and endeavored to utilize the 5 GHz band.

CYBER KILL CHAIN

Unlicensed National Information Infrastructure (U-NIII) Segments and IEEE Channels on the 5GHz Wi-Fi Spectrum



Co-tier interference (between neighboring femtocells) and cross-tier interference (among different tiers of the network) were also emulated so as to force the communications to return to Channel 40 (between 5170 and 5250 MHz) on U-NII-1. The Berkeley Packet Filter (BPF) was utilized to monitor the channels, specifically Channel 40.

An Even More Potent Cyber Kill Chain

Signal boosters have been utilized to bridge the gap for the “last mile” paradigm. **Ironically,** boosters can readily interfere with the existing communications used by system operators and linemen, who are servicing the involved critical infrastructure.

Incidental Emitters

The substantive portion of the noise emanating from electric utility equipment stems from incidental emitters. Yet, there are no specific limits on the conducted or radiated emissions.

Unintentional Emitters

This type of emitter intentionally generates an internal radio signal; it does not intentionally radiate/transmit it.

CONCLUSION

01

Availability for Emergency Services

Availability for emergency services is significant for modern society. The number and privatization of various communication backbones has fueled the use of private-owned-signal boosters.

02

Communication Networks Degradation

Cases of misused cellular boosters, deliberate Bluetooth congestion, and intentional interference with wi-fi and last–mile communication technologies indicates that it is possible to interfere with both cellular and VoIP 911.

03

Future Works

Future work will build upon the described experimentation/simulation by congesting Wireless Wide Area Networks (WWANs). In this way, various simulated resilient communications architectures can be better explored and examined.

Sources for the various Figures are specified within the paper.

Thank You

For Your Attention !