computers are bad

You are receiving this facsimile because you signed up for fax delivery of this newsletter. To stop delivery, contact Computers Are Bad by email or fax.

https://computer.rip - me@computer.rip - fax: +1 (505) 926-5492

2021-09-30 the original microcell

Many readers may know that, historically, telephone instruments (e.g. the thing you hold up to your face and talk into) have been considered part of the telephone system proper. In practice, that meant that up until the '70s most people leased their phones from the telephone company, and the telephone company maintained everything from the exchange office to the side of your head.

The biggest landmark in the shift of telephone instruments from “part of AT&T” to personal property that you can buy at WalMart is the “Carterfone decision.” The Carterfone precedent, that telephone users could connect anything they want to the telephone network as long as it is reasonably well-functioning and compatible, created the entire modern industry of telephones and accessories. What's only remembered a little hazily, though, is what the Carterfone actually was--the original device that fought for telephone interconnection.

The Carterfone was an acoustic coupler that allowed a telephone handset to be connected to a two-way radio. Essentially, it was the first form of telephone patch, although it was very simple and did not provide the automation that would later be expected from phone patches. A typical use-case for the Carterfone was to allow a dispatcher to connect someone in the field (using a mobile radio) to someone by telephone, with the dispatcher doing all of the dialing and supervision of the call.

The Carterfone was a long way from the wireless telephony systems we use today, but it is a common ancestor to most of them. It, and several other early telephone radio patch systems, introduced the concept that telephones could be divorced from their wires. Of course this lead to the development of radiotelephony, cellular phones, etc, but great distances weren't required for the radiotelephone to be useful.

Well into the ‘90s it was common to see people walking around their homes trailing 50' of telephone wire. A great deal of couplers and long cables were available for the purpose, and it either replaced or complemented (depending on budget) the also common practice of providing a telephone jack in each room. Wouldn't it be easier to avoid the need for in-wall, under-carpet, along-baseboard, and trip-hazard wiring entirely by using some sort of local, low-power radiotelephone?

I am, of course, describing the cordless phone, and early cordless phones were not much more complex than low-power two-way radios. There is one primary way in which a telephone is different from a radio: telephones are full-duplex, while “radio” is generally taken to refer to a half-duplex system in which it is necessary to use a push-to-talk or other control to switch to transmit.

Nowadays we tend to take full-duplex communications somewhat for granted, because it is reasonably easy to simulate it through packetization. In the ’80s, though, when cordless phones became popular, packetized digital voice technology was still some ways from being sufficiently small and cheap to put in a consumer phone. Instead, full-duplex communication required that the handset and base station both transmit and receive simultaneously.

So, a cordless handset contained two radios, a transmitter and a receiver, and the base station contained two radios as well. There is a basic problem with operating two radios like this: the receive radio will typically be overwhelmed by the signal emitted by the transmit radio, and so unable to receive anything. There are various ways to solve this problem, but it becomes far easier if the simultaneous transmit and receive are at very different frequencies. For this reason, early cordless phone systems made use of pairs.

A typical design was this: the base station transmitted to the handset at around 1.7MHz, and the handset transmitted back to the base station at around 27MHz. The use of two different bands made it relatively easy for each receiver to filter out the signal from the nearby transmitter. Of course, the split-system between two bands can now result in confusion as it’s not always clear what a “27MHz phone” for example even means.

Signaling was extremely simple, generally constrained to something like the phone emitting one fixed tone to indicate that the base should go off-hook, and another fixed tone to indicate it should go on-hook. Since DTMF was generated on the handset, no other signaling was required. This allowed the implementation to be almost entirely analog.

Actual modulation was FM, and on early cordless phones channel selection was manual with only a small number of discrete channels available. This meant that interference and crosstalk between different cordless phones was a common problem, one worsened by cordless phones sharing frequency allocations with some devices like baby monitors. Security was a very real problem, people did indeed listen in on other people’s cordless phone calls by repurposing consumer devices like baby monitors or using wide-band receive radios.

Later cordless phones continued to use this basic scheme, although a 47Mhz band was added into the mix. The use of the higher frequency bands had the major benefit of making the antennas smaller; 1.7MHz phones had required a telescopic whip antenna while 27MHz/49MHz phones could generally make do with a “rubber ducky” antenna more typical of cordless phones today.

More interestingly, though, these later phones in the VHF low-band were capable of quite a few more channels and so introduced automatic channel selection. The need to implement link negotiation lead naturally to a more sophisticated signaling system between the handset and the base. Digital signaling allowed the base and handset to exchange commands, first enabling the “find handset” button on the base and later allowing the handset to control an answering machine integrated into the base.

The introduction of 900MHz phones (900MHz is a common ISM band used by a variety of devices) occurred somewhat in a transitional period, as there are both analog and digital phones made for 900MHz with various combinations of signaling and security features. Digital encoding and the use of spread spectrum tended to improve audio quality but also security, because even if there was no encryption decoding required a specialized device... and spread spectrum is itself a form of security if the sequence is determined in a secure fashion. Digital cordless phones largely eliminated eavesdropping except by particularly determined opponents, but generally only did so by raising the attack cost (requiring a decoder) rather than by employing strong security.

The 900MHz band is crowded with devices, as are 2.4GHz and 5.8 GHz where various late-'90s and early-'00s digital cordless phones operated. This often translated into disappointing range and reliability, and moreover there was a serious lack of standardization. Standardization tends to be less important for cordless phones because the base and handsets are sold together to the extend that consumers have no real expectation of them being interchangeable (technically they often are but it is difficult to determine between which devices). A bigger issue was a lack of consumer understanding of the different features that cordless phones carried. Was any given phone secure (in that it employed some type of encryption)? Was it going to be more or less subject to interference from the microwave oven? What about range?

All of these questions would be best addressed by the industry concentrating on a standard cordless phone implementation, and the allocation of a dedicated band for these devices would significantly reduce interference problems. The confluence of these two interests lead to a major standards effort in the early '00s that culminated in the adoption of a European standard which had been the norm in Europe since the '90s: DECT.

DECT is a very interesting beast. While DECT is now strongly associated with consumer cordless phones, it was always intended for much more ambitious use-cases. DECT could serve as the entire wireless plane for a corporate PBX system, for example, using centralized base stations (ceiling mount perhaps) to set up calls and signaling between a variety of handsets carried by employees [1]. DECT was even contemplated as a cellular telephony standard, with urban-area base stations managing large numbers of subscriber handsets.

In practice, though, DECT has a much more modest role in the US. First, there is a matter of naming. DECT in the US is referred to as DECT 6.0, which has created a false impression that it is either version 6 or operates at 6.0 GHz. In fact, DECT 6.0 operates in a 1.8GHz band allocated for that purpose and the name is just marketing fluff because 6 is a bigger number than the 5.8GHz cordless phones that were on the market at the time.

DECT makes use of frequency-hopping techniques as well as digital encoding that allow for active mitigation of interference based on time-division multiplexing. The takeaway is that, generally speaking, DECT phones will not interfere with other DECT phones. This addressed the biggest performance problems seen in congested areas.

DECT is, of course, packetized, and took many tips from the simultaneous work on ISDN in Europe. The DECT network protocol, LAPC, is based on the ISDN data link layer. Both are based on HDLC, an ISO network protocol that was derived from IBM's SNA. So, in a vague historical sense, modern cordless phones speak the same language as late '70s big iron, but over a wireless medium.

LAPC is a fairly complete network protocol, even from a modern perspective, and provides both connection-oriented and connectionless communications. Like most network protocols from the telecom industry, DECT supports defined-bandwidth connections by means of allocating "slots" in the network scheduling.

On top of LAPC a variety of functionality has been implemented, but most importantly basic call control (supervision) functionality and set up of real-time media channels using various codecs. Common codecs are ADPCM and u-law PCM, which both provide superior call quality to the cellular network (when HD voice does not succeed).

Because of DECT's greater ambitions, there is also a management protocol defined which allows handsets to register with base stations and exchange subscriber information. This allows cellular-like behavior that supports environments where there are multiple base stations with handsets roaming between them.

DECT supports authentication and encryption, but implementation is very inconsistent. The standard authentication and encryption protocol until around a decade ago was one with known weaknesses. As a practical matter, the use of FSS and TDMA in DECT makes active attacks difficult, and so DECT "exploits" do not seem to have ever been particularly common in the wild... but it certainly is possible to intercept DECT traffic, which lead to a change in standards to 128-bit AES encryption with improved key negotiation. Unfortunately it's not always easy to tell if devices make use of the newer encryption capability (or any at all), so security issues remain in practical DECT systems.

That's a lot about what DECT actually does, but what about the weird things it could do and usually doesn't? Those are my favorite kinds of things.

Protocols have been defined to run IP on top of DECT. IP-over-DECT was actually very competitive with 801.11 WiFi--it was slow (0.5mbps) but comparatively very reliable. A particular strong point for DECT was its origin as a possible cellular standard: DECT has always handled roaming between base stations very well, something that multi-AP WiFi systems struggle with in practice to this day. This made DECT a particularly compelling option for data networking in large, industrial environments. DECT IP networking was integrated into some industrial hand-held PC systems but was never common, despite efforts to commercialize a very WiFi-like DECT system under the name Net3. Another DECT computer networking initiative ran under the name PADcard and seems to have been launched on a few consumer products, but fizzled out very quickly.

What about DECT as a public cellular telephony standard? This doesn't seem to have really materialized anywhere. DECT had success in large-area applications like mines, but these were all still private corporate systems. DECT development for large systems ran pretty simultaneously with the development of GSM, which quickly gained more traction in DECT's European stronghold.

Despite DECT's failure to achieve its full potential, it has brought a surprising level of sophistication to the humble cordless phone. Modern cordless phones are almost exclusively DECT and take advantage of DECT's capabilities to offer multiple handsets per base station, intercom calling between handsets (often both dialed and "page" or broadcast), and a solid-state answering machine integrated into the base station and controllable from handsets. All cool features that no one uses, because now we all have cellphones.

[1] This use-case has obtained some success in the US in retail environments. Pacific Northwest retailer Fred Meyer's, for example, at least prior to the Kroger acquisition, armed each staff member with a DECT handset and earpiece at most stores. The advantages of this type of setup are clear: DECT handsets can be similarly priced to two-way radios but allow full-duplex communication and a "hybrid" model of radio vs. telephony behavior, by either selecting an intercom channel or dialing a number to reach a specific person. DECT in retail is likely giving way to IP-based solutions like Theatro (in use at some Walgreens locations), but a great many retailers (most Wal-Marts, for example) still use basic two-way radios on MURS or color dot channels.

PBX DECT systems are still available though, and I remain tempted to buy the DECT gateway for the '90s digital PBX that runs in my office closet. More in the modern era, because DECT is better established than WiFi for telephony applications there are a lot of "Cordless IP phones" that handle all the IP in the base station and use DECT to reach the cordless phones. These are basically just IP evolutions of the older approach of a DECT module connected to analog accessory ports or a dedicated board in the PBX.

A special bonus addendum for the Hacker News crowd: After I wrote this, I somehow ran into the Japanese Personal Handy-Phone System. It's a moderately successful (for a time) cellular service using a technology that was very similar to DECT. Despite the Wikipedia article sort of making it sound like it, PHS does not seem to have actually been based on DECT in any way. It looks like a case of parallel evolution at the least.