Paper #1251 Special Session TH-SP.1P.8

Wideband Wide-Scan Millimeter-Wave Phased Arrays for Enhanced Security/Privacy and Performance in 5G Mobile Wireless

Johnson J. H. Wang
Wang Electro-Opto Corporation
Marietta, Georgia USA
email: jjhwang@weo.com

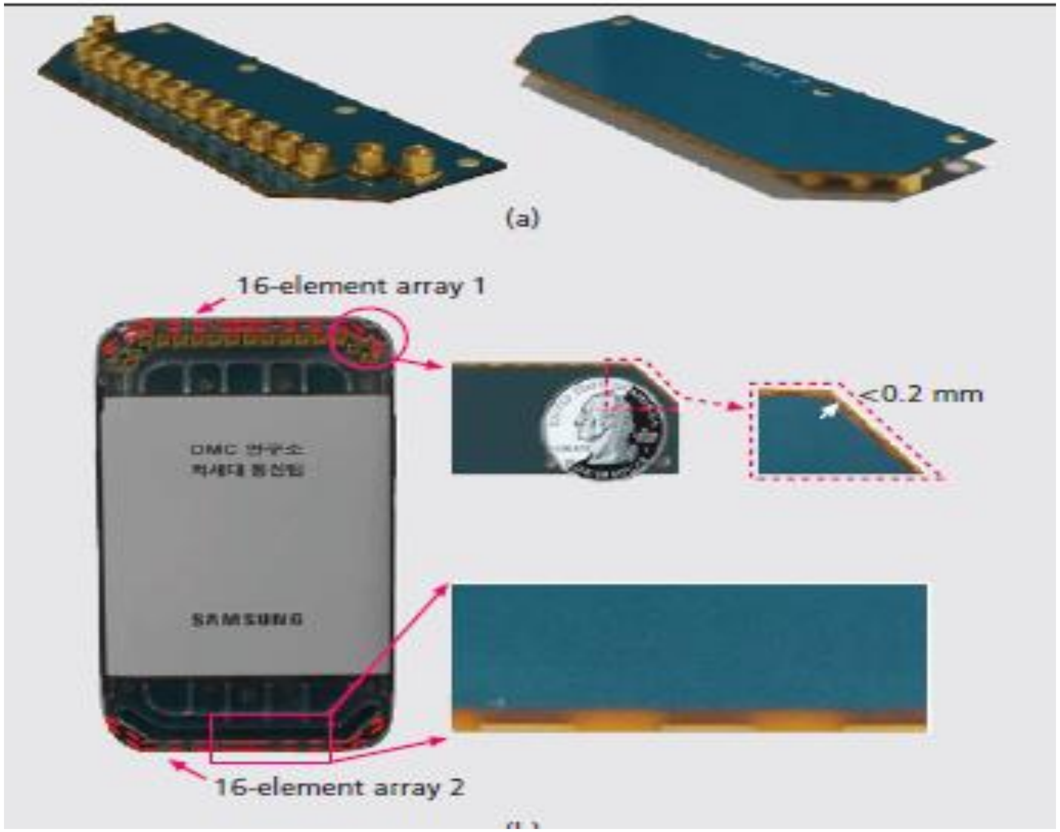
2017 IEEE International Antenna & Prop. Symposium and URSI Radio Science Meeting
San Diego, CA, USA
July 13, 2017

Milestone demonstration of 5G vision enabled by mmWave phased array ⟶ Promises and Concerns!

- *Grandeur 5G* vision using mmWave phased arrays on cell phones promises
  - Big-data
  - IoT (Internet of Things)
  - Cloud
- **New concern that 5G may be devastated by security failures in cyberspace!**

  This author* suggested in 2016 that wideband wide-scan mmWave phased arrays can enable a physical-layer security against cyberspace hacking!!!

**2016 IEEE Phased Array Symp.*



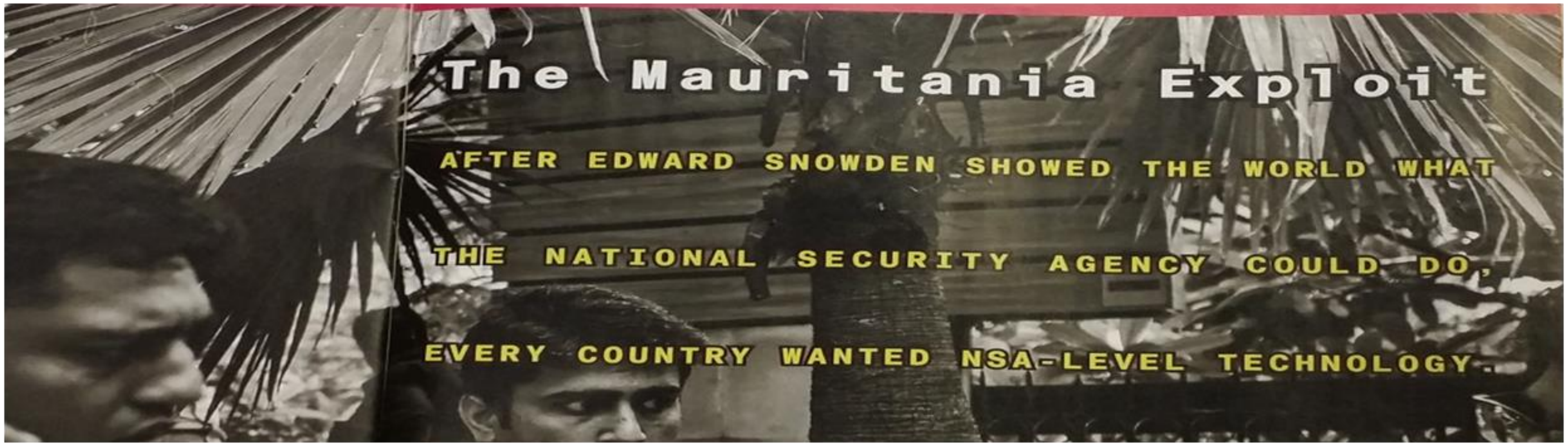
W. Hong et al, "Study and Prototyping of Practically Large-Scale mm Wave Antenna Systems for 5G Cellular Devices," *IEEE Communications Magazine*, September 2014.

Samsung 16-element array demo at 28 GHz

This paper discusses security/privacy concerns in 5G and proposes a solution

- Cyberspace hacking and security failures recently become daily news, frightening the public.
- So far the solutions planned by the global 5G community rely almost exclusively on cryptographic technology.
- This paper
  - Shows fundamental limitation of cryptographic technology —as it is based on an outdated Information Theory (ITh).
  - Proposes a physical-layer security following the approach taken by the defense and aerospace industry (DAI).

January 23-29, 2017



also, potentially, journalists, activists, and political opponents.

From Wolf, Mauritania sought software that would allow it to attack multiple targets connected to a large network. This could include, notably, a nationwide mobile phone provider—an especially attractive mark in a country that has only 51,000 fixed phone lines and where even goat herders have cell phones. Wolf's promotional literature promised customers the ability to perform a silent SMS attack, a sophisticated technique that allows full control of someone's smartphone without requiring the target to click on a link or otherwise interact.

The cyberspace is new and dynamic!

- The cyberspace dawned in1948 with Claude Shannon's Information Theory (ITh), as a man-made, virtual, notional, digital space, in which the time *t* is a magic variable (or dimension) analogous to its role in the physical space.

- Since then, mathematical formulation of cyberspace has been vigorously developed — on the crutch of the theory of stochastic processes, which are focused on a set of real or complex time functions $x(t,\zeta)$ — to this date.

The time *t* is a magic variable (and/or dimension) in both cyberspace and physical space

When man began to venture into deep space (in the infinitely large distance) and the atomic structure (the infinitely small subspace), classical Newtonian physics had to be modified by tweaking the concept of *time*—

- With the theory of relativity and Hamilton-Jacobi equation in celestial mechanics for the former;
- With Schroedinger's equation in quantum mechanics for the latter.

Information Theory (ITh) and new Quantum mechanics (QM) of 1925 are in similar mathematical formalism

- Quantum Mechanics (QM): Old QM (Plank 1900)

  ↓ 25 years

  New QM (Bohr, Heisenberg, Schroedinger; 1925)

- Information Theory (ITh): Claude Shannon 1948

  ↓ 69 years — Foundation unchanged

  Now 2017

It’s time to rethink Shannon’s Information Theory (ITh)—like the revision of Newtonian physics a century ago by Theory of Relativity and Quantum Mechanics!

- The reign of classical digital communication theory (Claude Shannon 1948) has been **69 years**. With the fundamentally changed global political-economic landscape, the requisite conditions and assumptions of information theory and their derivatives are increasingly more difficult to postulate.
- ***It is time to rethink the magic dimension (or variable) of time t in 5G***

  as 5G moves toward and beyond air latency of <1 msec and cell throughput of > 10 Gbps at mmWave frequencies.

Fundamental assumptions of Shannon's Information Theory (ITh) are no longer valid in cyberspace!

- The changing Cyberspace
  - 1948 Shannon's ITh ignored anything "biological" or intelligent conveniently.
  - 1991 anti-virus software began to have a tiny market.
  - 2000 Intelligent elements entered—GPS service disabled in Washington DC region by a 5-watt jammer!
  - 2012 Cyberspace hacking began to take off! End of the Age of Innocence!
- The stable Physical Space:

  Quantum Mechanics is still adequate for Physical Space

Now ITh guru Dr. Bob Lucky— who admires Shannon's 1948 paper as "the greatest work of genius" — lamented*

- Data ⟶ Big Data ⟶ Humongous Data ⟶ CLOUD!
- Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?
- We have come a long way since Claude Shannon,…in 1948, could simply ignore the knowledge problem by writing: "Frequently the messages have meaning….These semantic aspects of communication are irrelevant to the engineering problem."

***R. W. Lucky, "The counterintuitive cloud," IEEE Spectrum, p. 25, May 2017.**

The global cyberspace now has characteristics akin to some biological system

- The phenomenal success of 4G gave rise to ubiquitous mobile connectivity, projected to reach 80 Billion devices in 2020.
- As a consequence, the global cyberspace now has characteristics akin to biological systems.
- The air interface for each IoT (Internet of Things) is an open door, vulnerable to penetration (accidental, dubious, or malicious).
- The global cyberspace is like the Physical Space on Earth in mid-1400s — when the Black Plague killed 1/3 to ½ population in many parts of the world!

The global cyberspace now is akin to a humongous intelligent system

- With the rise of artificial intelligence and intelligent machines, the global cyberspace now also has essential characteristics of an intelligent system — as intelligent as the ensemble of humans and their machines on earth having some sort of connectivity to the outside world.
- But the modern global cyberspace is weakly regulated (ad hoc or anarchy)
  - like the world of 3000 years B.C. …….

Side notes on semantics

- Biological System = a system with at least some intelligence.
- Intelligent System can be a Biological System or can mimic a Biological System to a certain degree.

For secure communications, the easy route for 5G is to crossfertilize from military handheld radios!

- Since1980, US military has been developing, and recently deployed, handheld radios capable of secure Communications, Command, Control, Computer, Intelligence & Electronic Warfare (C4I&EW), notably under two contiguous DoD Technology initiatives:
  - SpeakEasy: 1980-2000 (DARPA & Army CERDEC)
  - JTRS: 2000-today (mainly Army CERDEC).
- They are software-defined radios (SDR) using antennas with
  - Ultra-wide and multiple bandwidths
  - Sophisticated radiation properties (patterns, polarizations, multimode, smart, etc.)
- Several other countries have also launched similar thrusts since late 1990s.

Specifications for:

Harris Falcon III® AN/PRC-152A Wideband

GENERAL	
RT Nomenclature	RT-1916x(P)(C)/U
Frequency Range	30 - 870 MHz Narrowband: VHF 30-225 MHz, UHF 225-512 MHz Legacy SATCOM: RX 243-270 MHz, TX 291-318 MHz High Band (VULOS/P25): 512-520 & 762-870 MHz Wideband: 225-450 MHz
Channel Spacing/Bandwidth	Narrowband: 8.33,12.5, 25 kHz-AM, 12.5, 25 kHz-FM SATCOM: 5 kHz, 25 kHz Wideband: 500 kHz, 1.2 MHz FM Deviation: 5 kHz, 6.5 kHz, 8 kHz

A preliminary scale model for study at WEO

- Two thin subarrays are symmetrically positioned, and "integrated" into the surface of a generic platform.
- The subarrays' orientations about Z, the center axis of the platform, are varied, and aided by electronic beam steering, to attain full spatial coverage needed for the requirements.
- Based on WEO's Traveling-Wave Antenna Array (TWAA) as a Multioctave Planar Phased Arrays (MPPA) at TRL-7 and MRL-7*

***J. J. H. Wang, 2016 IEEE International Phased Array Symp., Waltham, MA, October 2016.**

Comparisons with Samsung's data

- Samsung used two essentially 1-dimensional 16-element arrays of narrow bandwidth were integrated into a Samsung cellphone,
- The patterns recorded and displayed appear to be in the plane of the smartphone surface, judging from the directivity and first sidelobe level of the pattern for 0° scan.
- Conceivably, the patterns on a plane perpendicular to the planar surface of the Samsung phone would have much lower gain and directivity. Thus the signal-to-noise ratio in this case might be considerably lower.
- Lower directivity, with MIMO over multi-band and wideband, covering expanded 4G frequencies and mmWave frequencies together appears to be a practical solution—with cost, power, and packaging constraining the ultimate performance goals!

Constraining factors in implementing MIMO design

- At 60 GHz (mmWave), antenna aperture size A
  - A> 1 λ^2 in LOS
  - A> 9 λ^2 in NLOS

  K. Haneda, C. Gustafson, and S. Wyne, 60 GHz spatial radio transmission: Multiplexing or Beamforming?" *IEEE Trans. Antennas & Prop*., Nov. 2013.

- At 2.45 GHz (4G frequencies)
  - Gain variation ~ 10 dB

  W. Fan et al, "Antenna pattern impact on MIMO OTA testing," *IEEE Trans. Antennas & Prop*., Nov. 2013.

Some favorable tail winds!

- Frequency diversity is less expensive to implement and has pivotal performance and reliability advantages.

  R. L. Freeman, "Radio System Design for Telecommunications—(1-100 GHz), Wiley, NY, 2008.

- Antenna design for a newly produced Army AN/PRC-152A wideband network handheld radio covering most bands over 30-870 MHz, and a newer model covering six functions ranging from 30 MHz to 2000 MHz, in a contiguous way.
  - J. J. H. Wang and J. C. Adley, "30-2000 MHz Multi-band Body Wearable Antenna (MBWA)," paper #2643, session FR-A1.3A.2, this Symposium tomorrow morning.

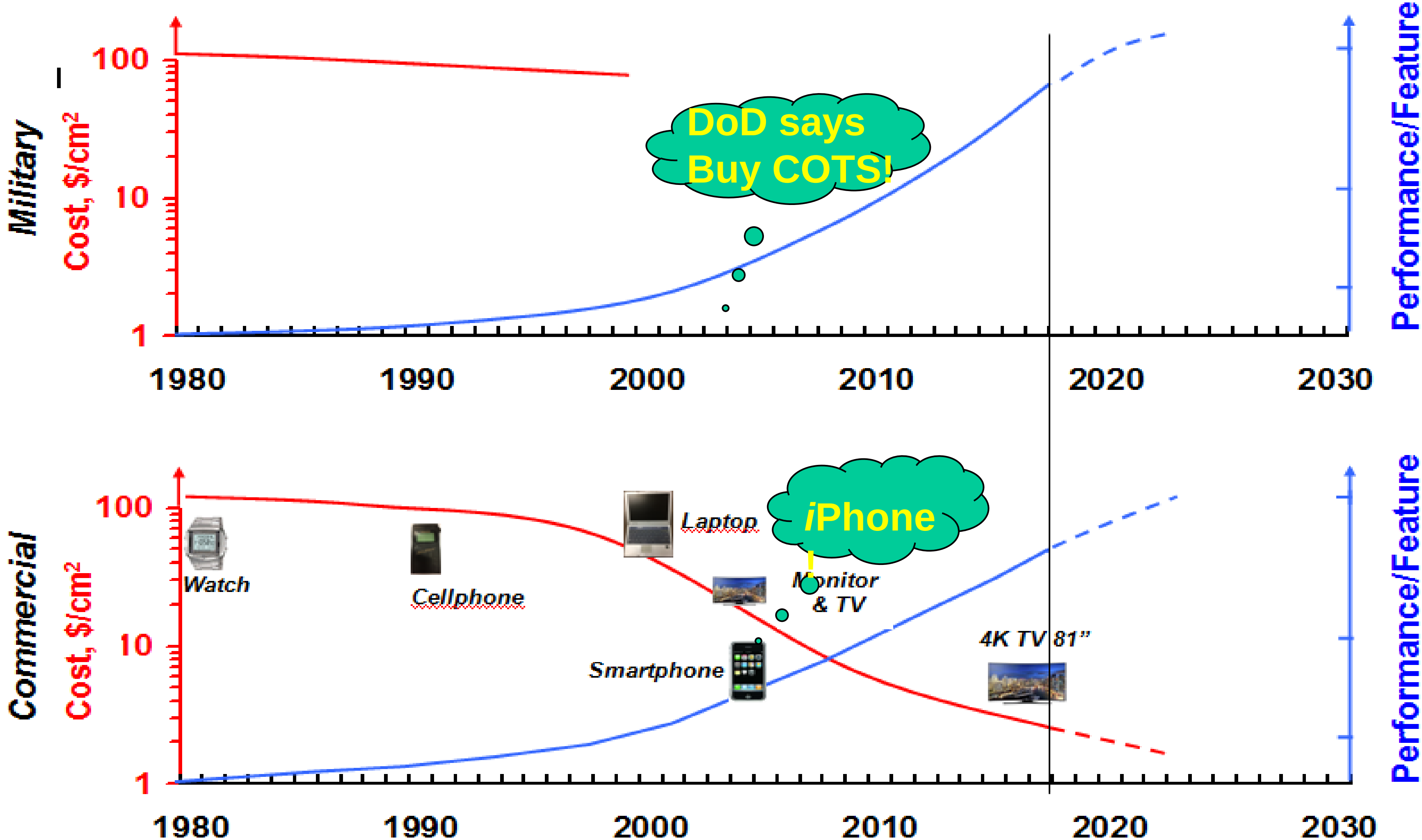
How to transform a $30K military radio to $400 5G phone?

- Overcome humongous cost and complexity
  - start with realistic scaled-down versions
  - teaming, joint or collaborative R&D efforts
- Engineering approaches
  - Downgrade, relax, and redefine specifications
  - Employ Massive MIMO (Multiple-Input Multiple-Output)
- Learn from *i*Phone history from Apple/Foxconn/Cingular?
  - Military radios : $3 Billion total (first 100,000 radio at $30,000 each including R&D & tooling cost costs).

↓

  - 5G phones : $40 Billion total (first 100 million secured phones at $400 each including 10% R&D & tooling costs)

Huge reduction in costs can be achieved by following historical path of Flat Panel Display (FPD) in Electronic Viewing



If the 5G spirit remains high, collective and competitive efforts on 5G should lead to success!