IARIA

NexComm 2021 Congress
ISBN: 978-1-61208-907-2
April 18, 2021 to April 22, 2021 - Porto, Portugal

Radio Frequency Fingerprinting with Polarization Mode Dispersion

Page Heller
Endpoint Security Inc

ENDPOINT

Trends in Industrial Wireless Technology

MOL Danube Refinery

100 control valve positioners for M&D [1]

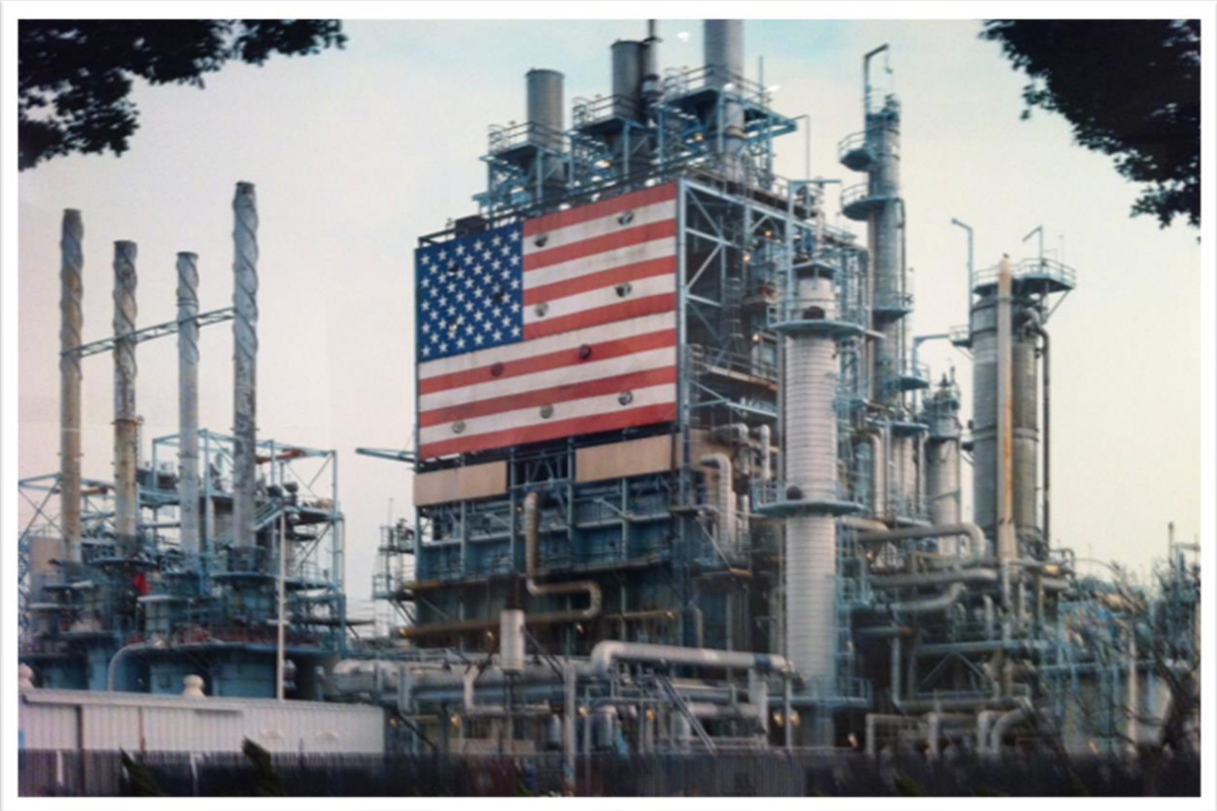
Ilsenburger Grobblech GmbH

Wireless thermometers for Alarms [2]

Oxea Chemical Plant

60 new wireless Sensors added last quarter[3]

BP Carson Refinery



400 wireless Sensors for Emission Compliance [4]

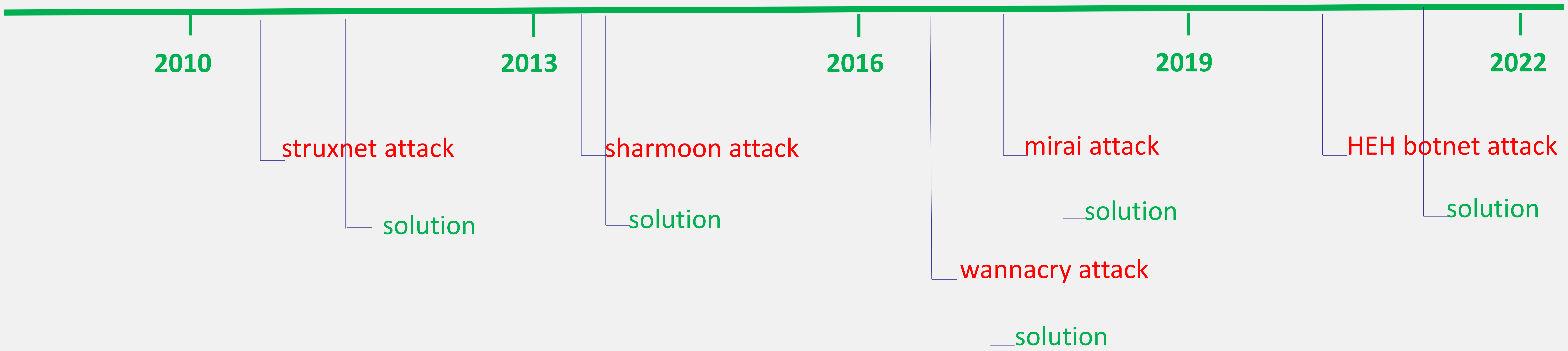
Improved Efficiency should not mean vulnerability to attack

The Challenge

Industry is using wireless sensors to improve operations

But, wireless devices are potential Entry Points into the network

State of Cybersecurity



2010

struxnet attack

solution

2013

sharmoon attack

solution

2016

wannacry attack

solution

mirai attack

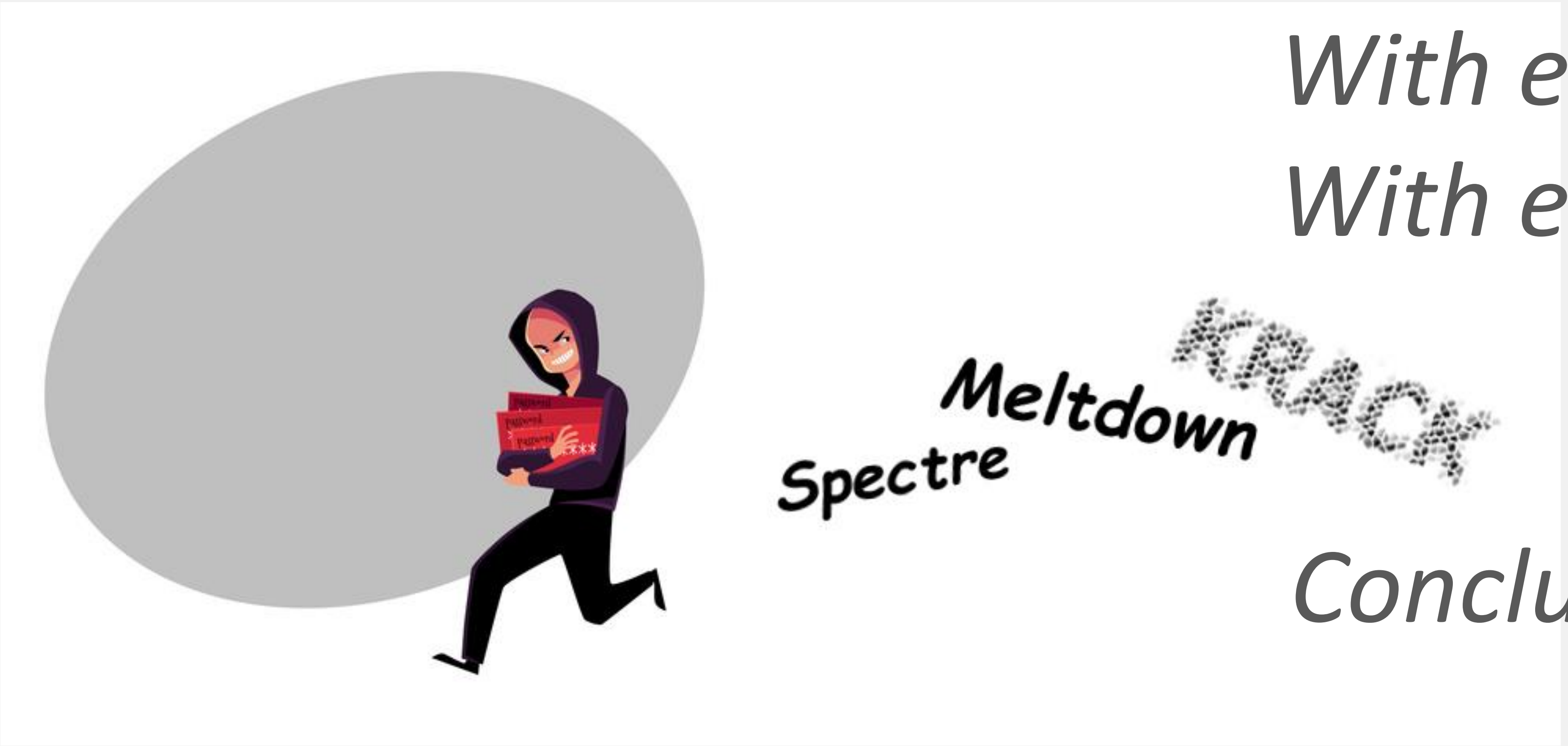
solution

2019

HEH botnet attack

solution

2022



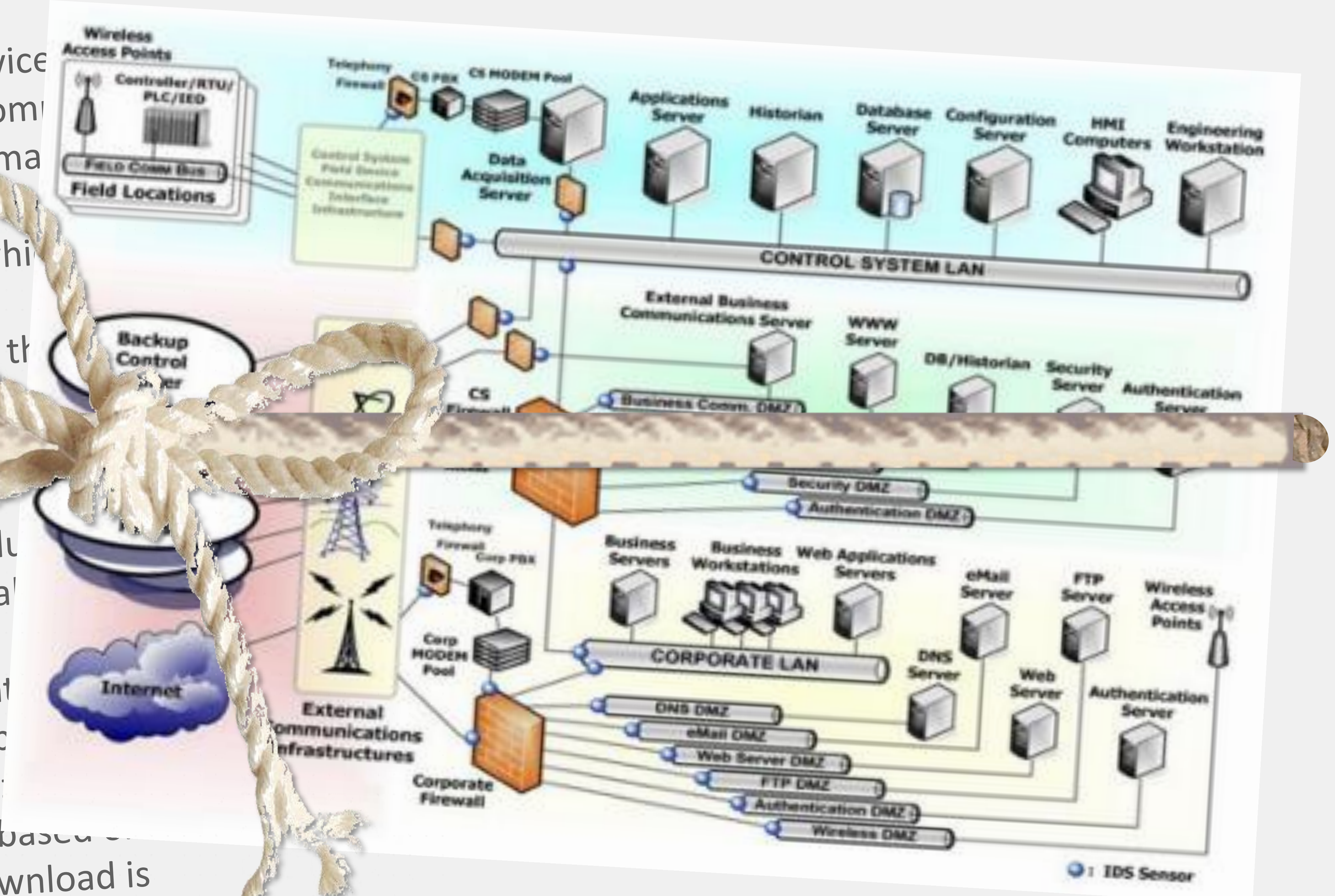
With every attack, a new solution is made.
With every solution there is a new vulnerability

Conclusion: we are chasing the perpetrator

Ties to Vendors Tightening

As security becomes more complex, vendors become sole source

JBOH (JavaScript-Binding-Over-HTTP) — A form of Android-focused mobile device
enables an attacker to be able to initiate the execution of arbitrary code on a com
link jacking — A potentially unethical practice of redirecting a link to a middle-ma
site or location rather than the original site the link seemed to indicate it [illegible]
SIEM (Security Information and Event Management) — A formal proces[illegible] by whi
an organization is monitored and evaluated on a constant basis.
[illegible] — A form of phishing attack which takes place over VoIP. In this at[illegible]k, th
[illegible] toll charge expens
VoIP systems [illegible]
clickjacking — A malicious technique by which a victim is tricked into [illegible]
other screen object other than that intended by or p[illegible]
ciphertext — The unintelligible and seeming random form of data that is produ
cryptographic function of encryption. Ciphertext is produced by a symmetric al
data set is transformed by the encryption process using a selected key.
block cipher — A type of symmetric encryption algorithm that divides data int
sections and then performs the encryption or decryption operation on each b
dividing a data set into blocks enables the algorithm to encrypt data of any si
drive-by download — A type of web-based attack that automatically occurs based o
act of visiting a malicious or compromised/poisoned Web site. A drive-by download is
accomplished by taking advantage of the default nature of a Web browser to execute mobile code,
most often JavaScript, with little to no security restrictions.

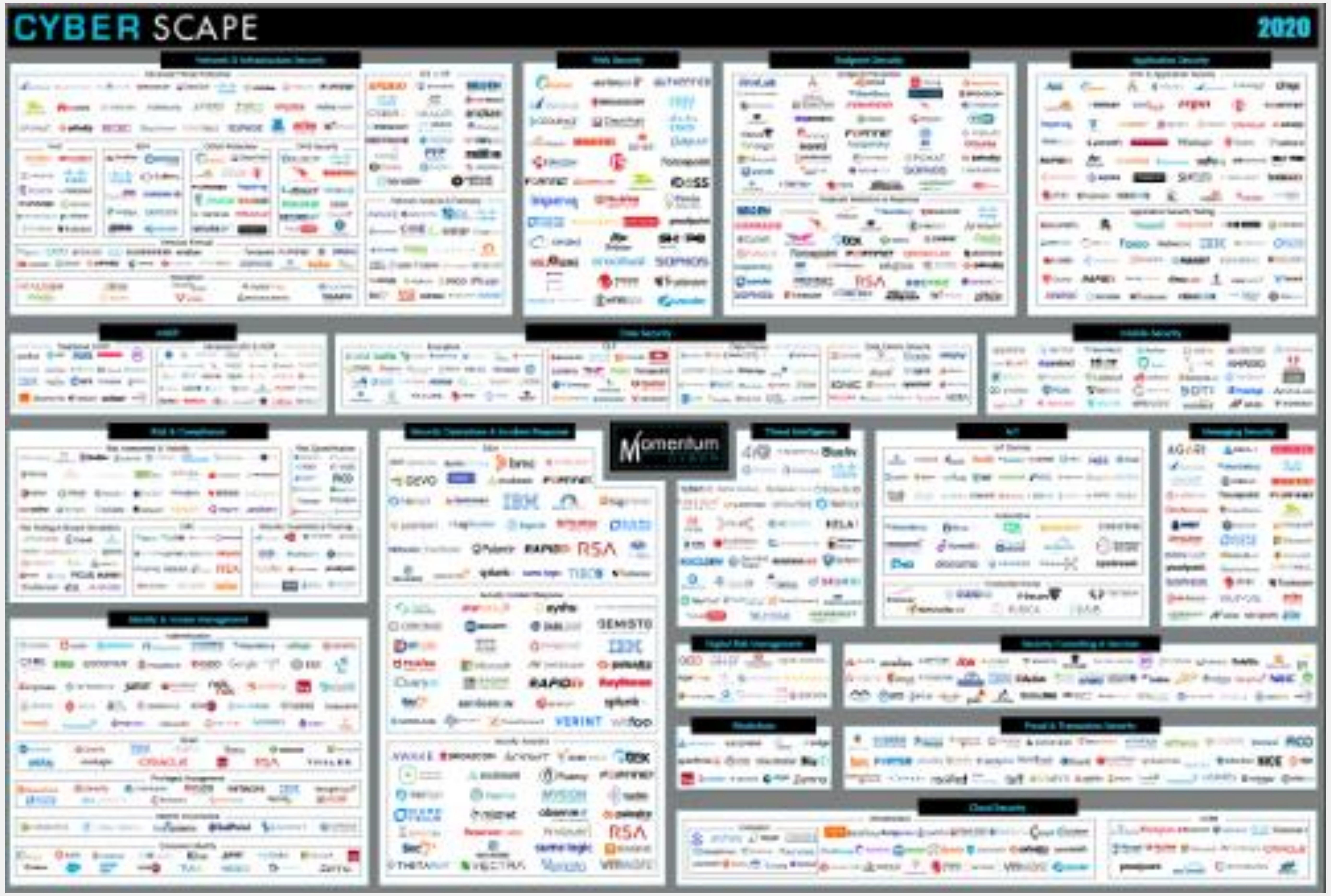


https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Decouple security solutions

Innovation Fatigue

Too many vendors offering too many solutions



Src: Momentum Partners

Enduring:

- Compliance testing difficult
- Problem-solving difficult
- Unintended consequences

Needed:

- Simple solutions
- Non-interfering

Weakest Point

Almost no one is looking backwards

A hostile attack will not come through the most recently installed high-tech equipment, it will come through old, cob-web covered, legacy devices

© Asmus Koefoed

Industry Statistics

opportunity

There are approximately 30 million wireless devices installed in industry. Half are inadequately protected from malicious attacks. Such attacks could result in significant down-time or even loss of life. Hardware-based security can stop that from happening.

30 million Wireless Industrial Devices

$1.7 billion Semicon Sales

6% CAGR

Why is Cybersecurity Important?

Successful attacks

- cause Quality Assurance failure
- cause plant shutdown
- cause potential employee injury

The problem is growing at an alarming rate

The Ideal Solution

Traits of an ideal solution:

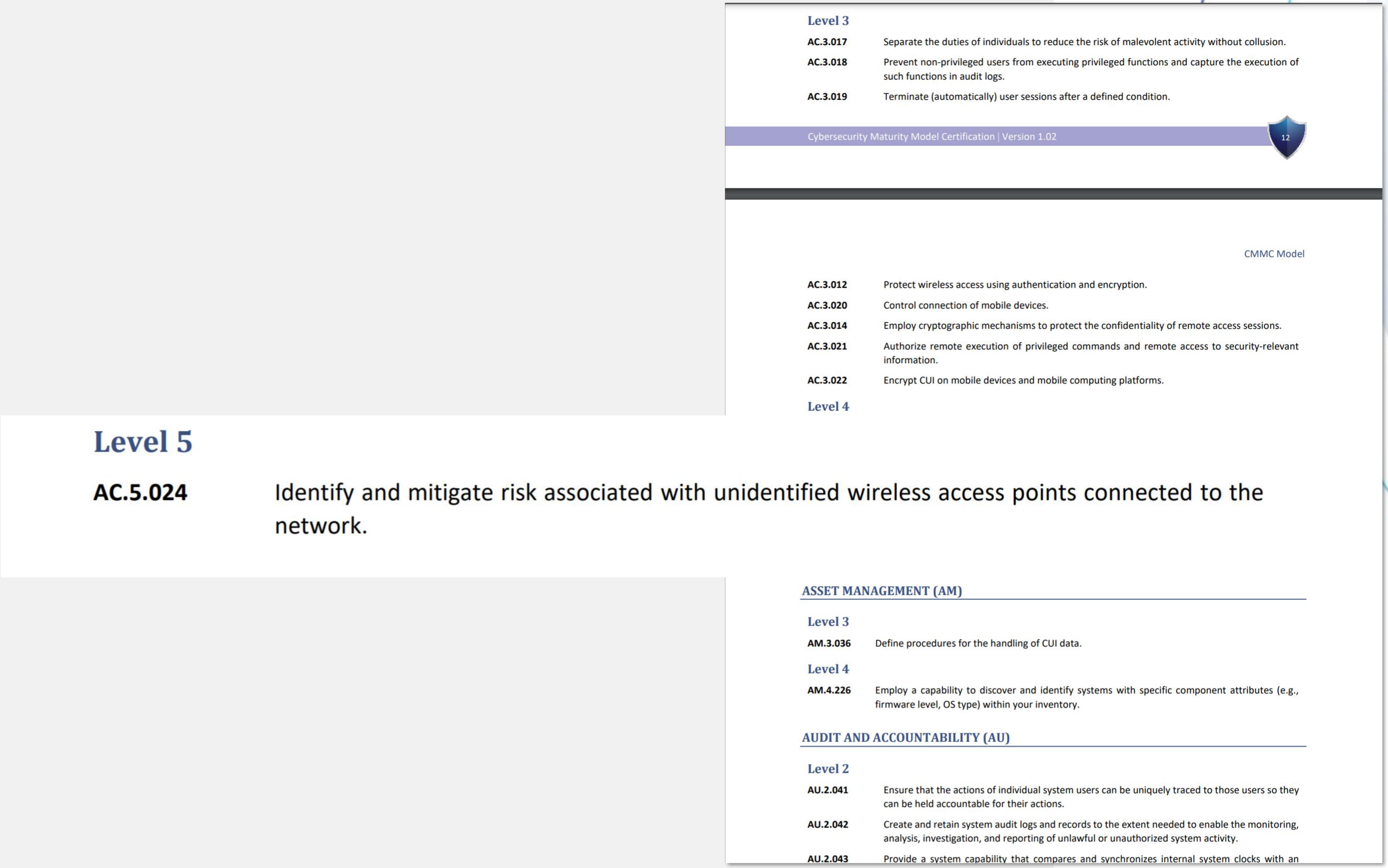
- prevents the intrusion
- is simple to implement
- is backward compatible

The Ideal Solution

Traits of an ideal solution:

- prevents the intrusion
- is simple to implement
- is backward compatible
- *is protocol agnostic*
- *takes us to the highest level of security*

Level 5 of CMMC



Level 3

AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

AC.3.019 Terminate (automatically) user sessions after a defined condition.

AC.3.012 Protect wireless access using authentication and encryption.

AC.3.020 Control connection of mobile devices.

AC.3.014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information.

AC.3.022 Encrypt CUI on mobile devices and mobile computing platforms.

Level 4

Level 5

AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network.

ASSET MANAGEMENT (AM)

Level 3

AM.3.036 Define procedures for the handling of CUI data.

Level 4

AM.4.226 Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.

AUDIT AND ACCOUNTABILITY (AU)

Level 2

AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

AU.2.043 Provide a system capability that compares and synchronizes internal system clocks with an

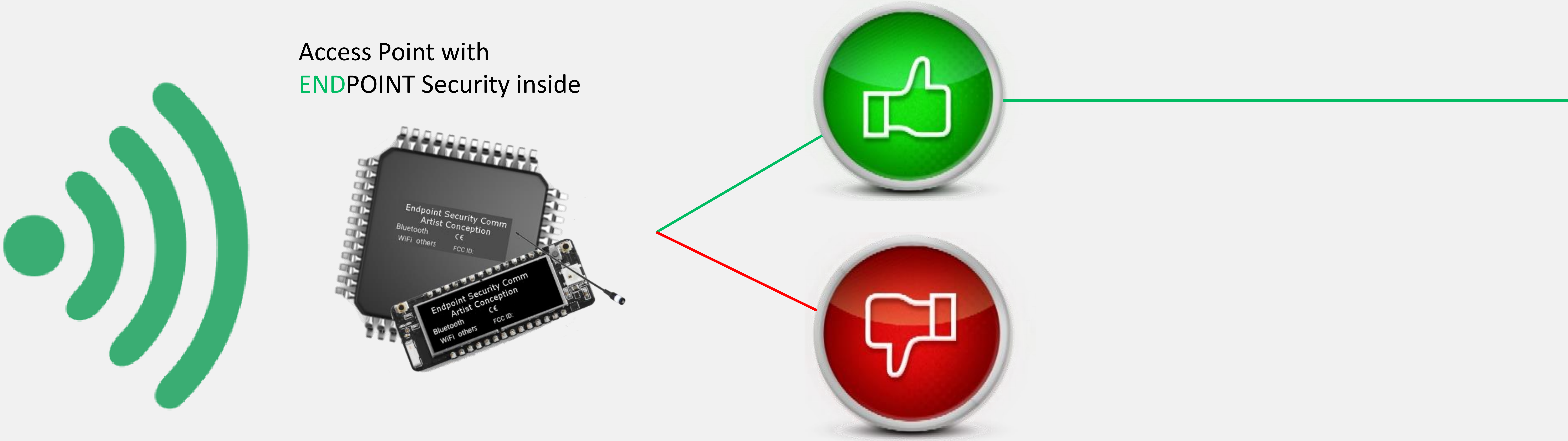
Sample Requirements

IEC 62443-4-2 Component Identification and Authentication Control

Feature	SL1	SL2	SL3	SL4
Identify and authenticate human users	X	X	X	X
Component shall enable the management of accounts	X	X	X	X
Component shall support the management of identifiers	X	X	X	X
Component shall support authenticator management	X	X	X	X
Password based authentication with defined password strength	X	X	X	X
Obscure authentication feedback during authentication process	X	X	X	X
Enforce unsuccessful login attempt limit, lock account	X	X	X	X
Provide warning message to individuals attempting to access the system	X	X	X	X
Uniquely identify and authenticate all human users		X	X	X
Software process and device identification and authentication		X	X	X
When PKI is used, the component shall integrate with PKI infrastructure		X	X	X
When PKI is used, the component shall check validity of certificates		X	X	X
Support for symmetric key based authentication		X	X	X
Unique software process and device identification and authentication			X	X
Authenticators shall be protected by hardware mechanisms			X	X
Prevent password reuse for configurable number of generations human users			X	X
Protection of public key via hardware			X	X
Protection of symmetric key data via hardware			X	X
Multifactor authentication for all interfaces				X
Prevent password reuse for configurable number of generations software process or device				X

The Solution

ENDPOINT provides an answer. Recognize authorized devices by their own, natural biometric fingerprint; found in the RF signal.

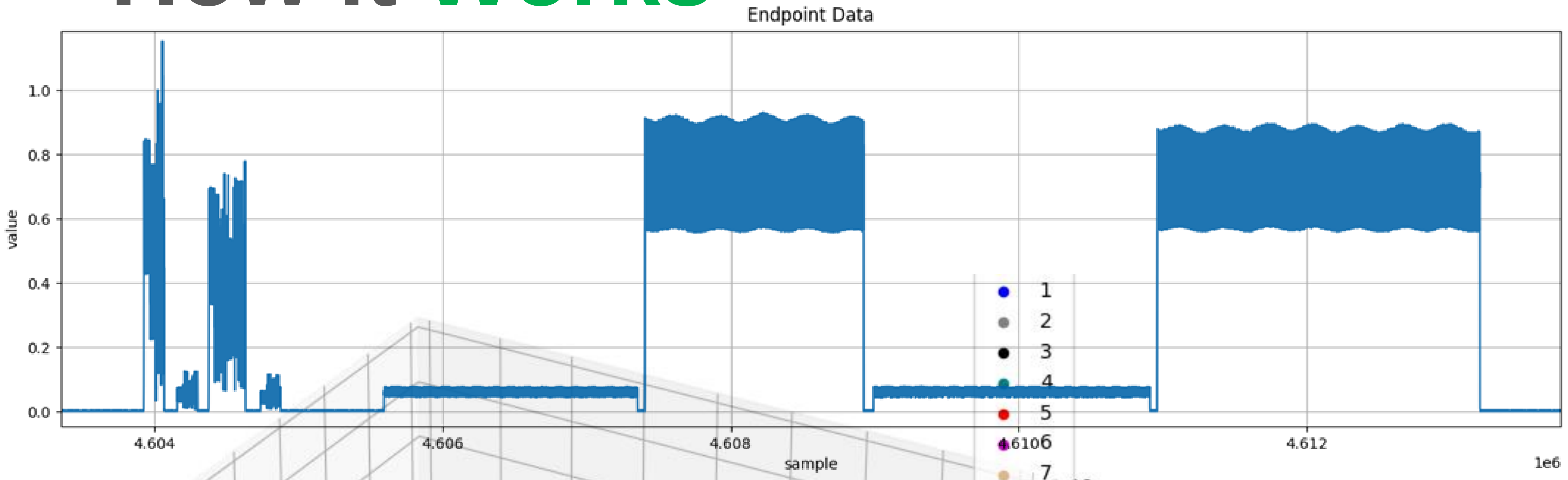


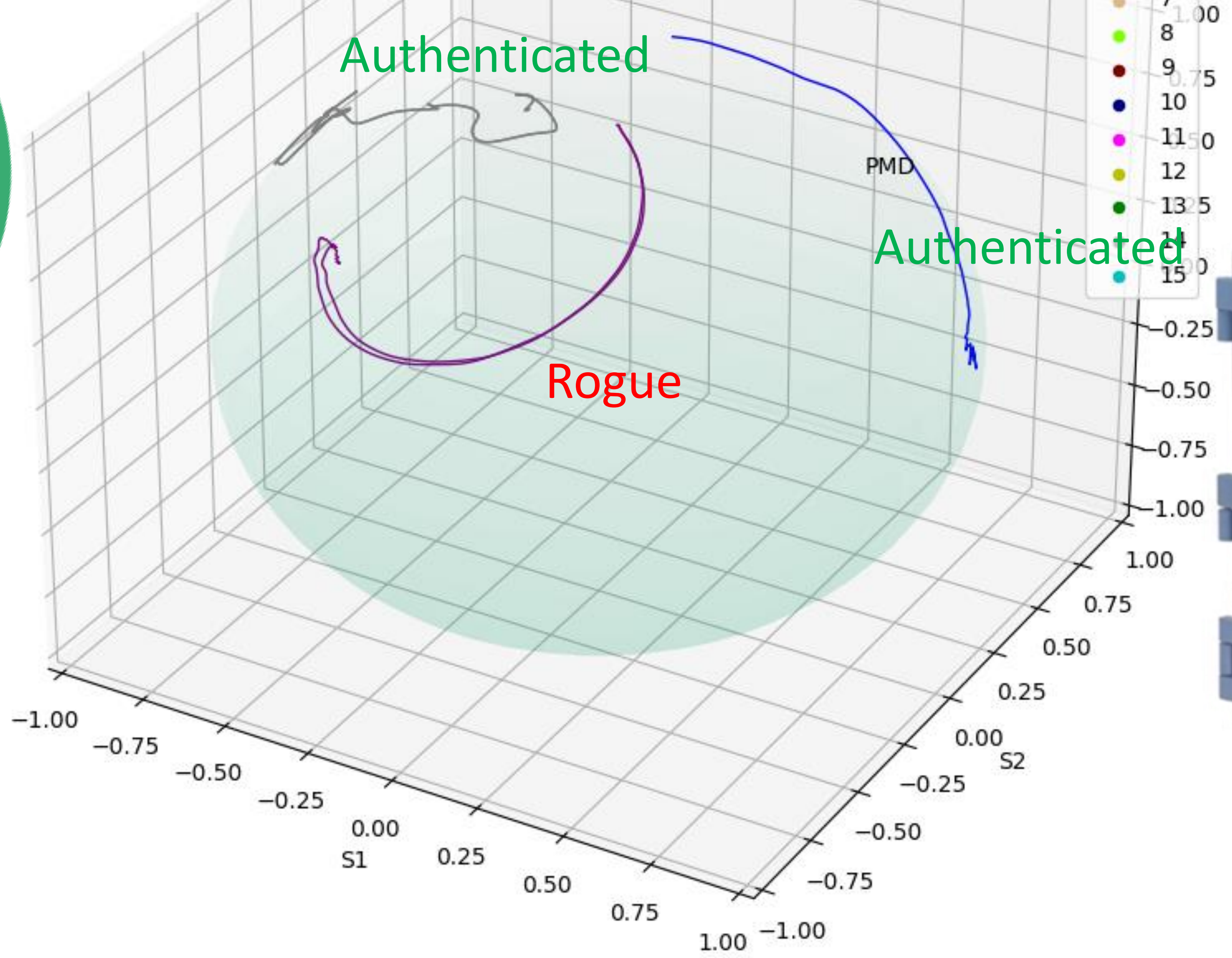
Access Point with
ENDPOINT Security inside

ENDPOINT The solution is protected with 9 patents and applications

How it Works

Camera monitoring
your process

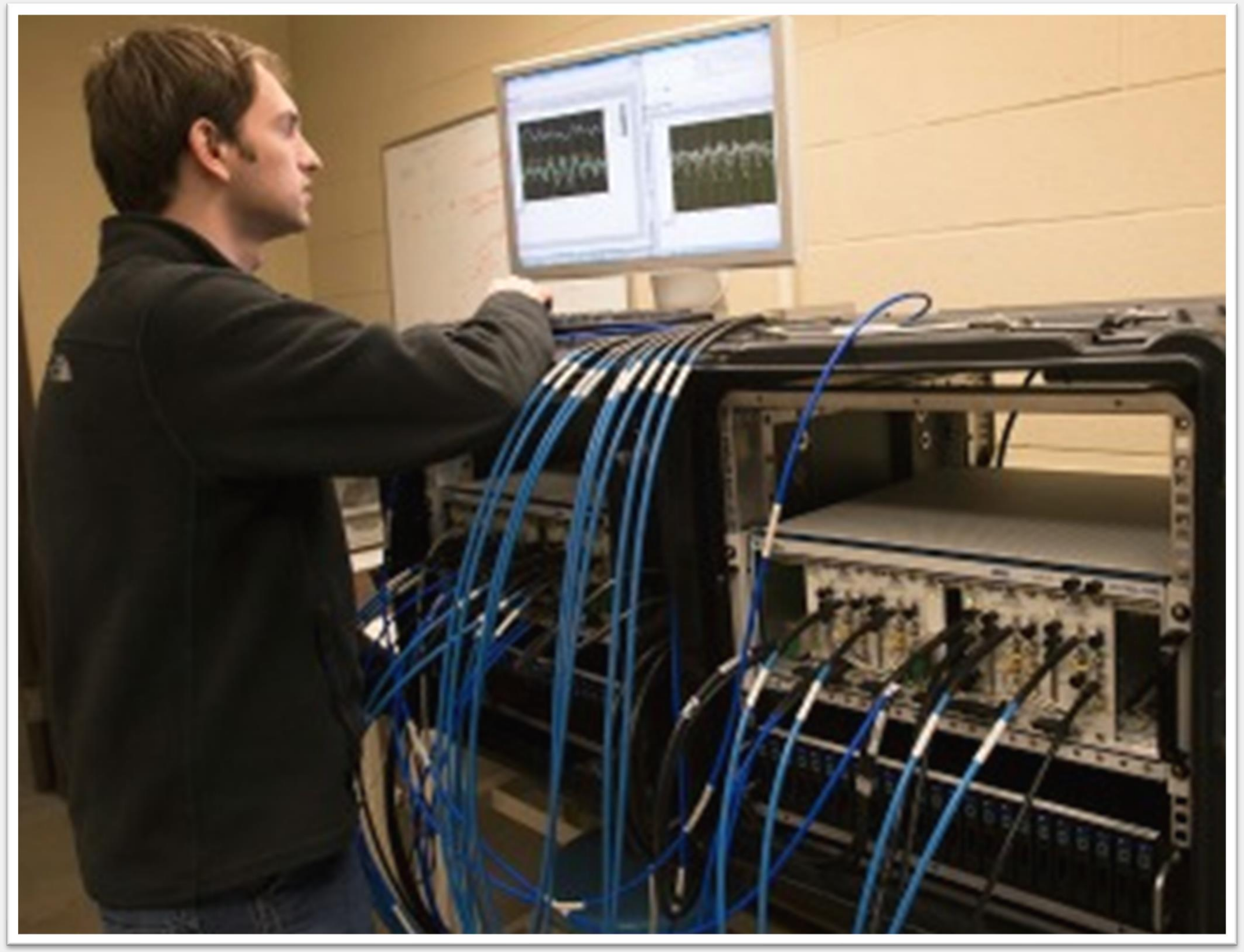




Access point

Authenticated sources are identified

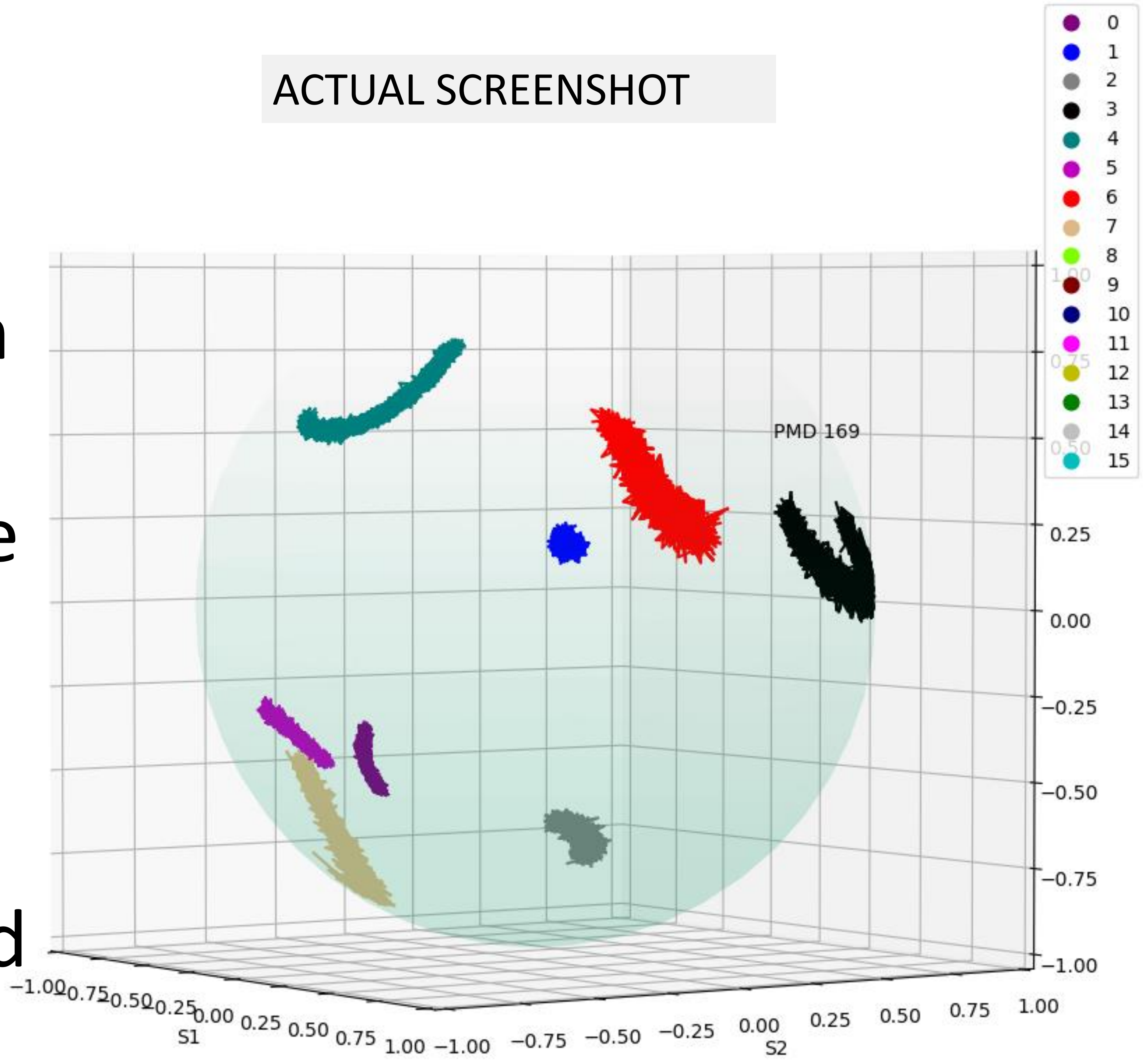
Notre Dame Laboratory



Two dual-pole antenna receivers monitoring 10 transmitting devices

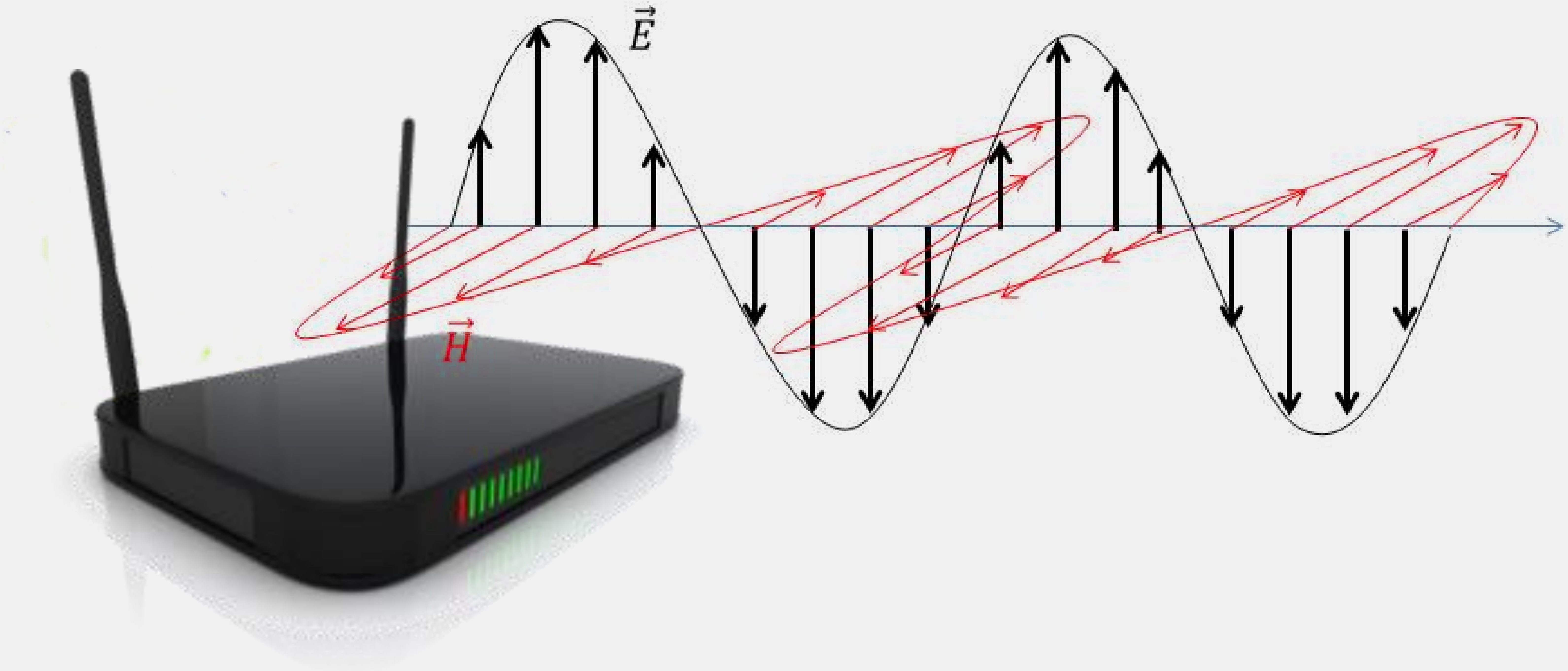
More on Signal Fingerprints

Here 8 devices each send 200 signals to an access point. The fingerprints are overlayed. One can see they can be clearly distinguished from one another.



ACTUAL SCREENSHOT

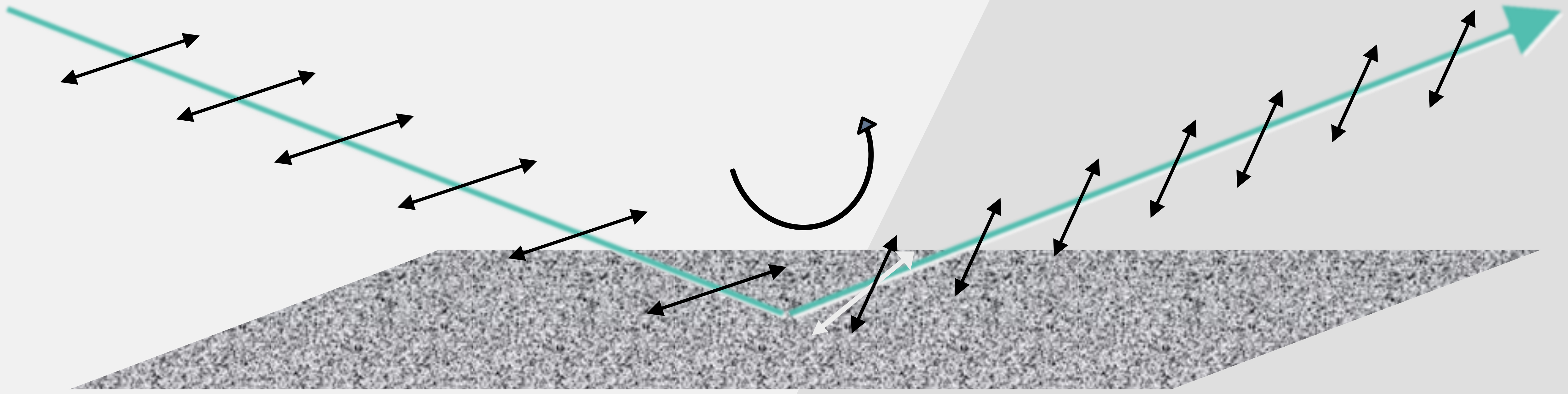
Background



The wireless signals will typically be transmitted with horizontal or vertical polarization; which can come, for example, from pole antennas like we are used to seeing on our routers at home.

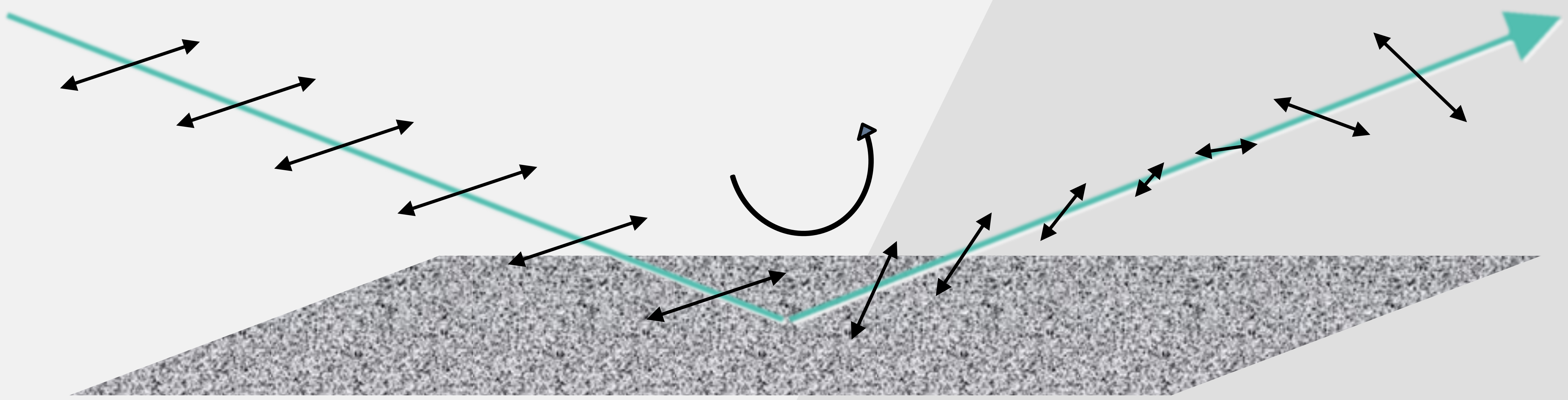
Antennas transmit polarized signals

Principle of Operation



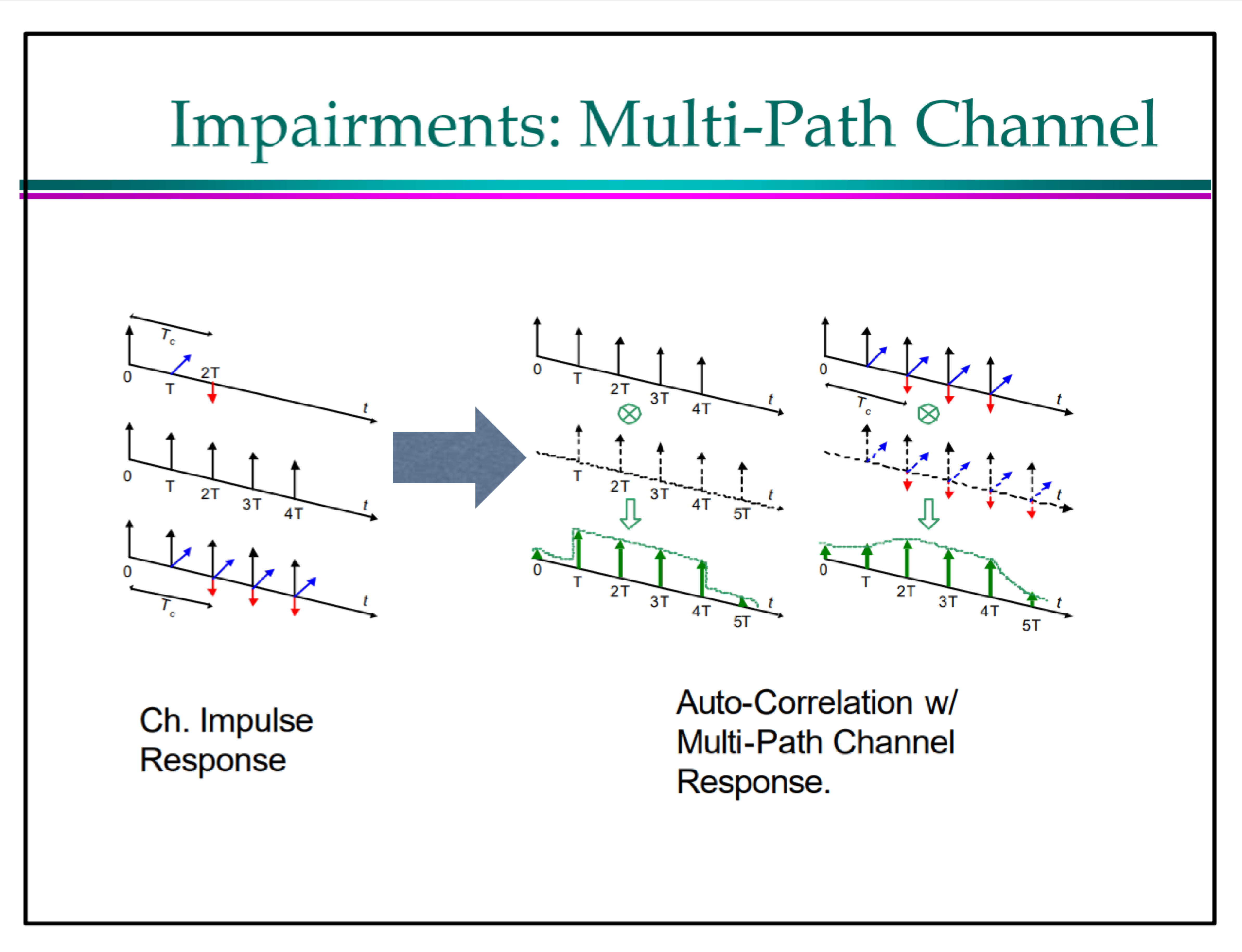
Polarization of a signal changes as it reflects off of surfaces

Principle of Operation



Polarization of a signal changes as it reflects off of surfaces

Polarization Mode Dispersion



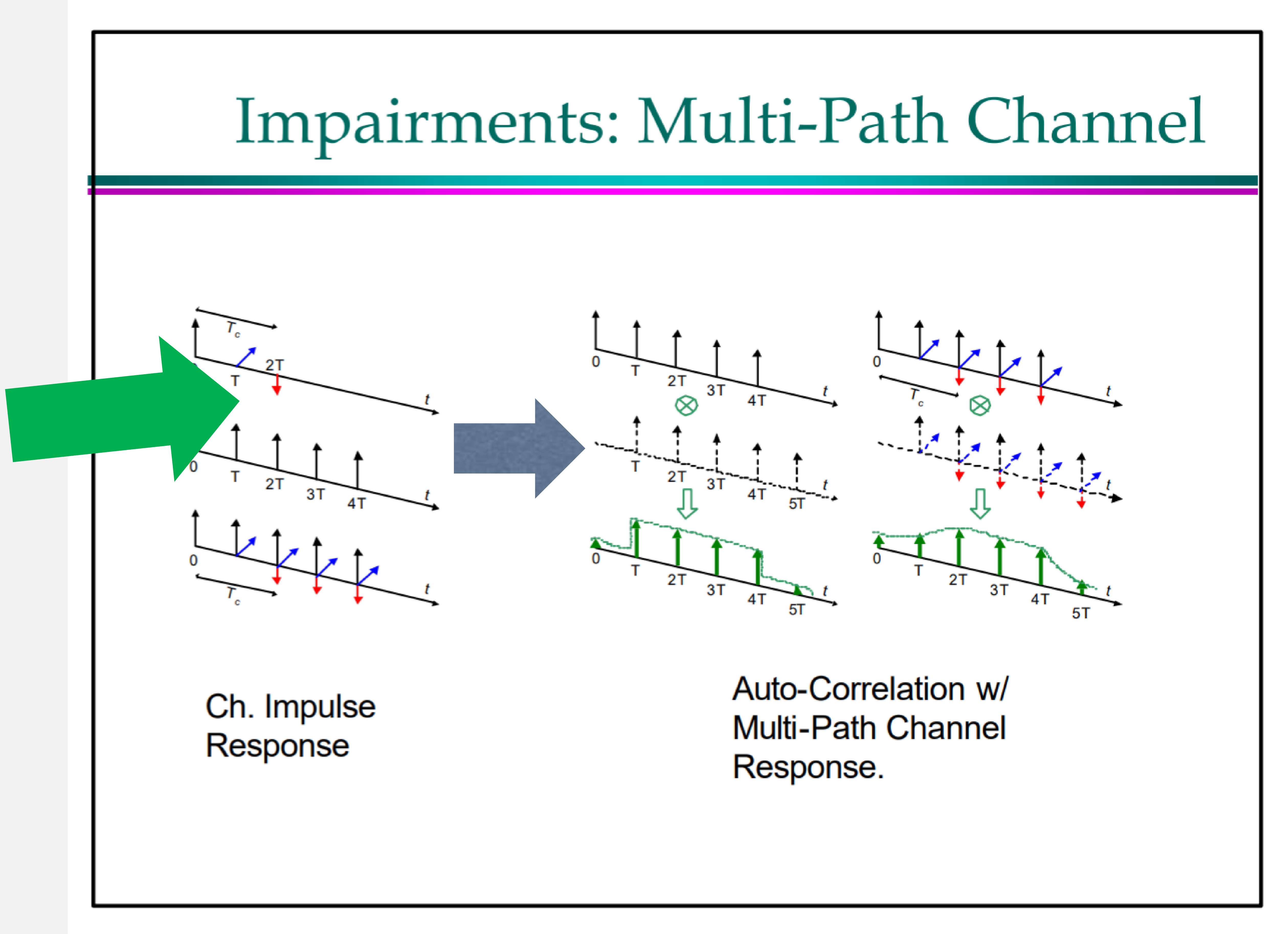
Impairments: Multi-Path Channel

Ch. Impulse Response

Auto-Correlation w/ Multi-Path Channel Response.

Berkeley EE225C Lecture Notes

Polarization Mode Dispersion



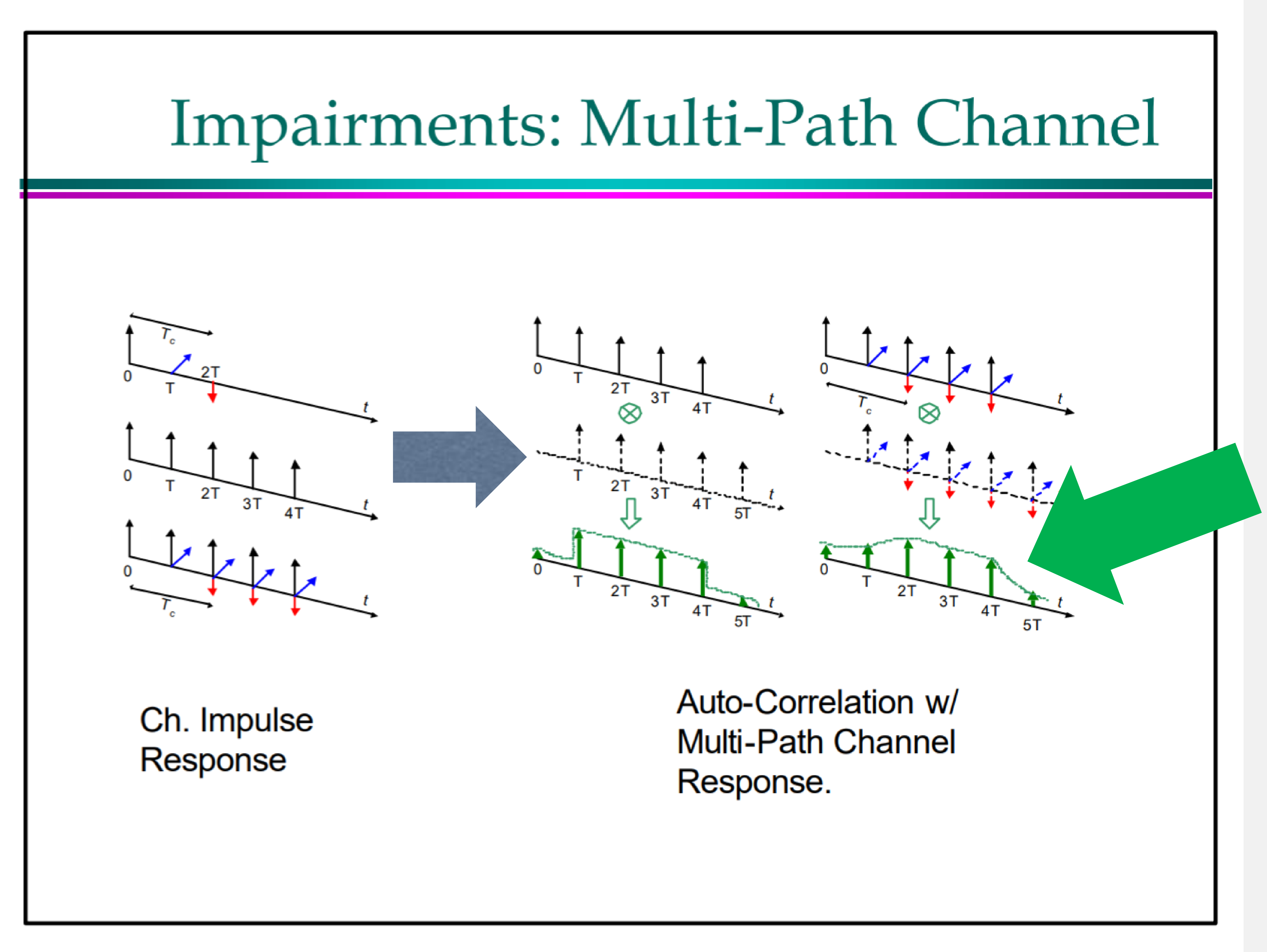
Impairments: Multi-Path Channel

Ch. Impulse Response

Auto-Correlation w/ Multi-Path Channel Response.

Berkeley EE225C Lecture Notes

Polarization Mode Dispersion



Impairments: Multi-Path Channel

Ch. Impulse Response

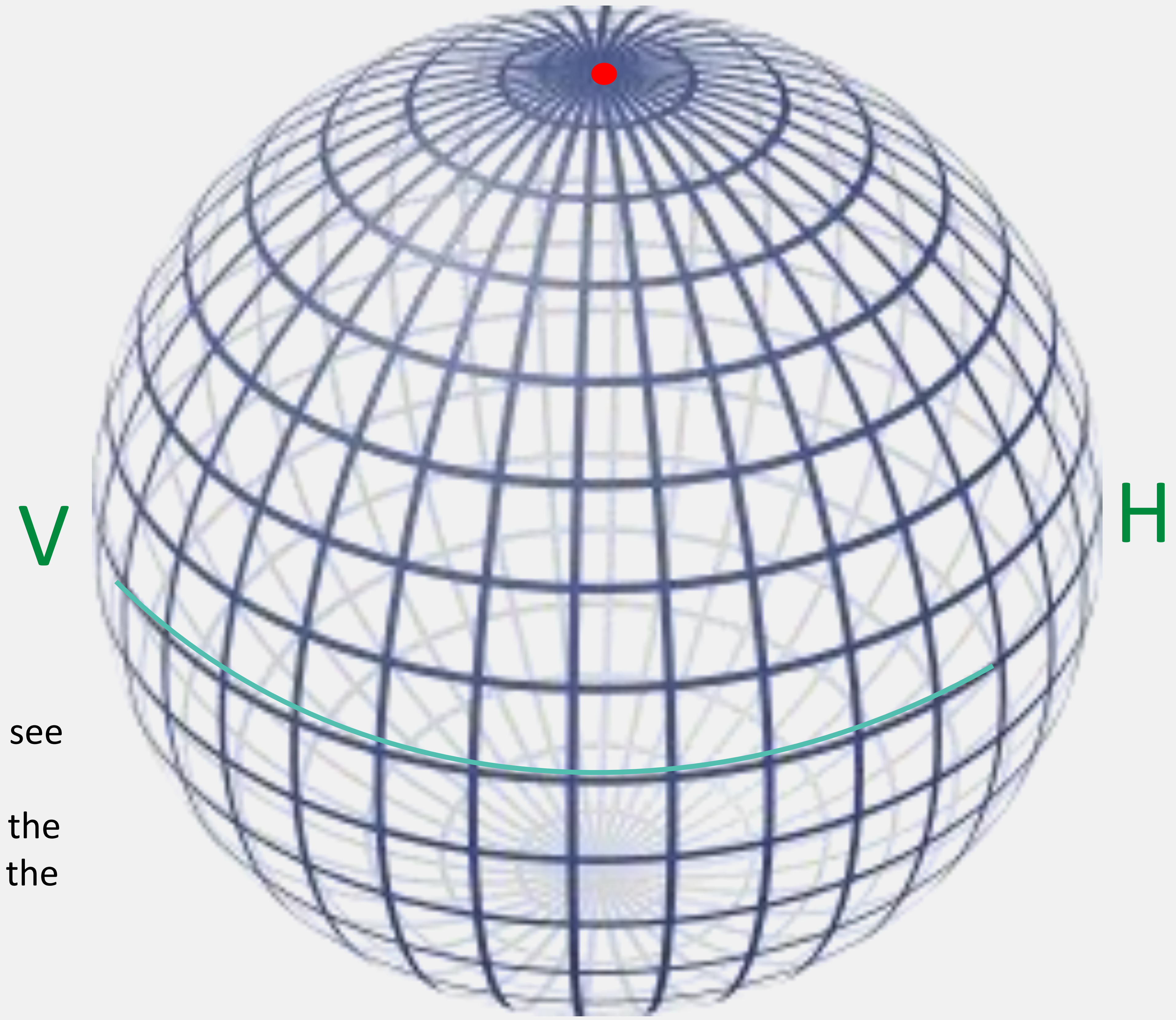
Auto-Correlation w/ Multi-Path Channel Response.

Berkeley EE225C Lecture Notes

Background

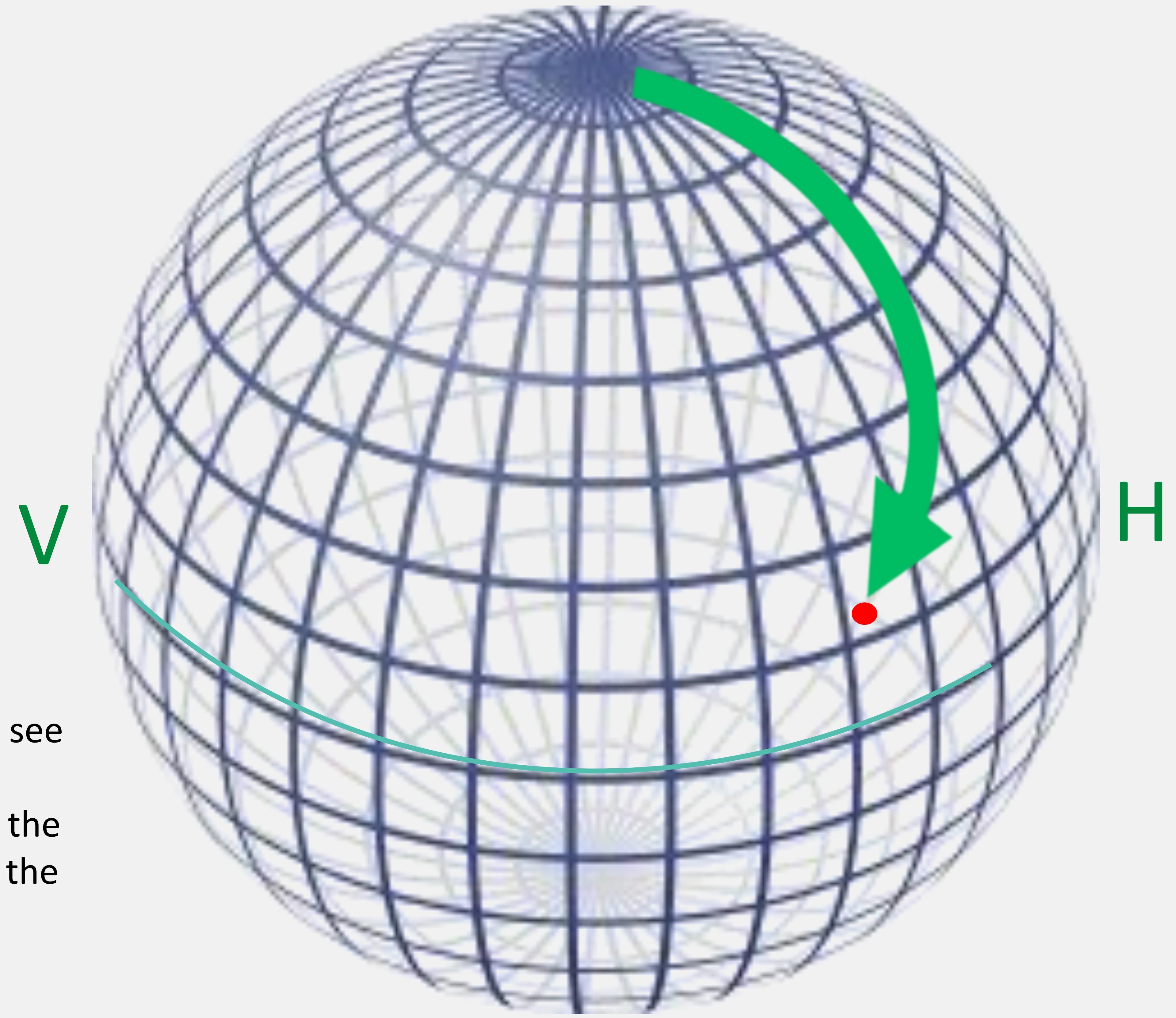
Poincaré Sphere

If a transmitted narrowband signal is received without any impairments, we would expect to see a point on the sphere; for example at the north pole if the antenna is emitting a left-hand polarized signal. However, in a channel where the signal reflects off of one or more surfaces, the received signal will exhibit modified signal polarization behavior. We might ideally show that the dot has moved from the pole because channel effects have modified the polarization state.



Background

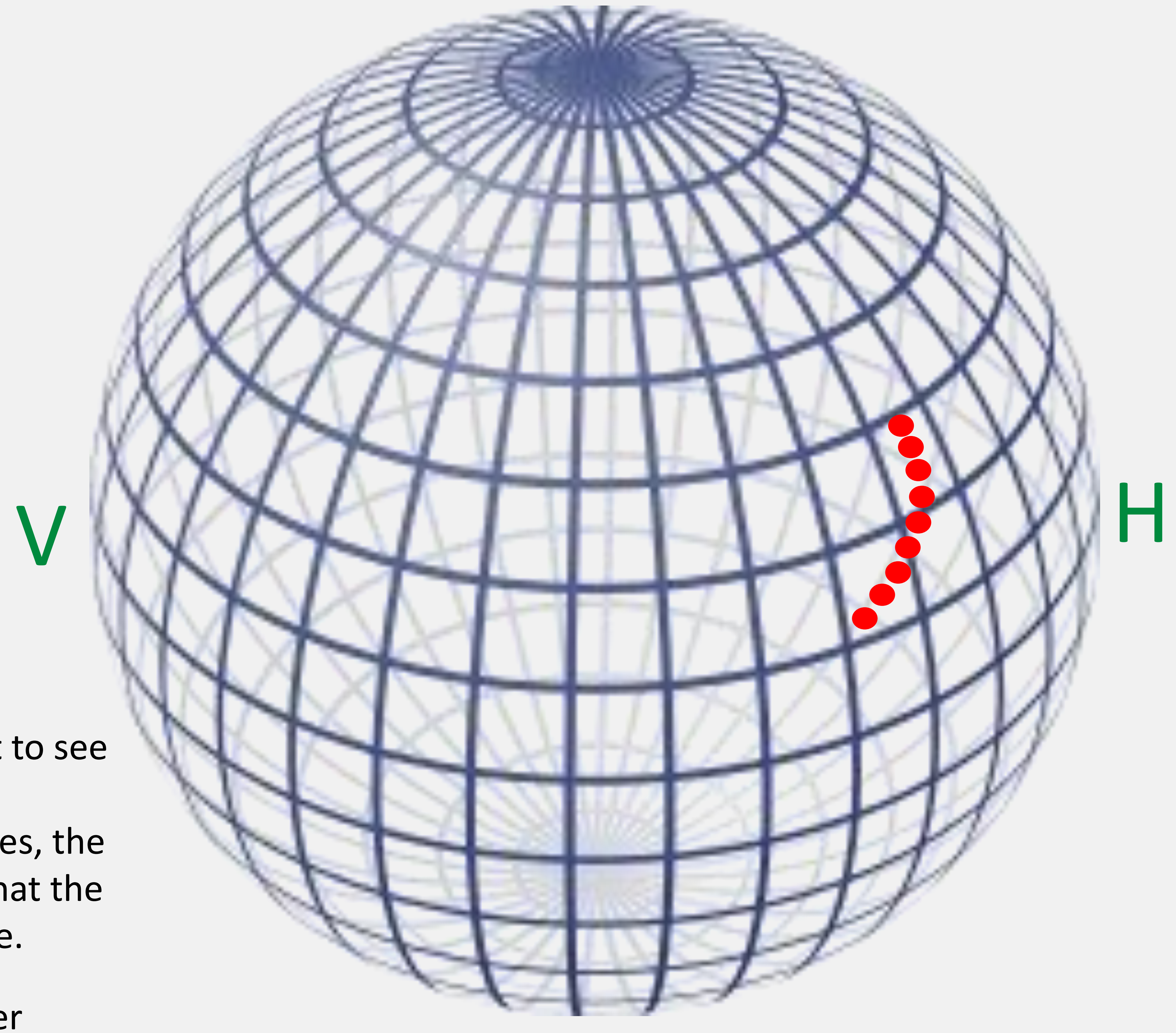
Poincaré Sphere



If a transmitted narrowband signal is received without any impairments, we would expect to see a point on the sphere; for example at the north pole if the antenna is emitting a left-hand polarized signal. However, in a channel where the signal reflects off of one or more surfaces, the received signal will exhibit modified signal polarization behavior. We might ideally show that the dot has moved from the pole because channel effects have modified the polarization state.

Background

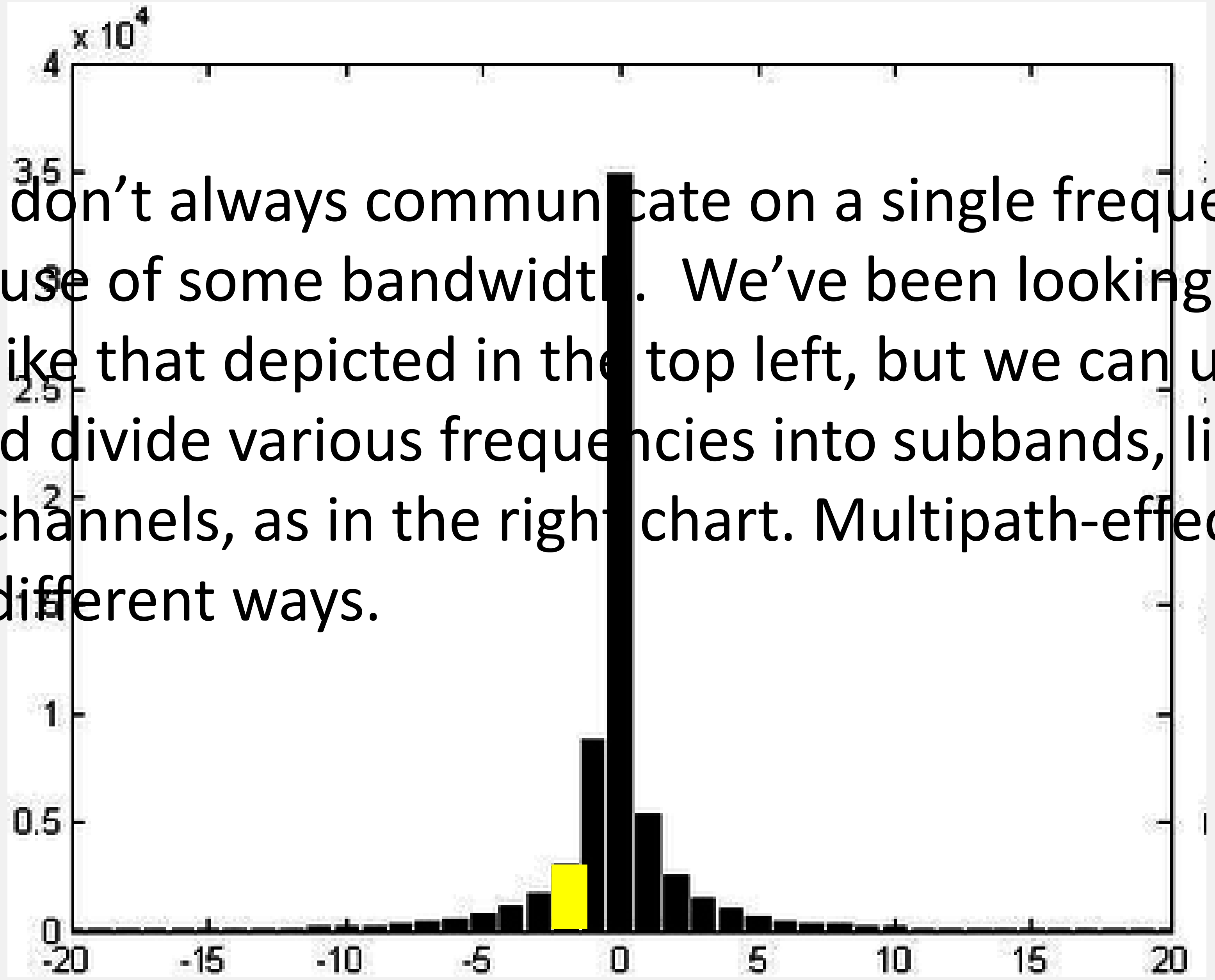
Poincaré Sphere



If a transmitted narrowband signal is received without any impairments, we would expect to see a point on the sphere; for example at the north pole if the antenna is emitting a left-hand polarized signal. However, in a channel where the signal reflects off of one or more surfaces, the received signal will exhibit modified signal polarization behavior. We might ideally show that the dot has moved from the pole because channel effects have modified the polarization state.

In reality, signals are comprised of multiple frequencies. Wide-band signals are spread over many frequencies, in fact. Different frequencies are modified differently in their polarization characteristics.

Of course, we don’t always communicate on a single frequency, but instead make use of some bandwidth. We’ve been looking at narrow-band signals, like that depicted in the top left, but we can use a wider bandwidth and divide various frequencies into subbands, like the lower left, defining channels, as in the right chart. Multipath-effects impact dispersion in different ways.



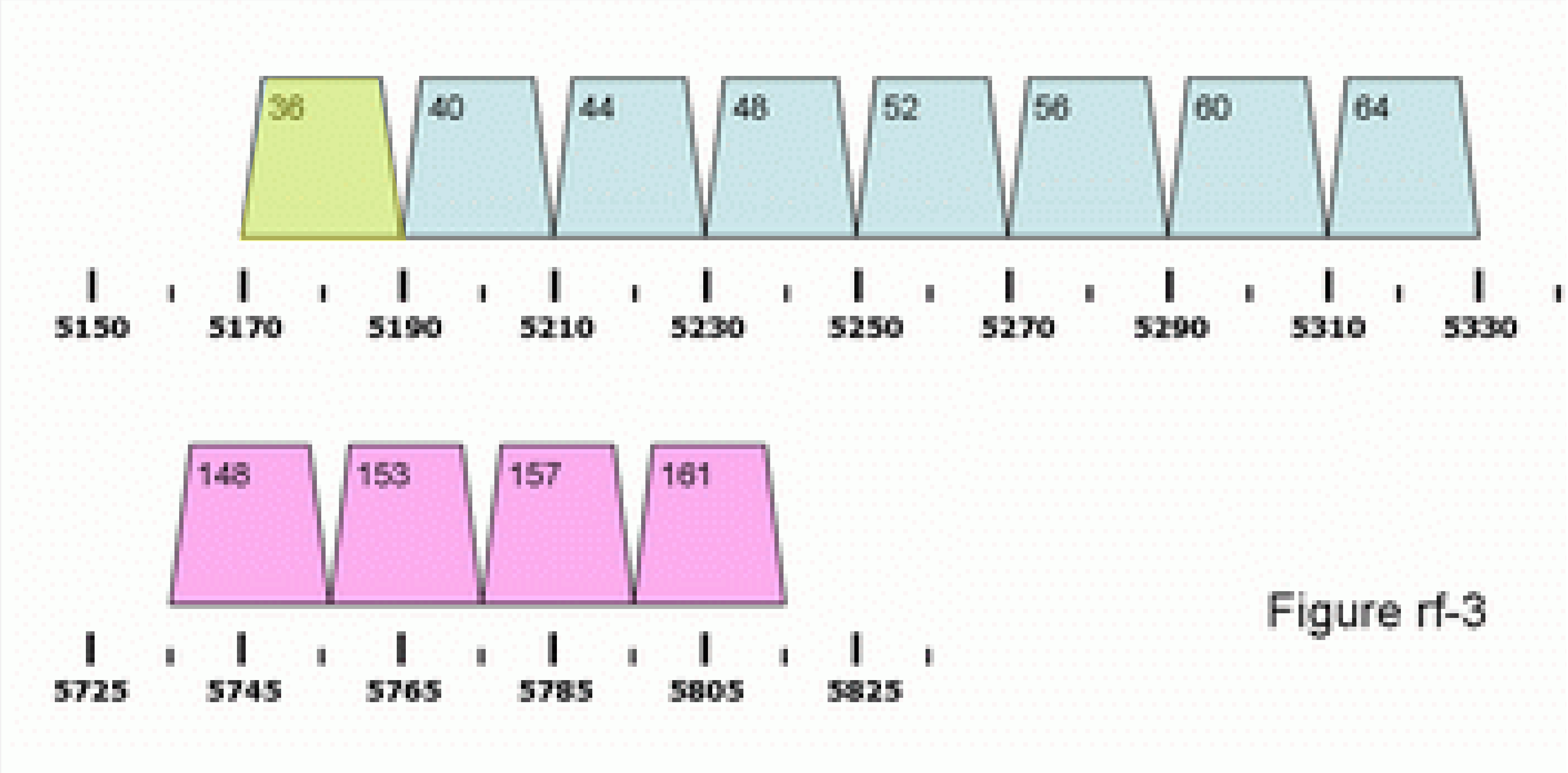
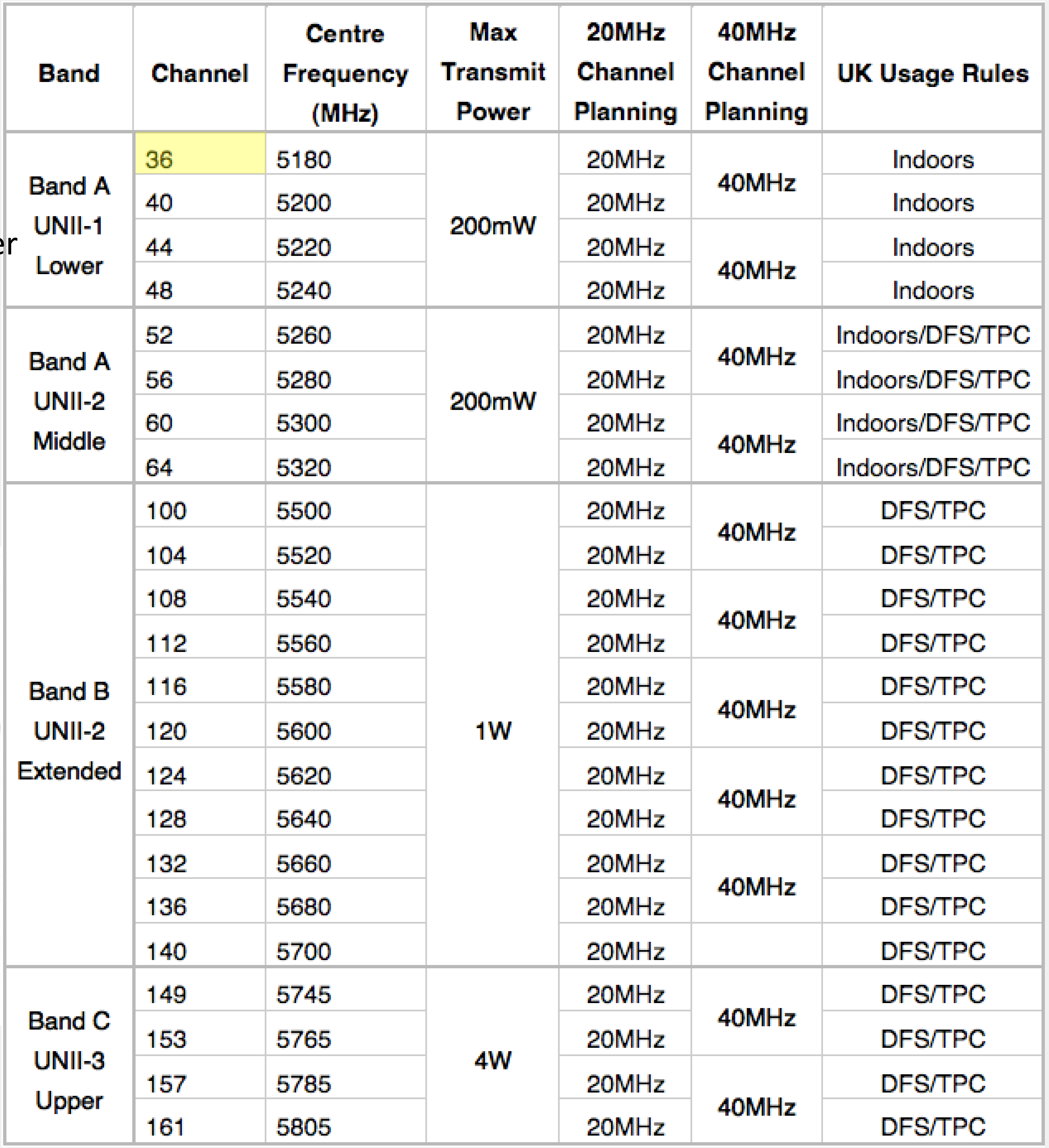
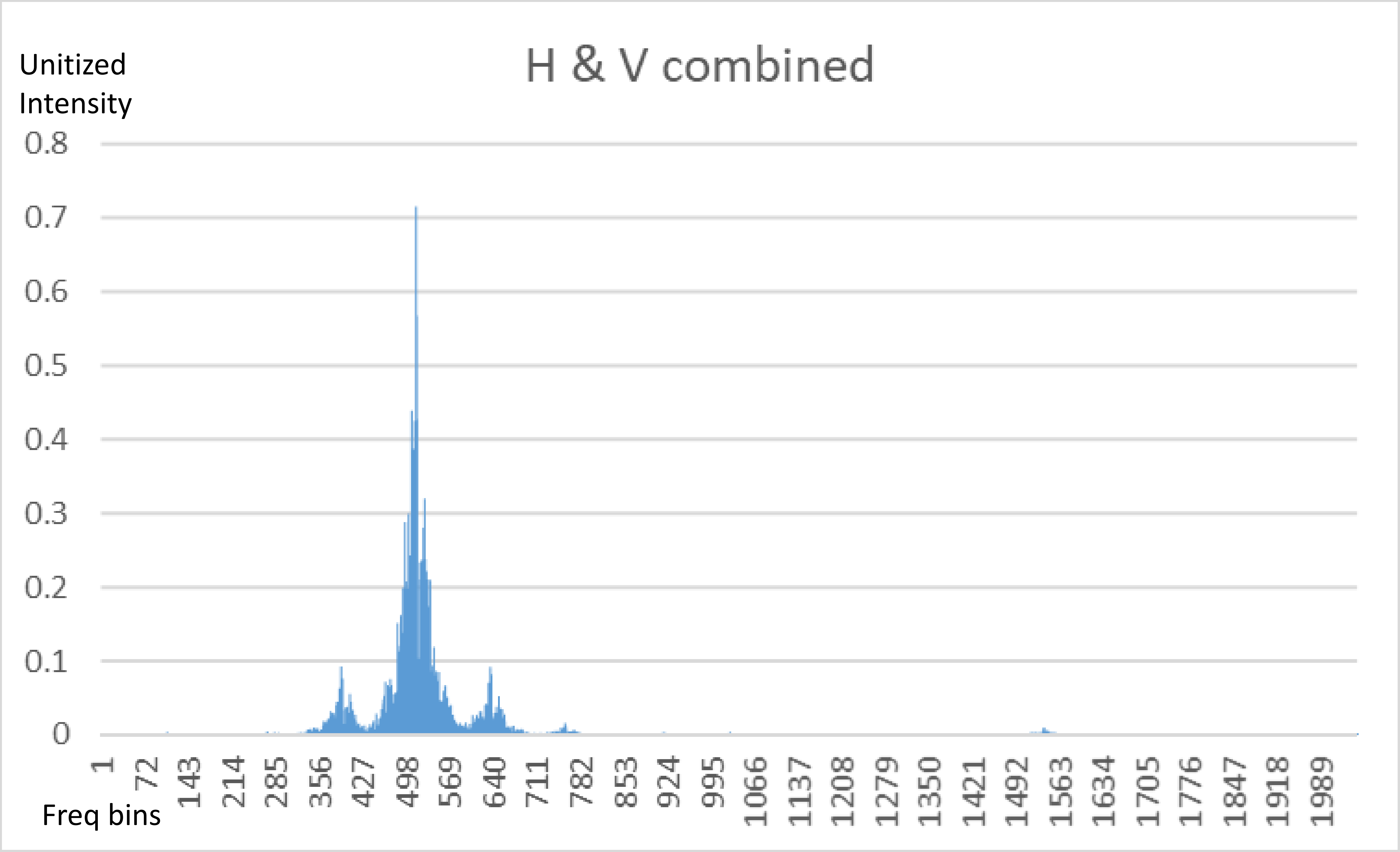


Figure rf-3

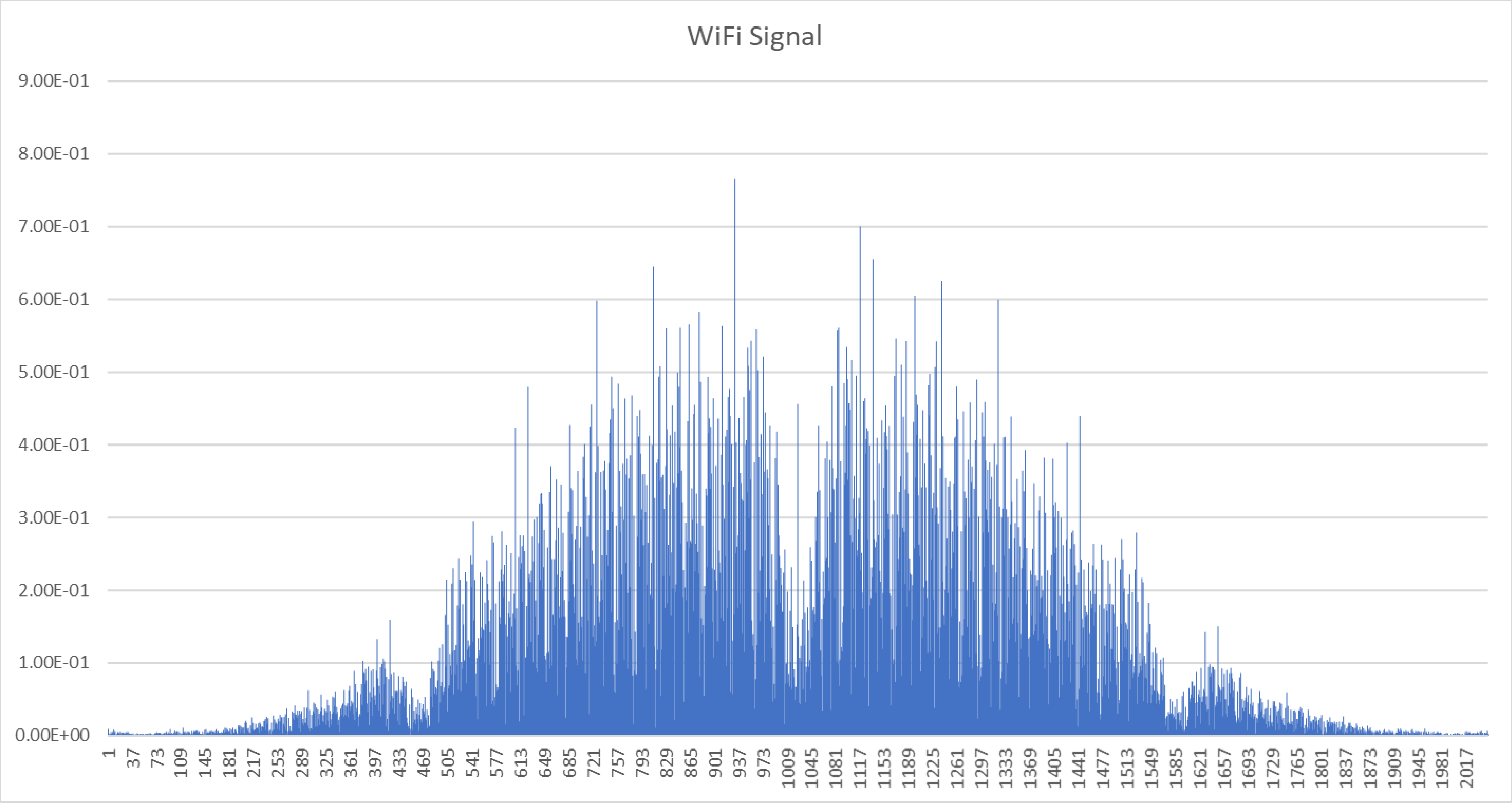


Band	Channel	Centre Frequency (MHz)	Max Transmit Power	20MHz Channel Planning	40MHz Channel Planning	UK Usage Rules
Band A UNII-1 Lower	36	5180	200mW	20MHz	40MHz	Indoors
	40	5200		20MHz		Indoors
	44	5220		20MHz	40MHz	Indoors
	48	5240		20MHz		Indoors
Band A UNII-2 Middle	52	5260	200mW	20MHz	40MHz	Indoors/DFS/TPC
	56	5280		20MHz		Indoors/DFS/TPC
	60	5300		20MHz	40MHz	Indoors/DFS/TPC
	64	5320		20MHz		Indoors/DFS/TPC
Band B UNII-2 Extended	100	5500	1W	20MHz	40MHz	DFS/TPC
	104	5520		20MHz		DFS/TPC
	108	5540		20MHz	40MHz	DFS/TPC
	112	5560		20MHz		DFS/TPC
	116	5580		20MHz	40MHz	DFS/TPC
	120	5600		20MHz		DFS/TPC
	124	5620		20MHz	40MHz	DFS/TPC
	128	5640		20MHz		DFS/TPC
	132	5660		20MHz	40MHz	DFS/TPC
	136	5680		20MHz		DFS/TPC
	140	5700		20MHz		DFS/TPC
Band C UNII-3 Upper	149	5745	4W	20MHz	40MHz	DFS/TPC
	153	5765		20MHz		DFS/TPC
	157	5785		20MHz	40MHz	DFS/TPC
	161	5805		20MHz		DFS/TPC

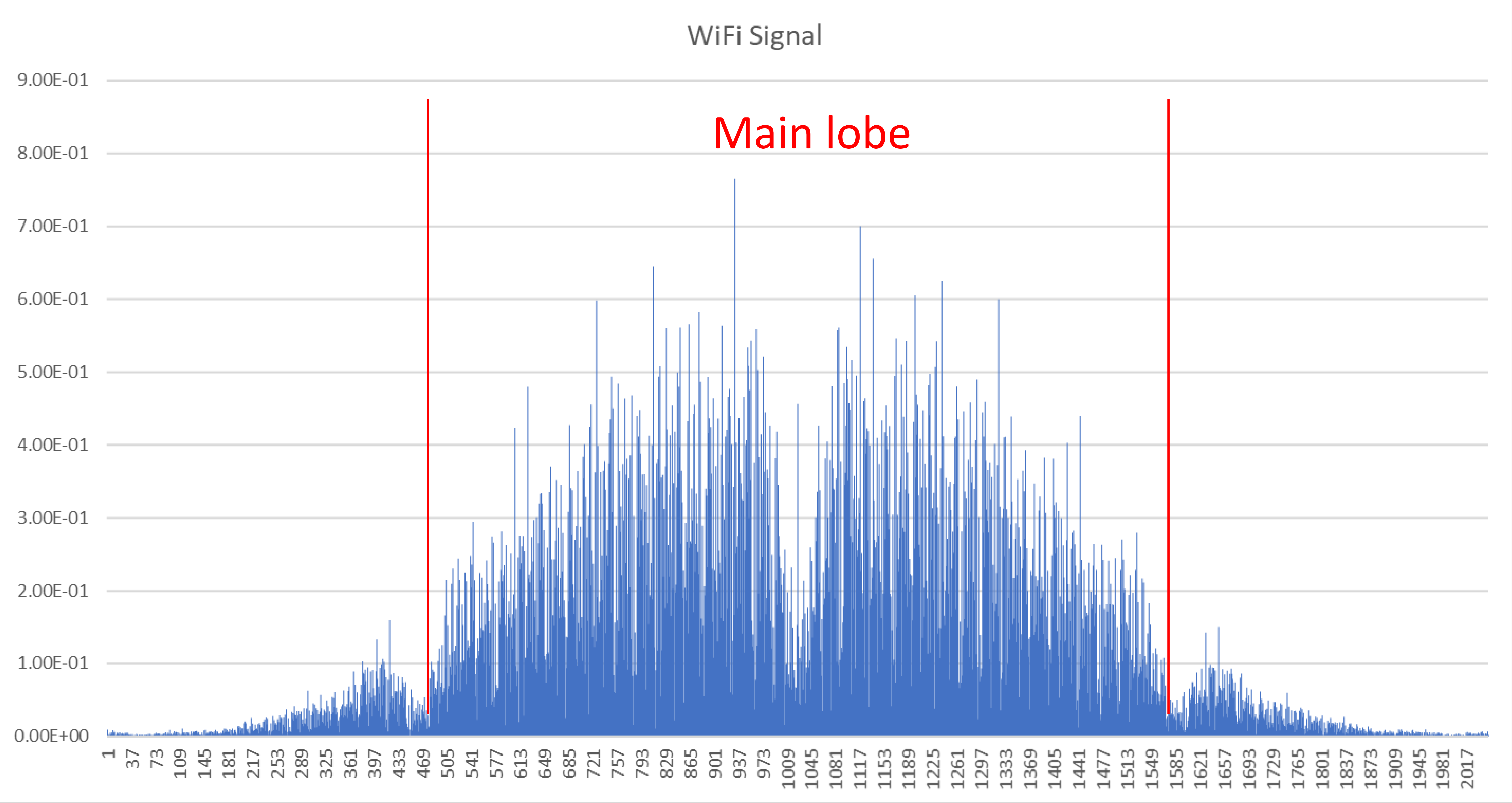
Bluetooth


H & V combined
Unitized Intensity
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1
72
143
214
285
356
427
498
569
640
711
782
853
924
995
1066
1137
1208
1279
1350
1421
1492
1563
1634
1705
1776
1847
1918
1989
Freq bins

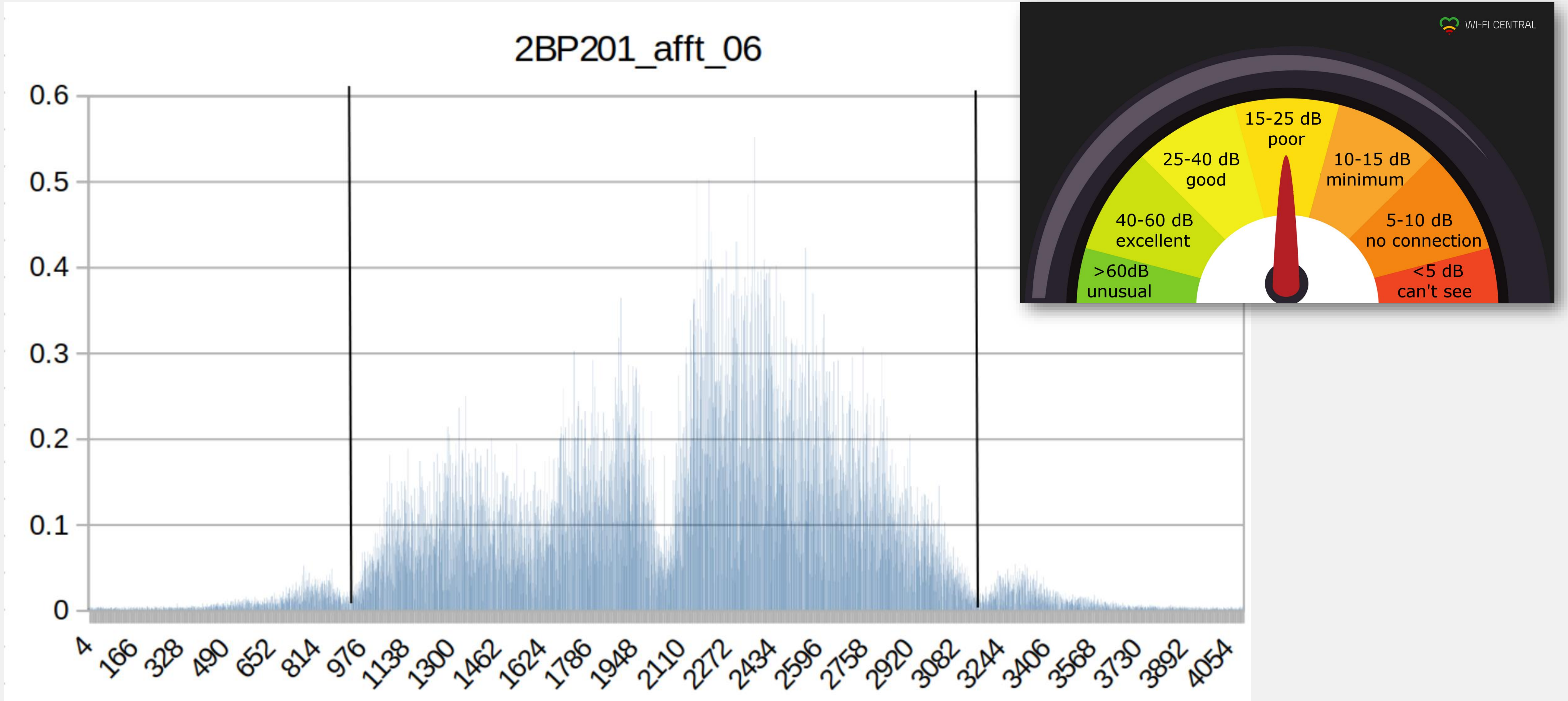
Frequency Domain



Frequency Domain



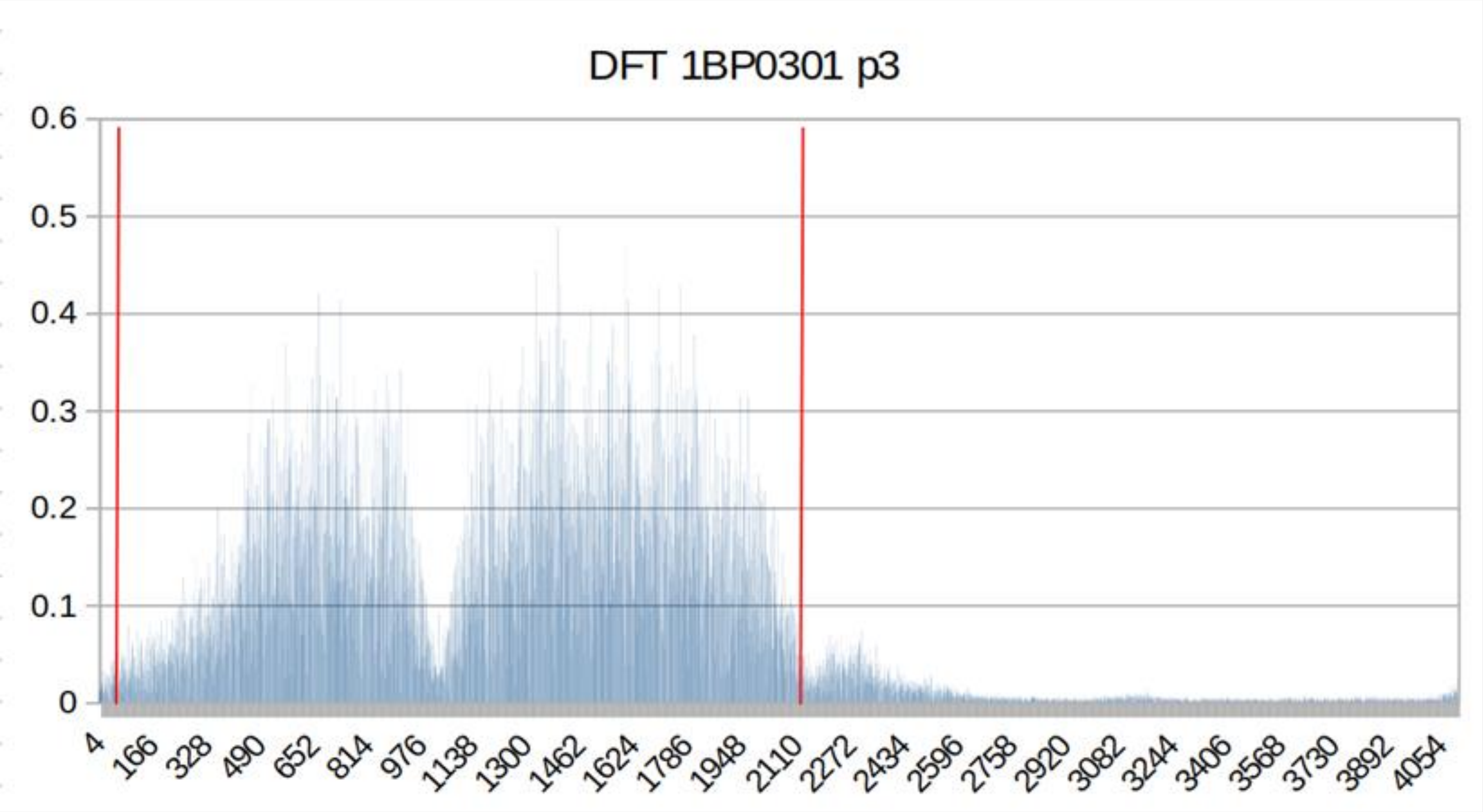
DFT Trimmed to Main Lobe

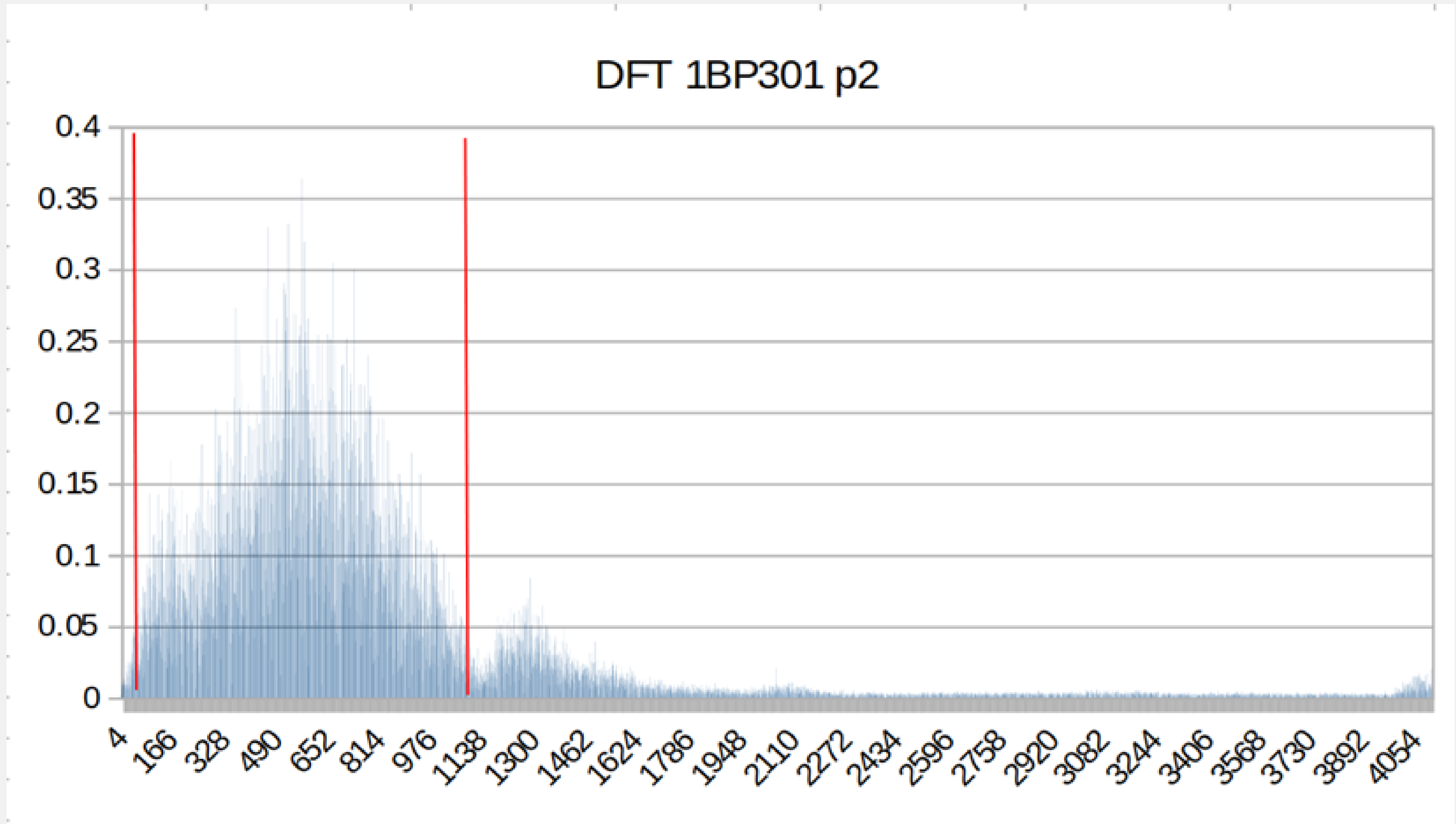


See ICDT paper: Wireless Frequency Data Manipulation for Embedded Databases used in Cybersecurity Applications

A poor signal is captured and its main lobe found.

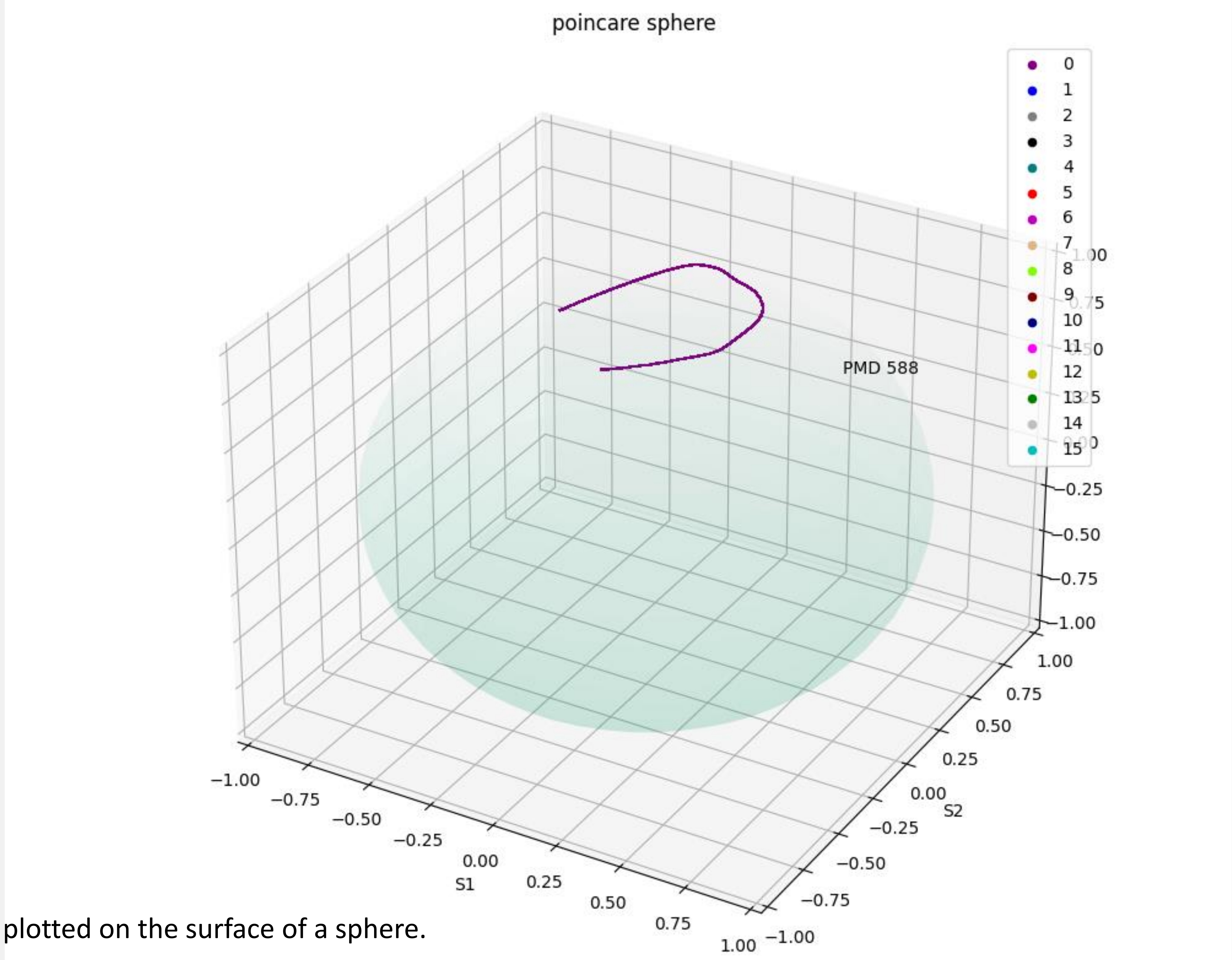
DFTs Off-Center





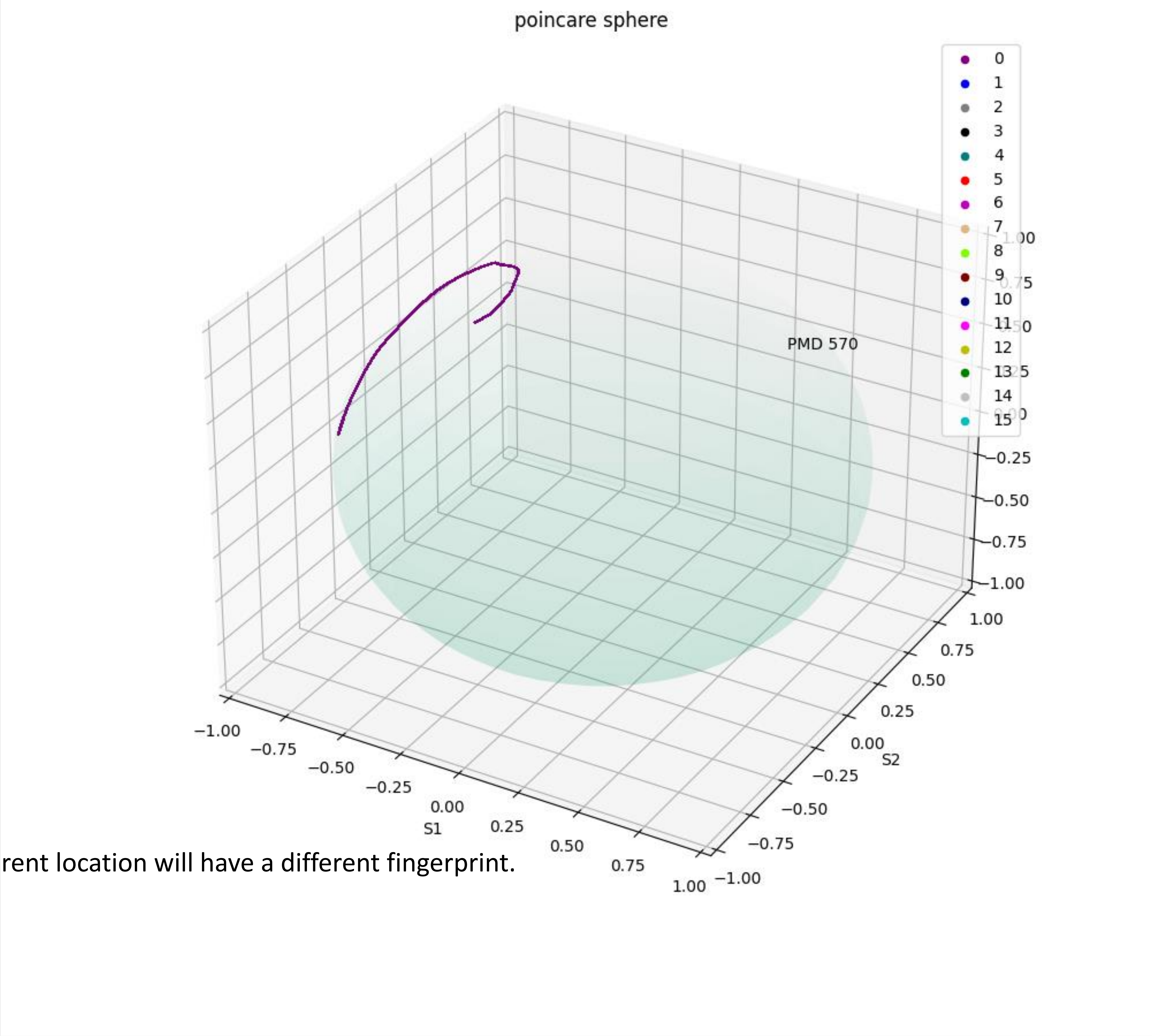
One must consider that the received signal may not be centered on the center frequency of the receiver when it is captured. For instance, the DFT on the left seems to be on WiFi channel 9 in this particular case where the receiver was centered on channel 10. On the right is likely one on channel 8 in the same case. Note that only half the main lobe is present. These cases are not a problem, however, since the polarization of the signal can be derived even from these.

Polarization Derived from DFT



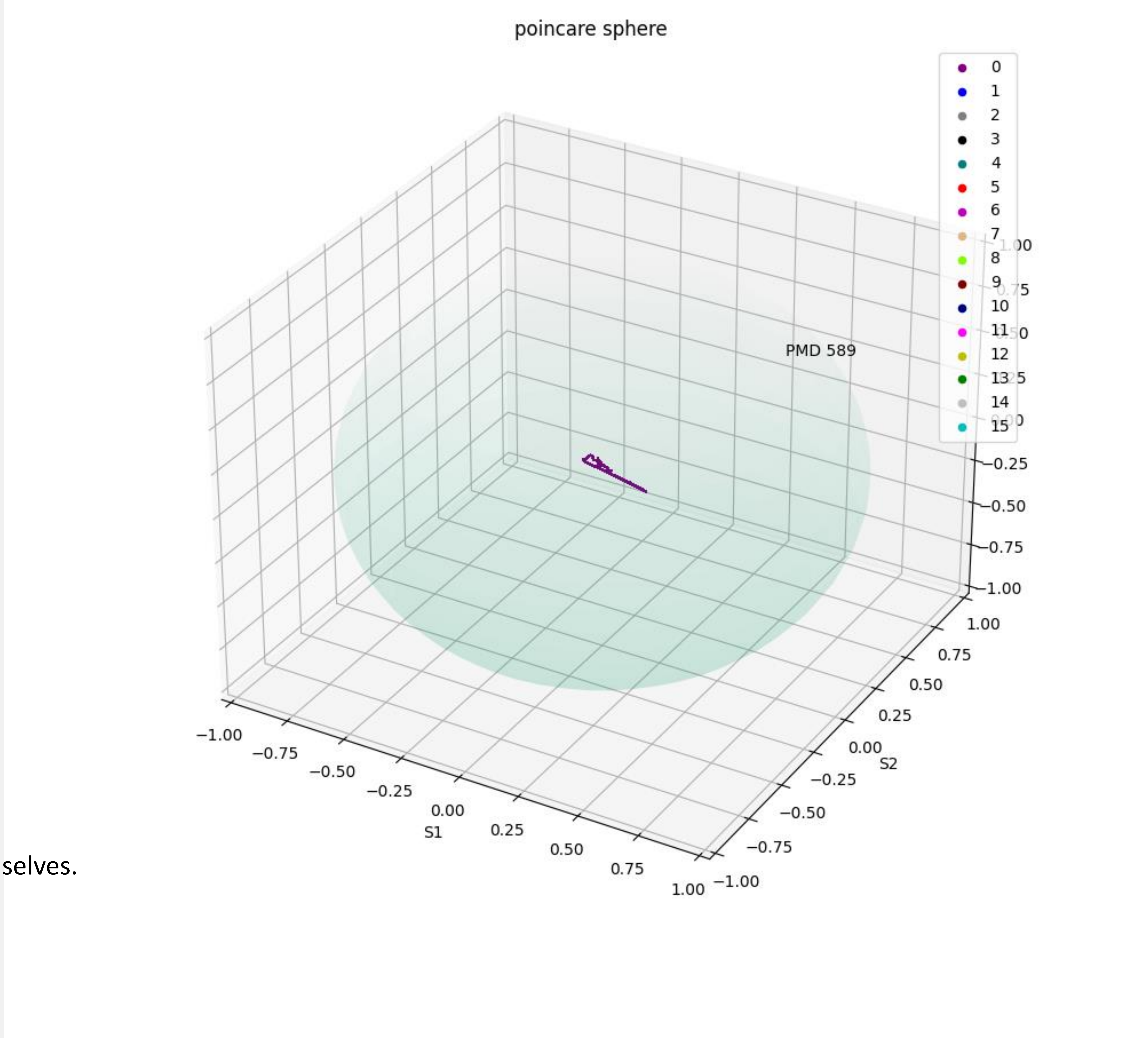
A signal is captured and its fingerprint plotted on the surface of a sphere.

Polarization Derived from DFT



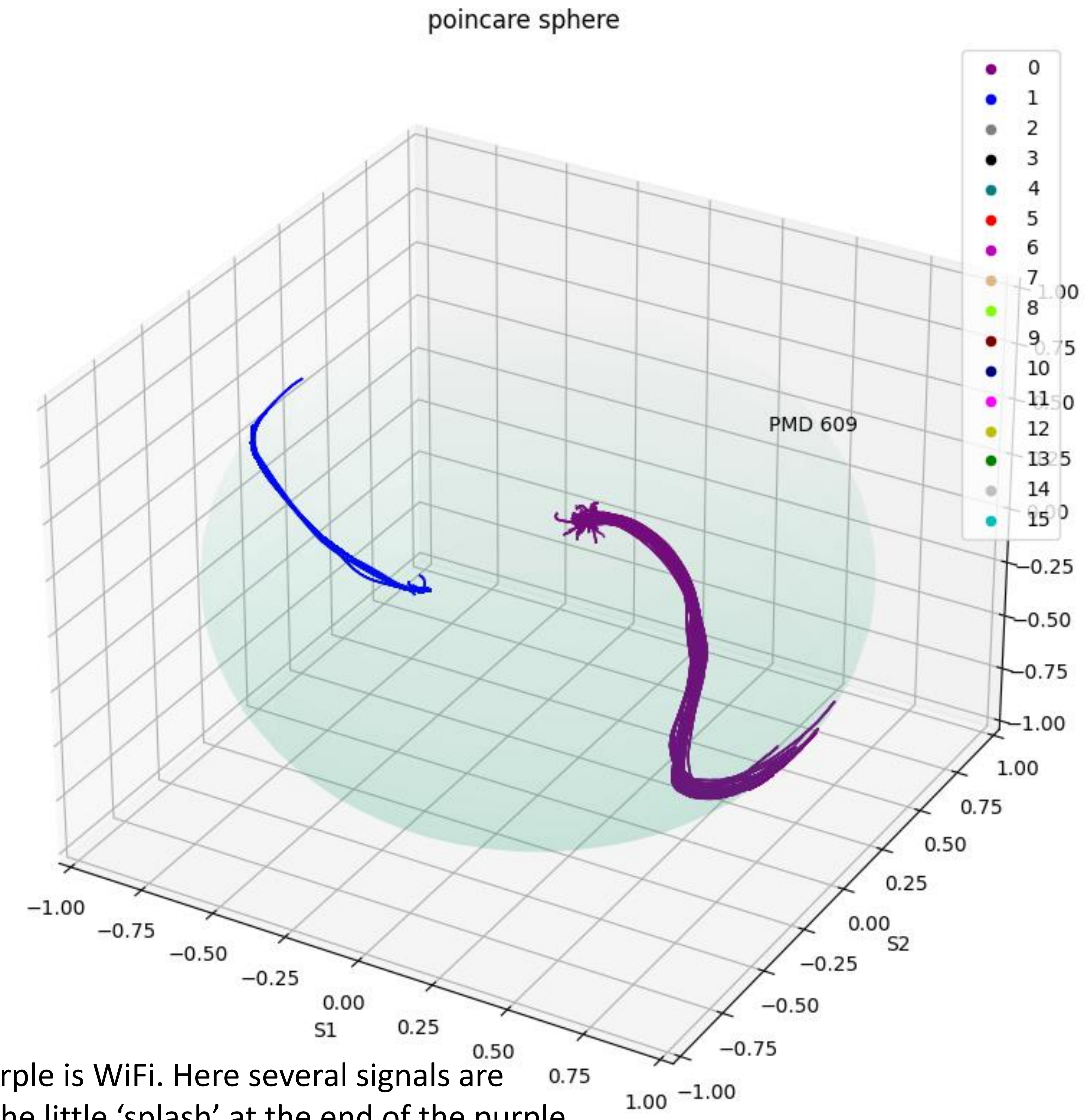
Even the same kind of device in a different location will have a different fingerprint.

Polarization Derived from DFT



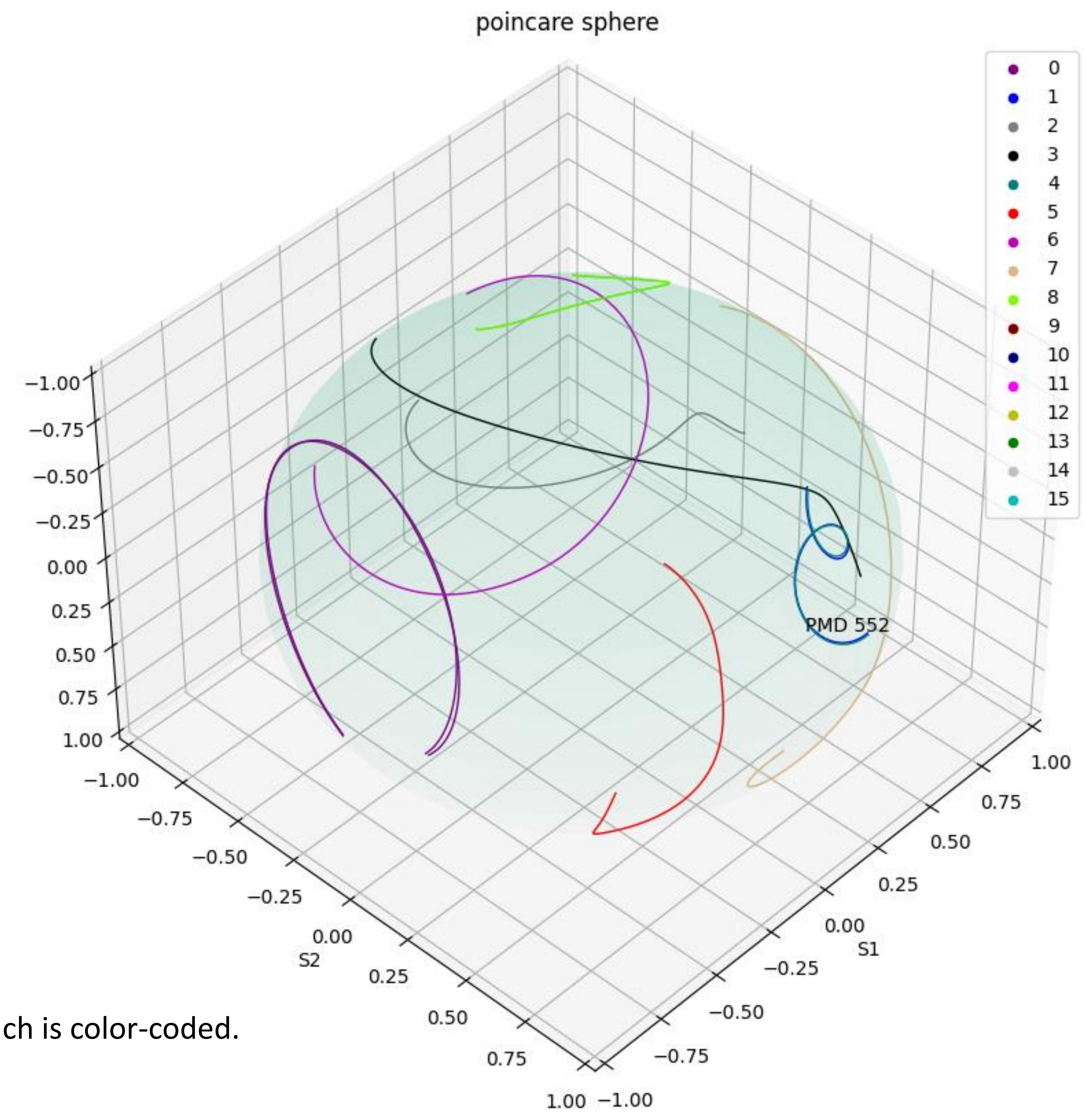
Fingerprints can double-back on themselves.

Polarization Derived from DFT



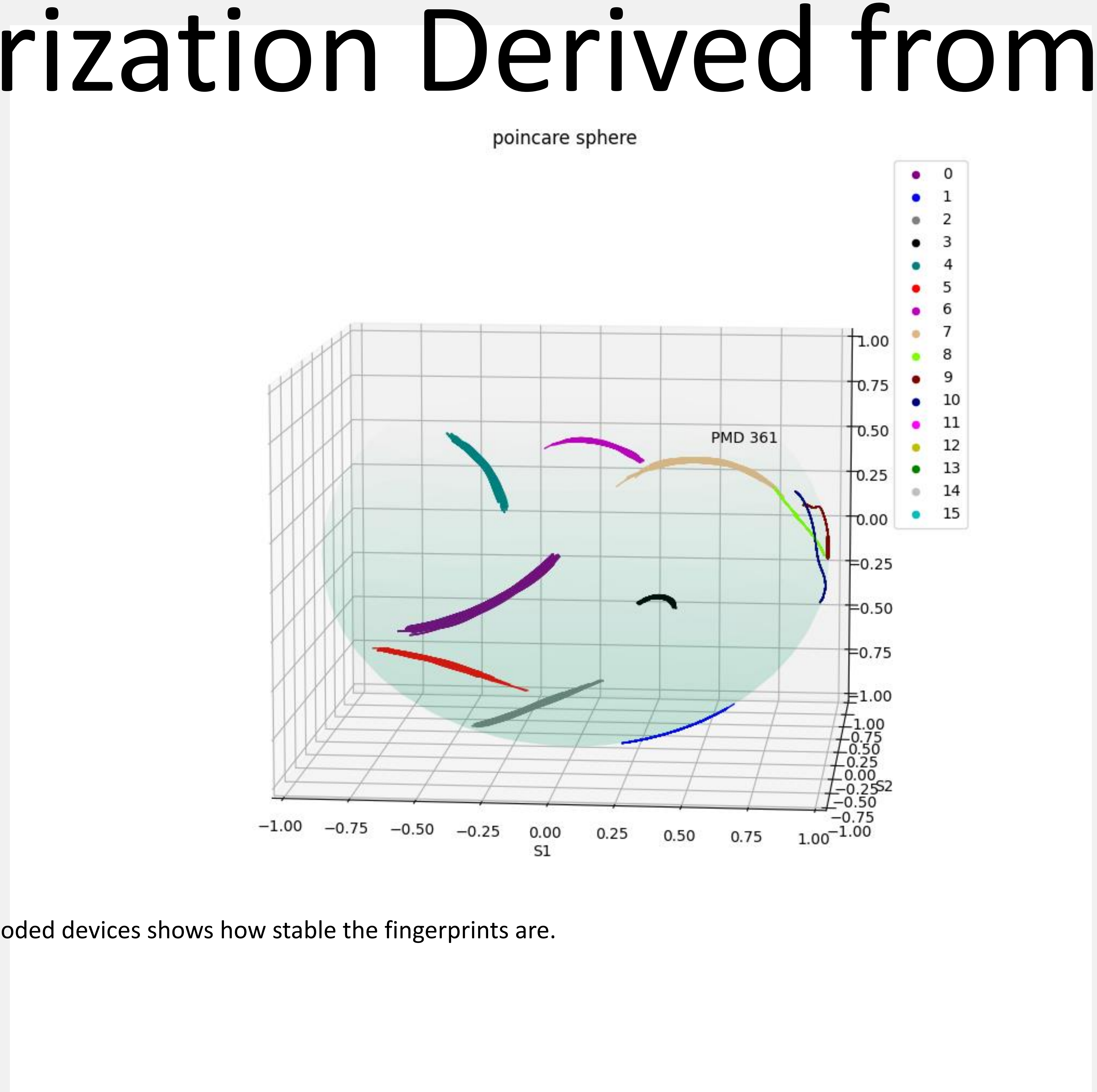
The blue fingerprint is a Bluetooth device and the purple is WiFi. Here several signals are overlapped to see how they might differ over time. The little 'splash' at the end of the purple fingerprint is the result of a side lobe getting into the calculations.

Polarization Derived from DFT



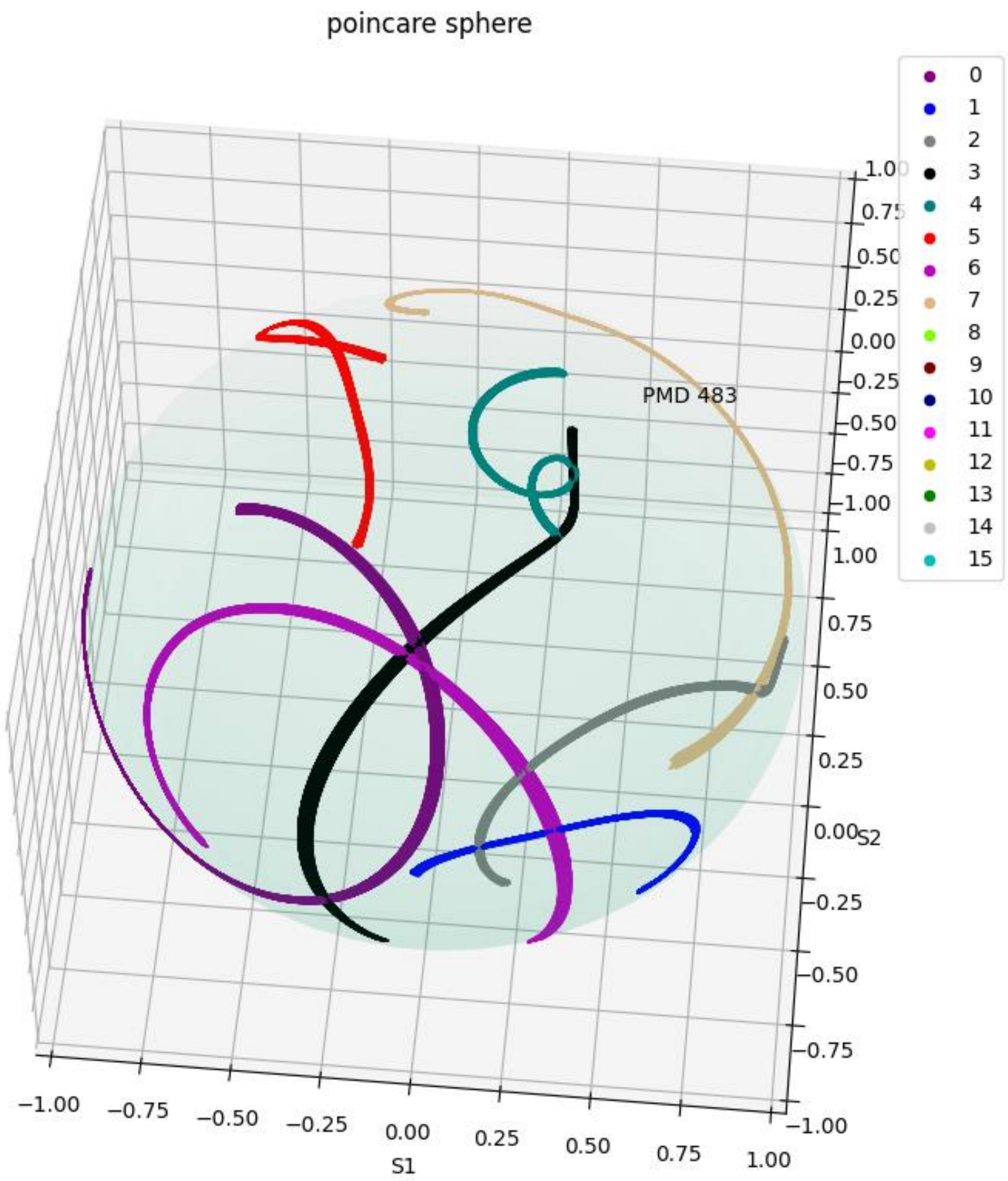
This chart was made with 8 different devices. Each is color-coded.

Polarization Derived from DFT



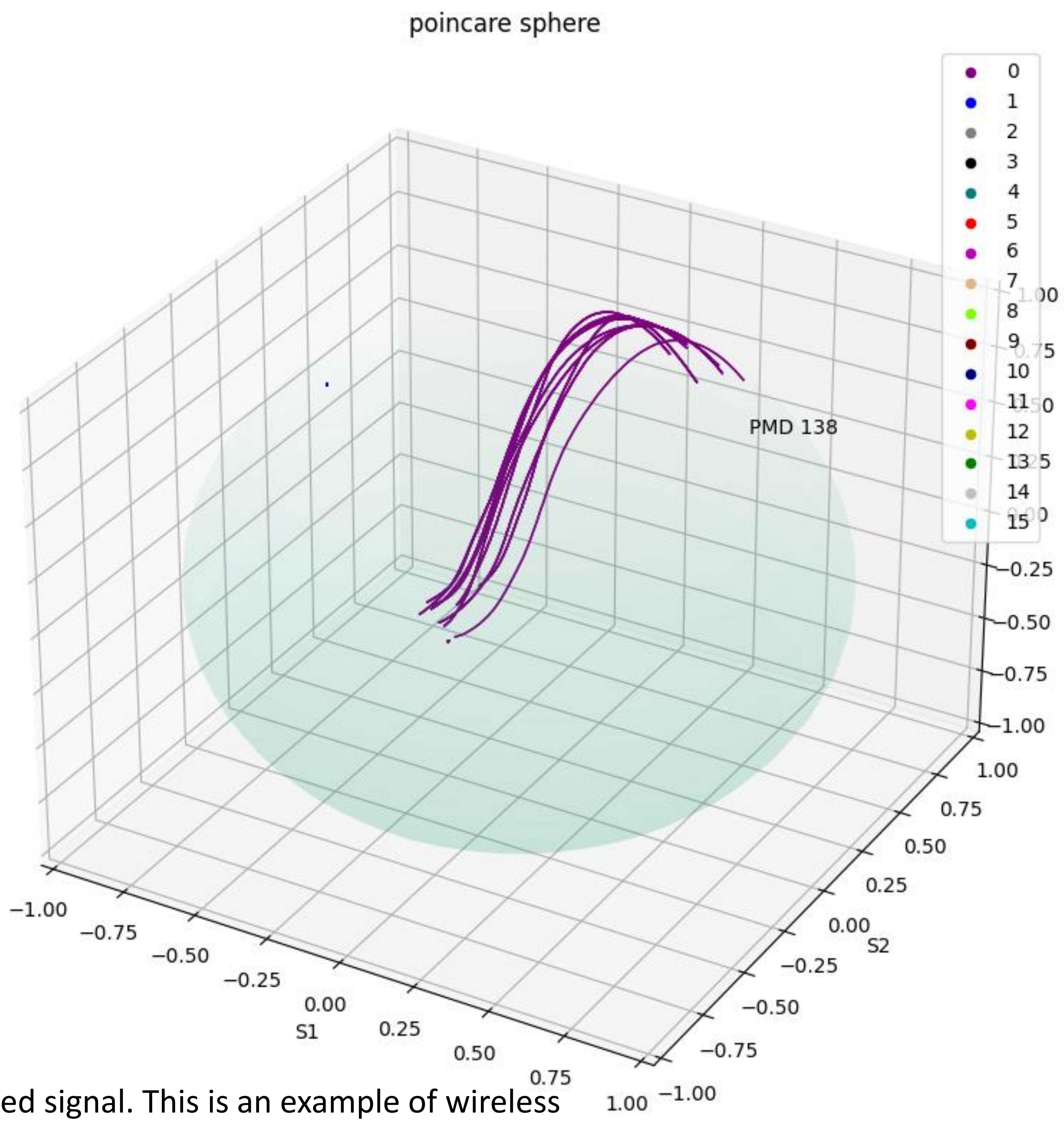
Overlapping 50 signals from 8 color-coded devices shows how stable the fingerprints are.

Polarization Derived from DFT



Overlapping 50 signals from 8 color-coded devices shows how stable the fingerprints are.

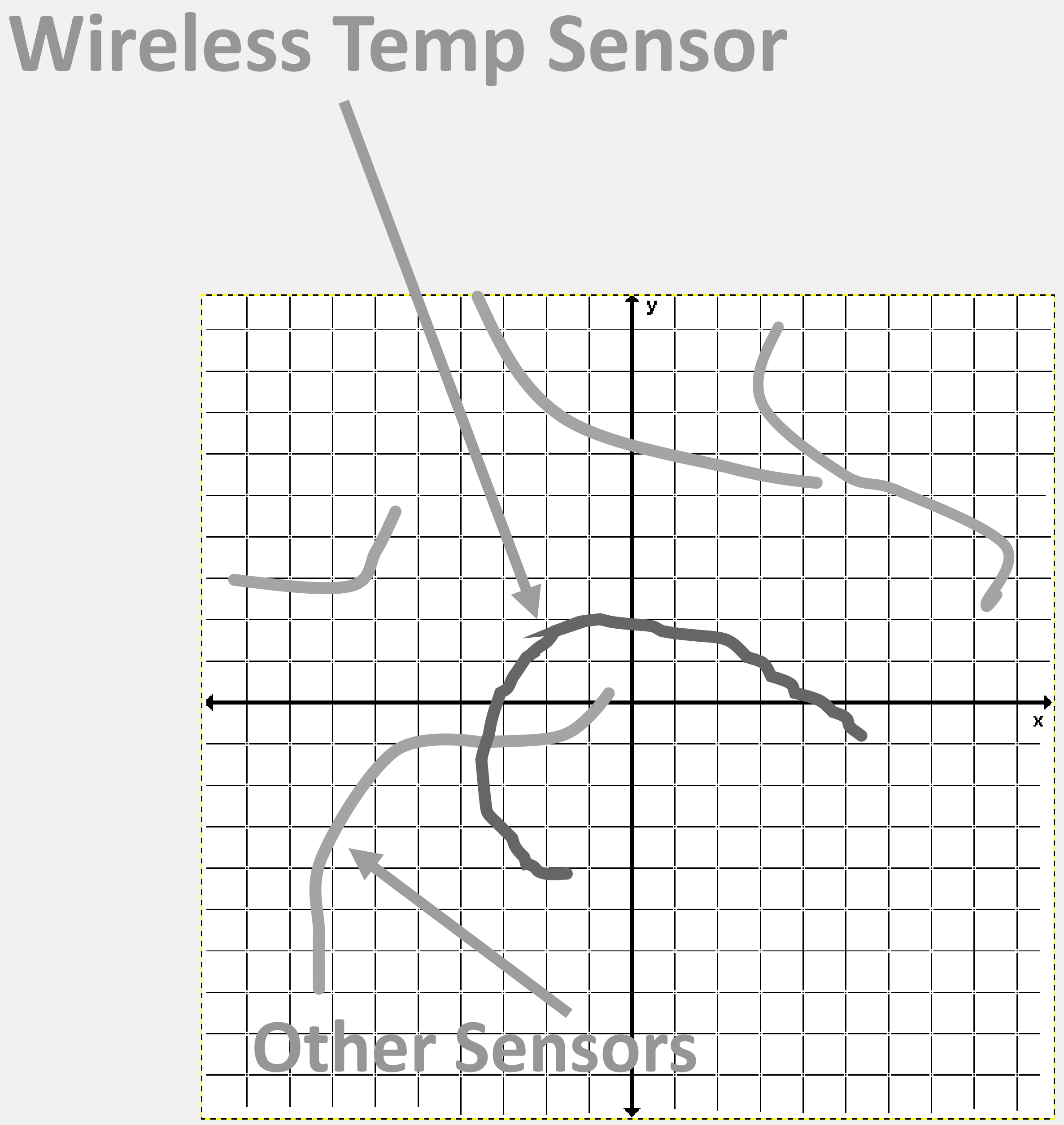
Polarization Derived from DFT

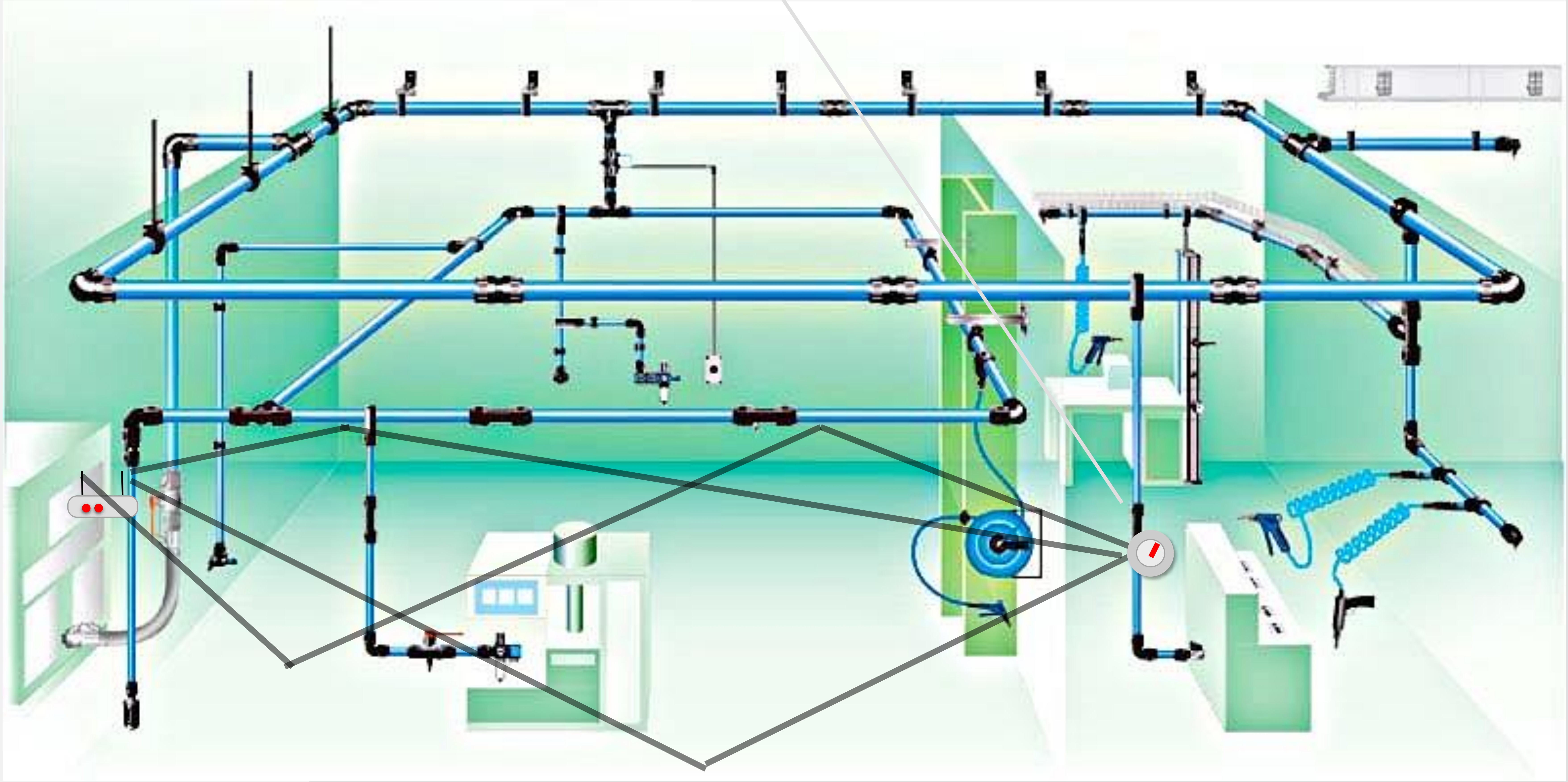


Motion in the path affects the dispersion of the received signal. This is an example of wireless device sending signals with a person walking in the multipath. Here, we can see that the affect is movement in the fingerprint in 1 of the 3 dimensions. The fingerprint of these signals, however, is recognized as coming from the same device, indicated by the static color.

How Fingerprinting Works

This temperature sensor communicates with a router, thereby establishing a fingerprint



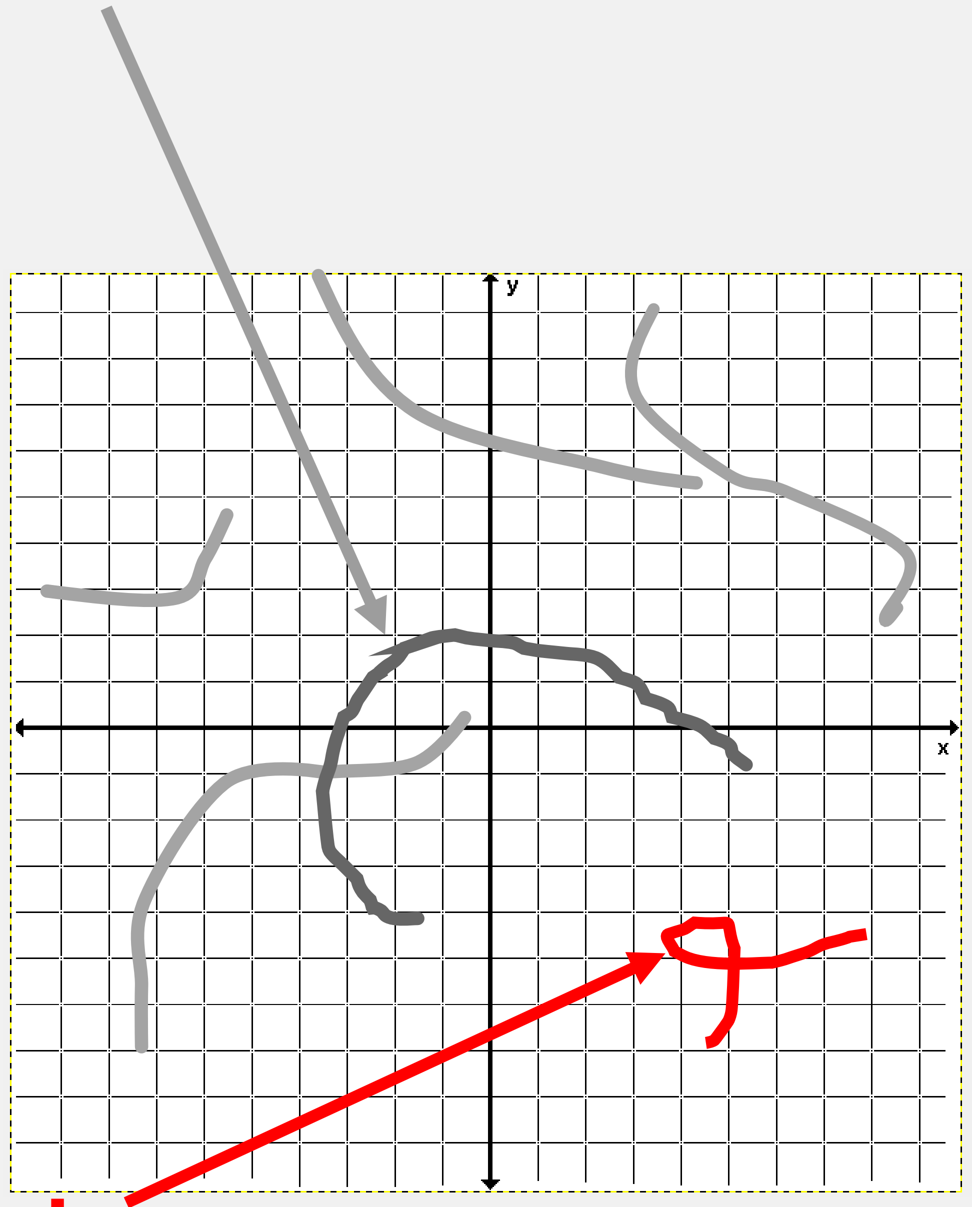


Natural Authentication done by characteristics of signal

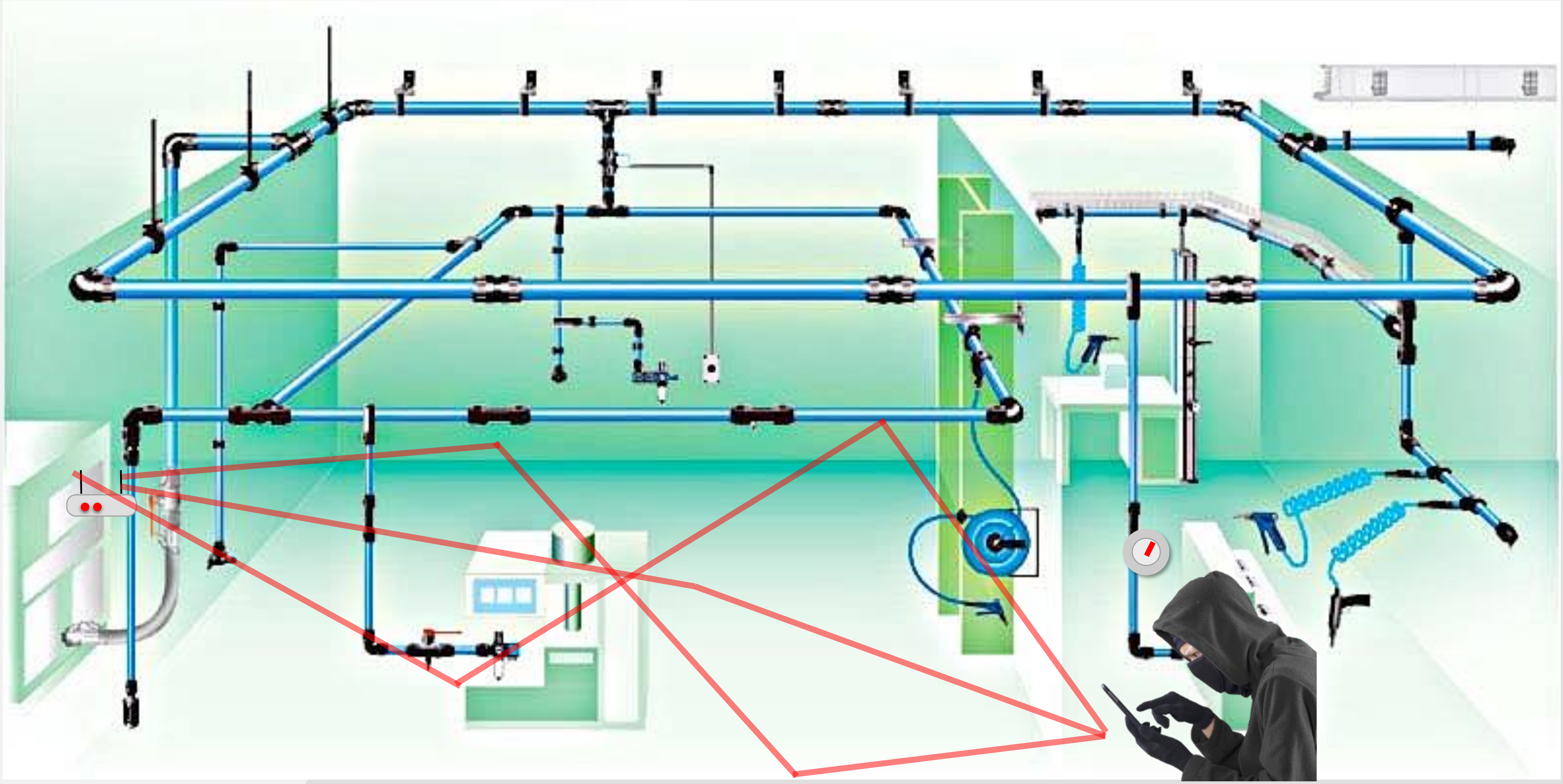
How Fingerprinting Works

But, a hacker's device looks entirely different to the router

Wireless Temp Sensor



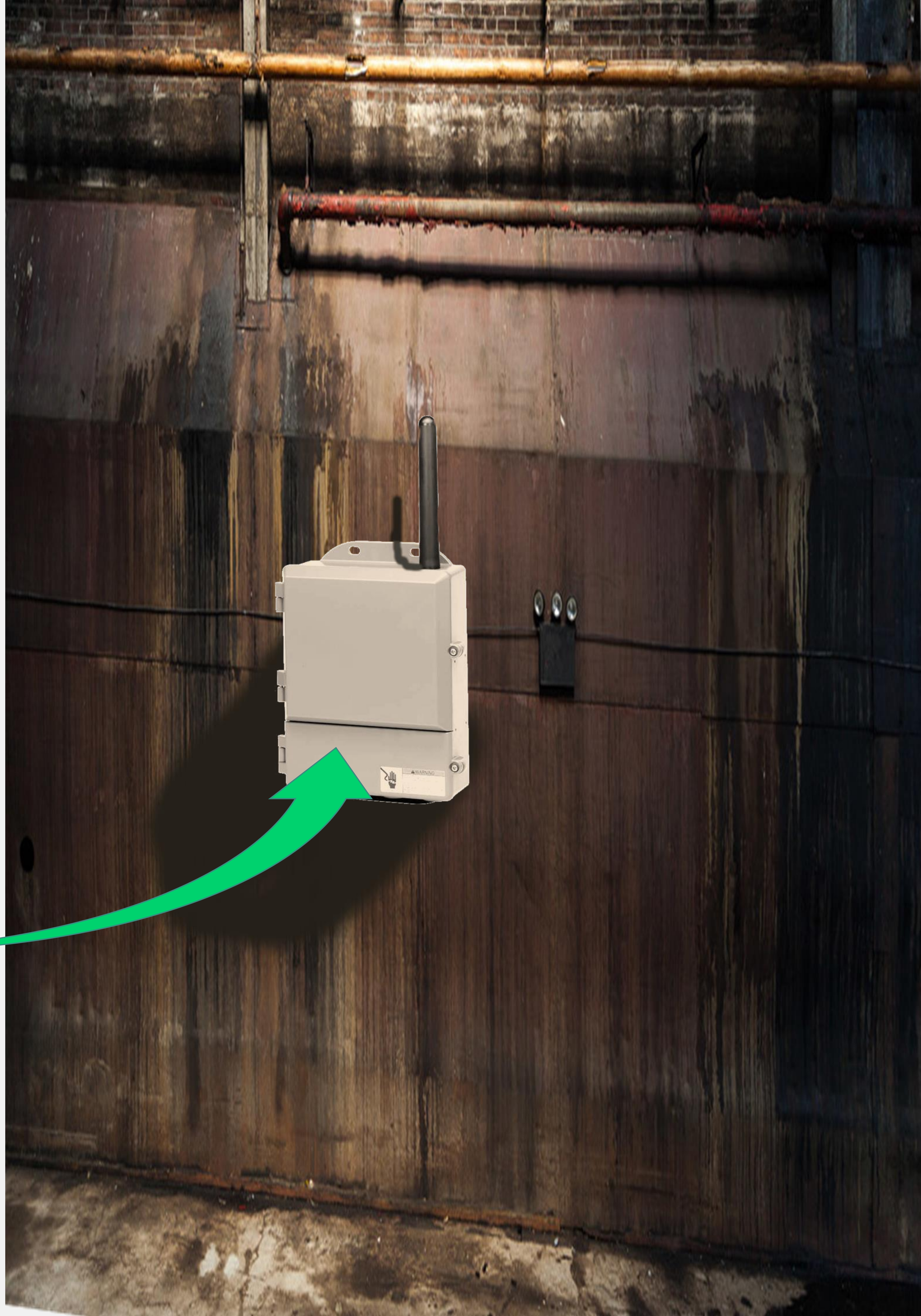
Hacker



Prevents Unauthorized Wireless Access

Implementation

Fingerprinting Technology



Fingerprinting advantages

No Encryption

No Security Key

Simplified Authentication Methods

No Network Protocol Layer Processing

Backward Compatible

Zero-Day Threat Prevention

Rogue Access Point Protection

No Need to Modify Endpoints

Protocol Agnostic

Near Zero-Touch Onboarding

IARIA

EndHackers

heller@endpointsecurityinc.com

linkedin.com/in/pheller

Page Heller, PE
Endpoint Security Inc
heller@endpointsecurityinc.com

ENDPOINT
Security Inc