Cheating Time

How to build your own DCF77 transmitter

Andreas Müller

cosin[2006]
CHAOS SINGULARITY
7TH UNTIL 9TH JULY 2006

1. Some infos about the speaker
2. Some infos about DCF77
   - What is DCF77
   - DCF77 protocol
3. Spoofing DCF77
   - Motivation?
   - How to spoof the signal
   - Signal generation with ATMega8
   - Signal generation with soundcard
   - Future of the DCF77 signal
   - Conclusions
4. Questions/Links

Some infos about the speaker

- studying electrical engineering and information technology
- Chaostreff Aargau
- other interests:
  - software defined radio
  - hardware misuse and reuse

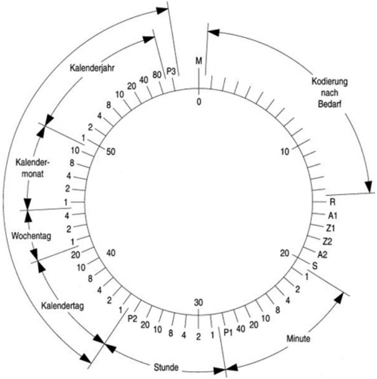
What is DCF77?

- official german time signal
- used by many radio controlled clocks for time synchronisation
- compatible to the swiss HBG signal (at 75kHz)
- callsign DCF77 (D: germany; C: longwave; F: near Frankfurt)
- time base is very accurate (atomic clocks used)
- accurate receiving ($<$1ms difference) is difficult
- widely available, due to low frequency

DCF77 protocol - signal characteristics

- continuous wave at 77.5kHz (LF!)
- amplitude lowered to 25% once per second
  - 100ms for low bit (0)
  - 200ms for high bit (1)
  - power is not lowered when new minute starts
- 60 bits are transmitted in one minute
- additionally phase modulation, but most clocks don’t check that

DCF77 protocol - time code



- Z1: summertime; Z2: wintertime; A1: changing; A2: leap second; S: time start (always high)
- P1-P3: parity bits (even parity)
- numbers in BCD

DCF77 protocol - error checking

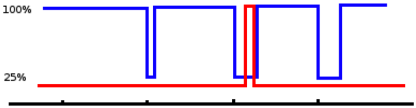
- protocol has error detection, but no security features
- 3 parity bits → 1/8 chance that random signal is correct
- most clocks receive 2 minutes until they accept the signal
- there’s no easy way to add security, because everyone should be able to use it

Why would anyone want to spoof the DCF77 signal?

- it's old, but still widely used (easy and cheap implementation!)
- from ptb.de:
  Zeitdienstsysteme bei der Bahn, im Bereich der Telekommunikation und der Informationstechnologie, bei Rundfunk- und Fernsehanstalten werden z.B. ebenso von DCF77 funkgesteuert wie Tarifschaltuhren bei Energieversorgungsunternehmen und Uhren in Ampelanlagen.
- just to give you some ideas, never tried by me

Spoofing - the smart way

- smart attack: just send wave for 100ms to change 200ms break to 100ms break
    - little power needed
    - very exact timing and power levels needed
    - hard to implement
    - 1 can be changed to 0, but not the other way



Spoofing - BruteForce

- brute force: send with more power than official sender
- the real signal will then be seen as noise by the clock
    - official signal is sent with 50 kW, but power drops with $1/m^2$ proportionality
    - for near range, very low power is needed for spoofing
    - easy to implement
- take care to set parity bits correct
- signal needs to be sent for a long time (at least some minutes)
- time base for sender should be stable

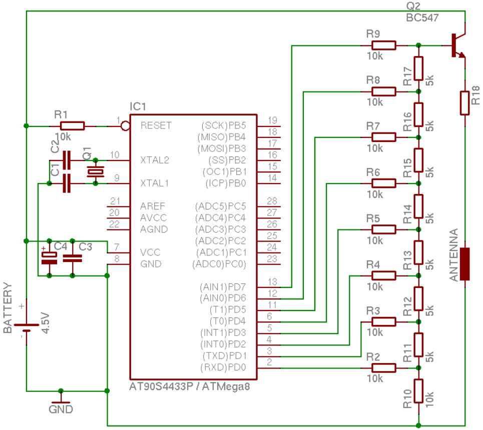
The almighty ATMega8

- 8bit RISC Microcontroller, up to 16MHz
- costs about 3 Euro per piece
- it's not a DSP
- some of the included peripherals:
  - IO ports, AD input ports
  - several timers (useful!)
  - serial interface, watchdog, etc

Sending the signal - using a microcontroller

- Hardware:
  - ATMega8 for signal and frequency generation
  - R-2R network for DA convertion
  - single transistor for current amplification
  - resistor to keep emitted power low
  - ferrite antenna (→ magnetic field is radiated)
- Software:
  - calculate DCF77 bits
  - assembler code for contionuous waveform output
  - timer generates 1 interrupt each second
  - at interrupt: delay 100ms or 200ms

Sending the signal - using a microcontroller

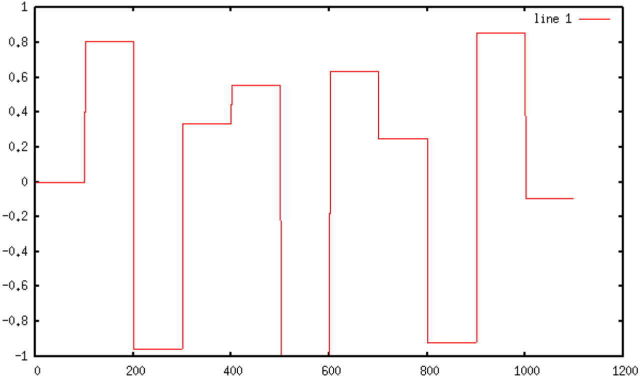


Sending the signal - using a soundcard

- soundcard is good for VLF (3-30kHz)
- DCF77 at 77.5 kHz is not much too high
- some soundcards work up to 96kHz, but most only to 22kHz (including mine)
- maybe using the 5th harmonic of a 15.5 kHz square wave
- square wave synthesis: $r(t) = \sum_{n=0}^{\infty} \frac{1}{2n+1} \sin((2n+1)t)$
- soundcards have lowpass filters to prevent output of aliases
- but we can take advantage of (usually unwanted) clipping

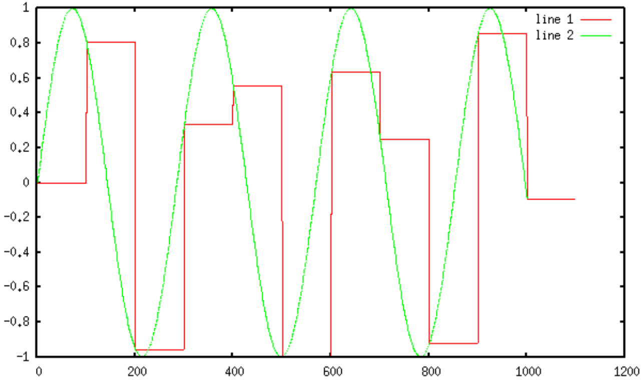
Sending the signal - using a soundcard

sinus signal after DA converter in soundcard:



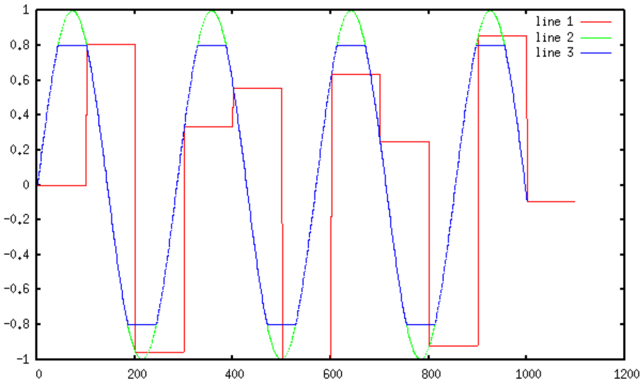
Sending the signal - using a soundcard

sinus signal after lowpass filter of soundcard:



Sending the signal - using a soundcard

signal with clipping (contains harmonics!):



Sending the signal - using a soundcard

Software and hardware Implementation:

- use xmms to create 15.5 kHz tone
  - add URL: `tone://15500/`
- C code controls mixer settings
- alternative: create mp3 for mobile spoofing
- antenna: use a speaker (creates magnetic field!)
- interesting legal question:
  - spoofing DCF77 is probaly not legal
  - playing a 15.5 kHz tone with a soundcard is certainly legal
  - as long as power is low, noone cares

Future uses of DCF77

- from ptb.de:
  [...] wurden bisher in den ersten vierzehn Sekunden jeder Minute nur Statusinformationen übertragen. Im Auftrag des Bundesinnenministeriums wurde untersucht, ob stattdessen im Gefahrenfall Warnhinweise an die Bevölkerung ausgesendet werden könnten. Der seit Mitte 2004 vorliegende Abschlussbericht favorisiert eine solche Nutzung. [...]
- using this for mischief would be rude/childish
- still it might not be the best idea to use DCF77 for emergency warning

Future uses of DCF77

DCF77 emergency warning clock

Conclusions

- spoofing the DCF77 signal is easy
- it can be done with hardware for $<$10 CHF
- amplification of the signal for greater range *would* be easy
- but if you try, you probably get your ass kicked very fast
- ATMega MCU’s are cool
- the soundcard can also be used for some fun stuff (besides playing sound)

Questions?

Further infos:

- Wikipedia: `http://de.wikipedia.org/wiki/DCF77`
- Physikalisch-Technische Bundesanstalt: `http://www.ptb.de/de/org/4/44/442/dcf77_1.htm`
- detailed description of DCF77: `http://www.ptb.de/de/org/4/44/pdf/dcf77.pdf`
- slides were created with LaTeX; plots were done with `octave` and `gnuplot`