Towards a traffic measuring surveillance system utilizing tire pressure monitoring systems

Jan Schulz[1], Yasin Walayat[2]

[1]Institute of Transportation Systems, German Aerospace Center (DLR), Berlin, Germany
[2]Institute of Aeronautics and Astronautics, Berlin Institute of Technology, Berlin, Germany

Introduction

Communication messages of tire pressure monitoring systems (TPMS) can be eavesdropped in order to detect and re-detect vehicles for measuring travel times. The European Union (EU) mandates TPMS starting November 2012, thus the dissemination level of motor vehicles coming with TPMS will theoretically increase during the next years up to 100 percent. First results on the way to a traffic detector utilizing communication signals of TPMS are presented below. Starting with the reception of TPMS signals, the demodulation and decoding afterwards, followed by an analysis of the message's bit field the sensor's ID and further information are extracted from the raw signal.

Approach

First tests were conducted with an aftermarket TPMS. If the moment of transmission is known – the sensor can be triggered by removing and reinstating the battery – the raw signal data is easy to find and to capture. Therefor the Universal Software Radio Peripheral (USRP) from ETTUS Research LLC in conjunction with GNU Radio was used.

Fig 1: Aftermarket TPMS sensor

Fig 2: Software radio platform USRP

Since the protocols do not rely on cryptographic mechanisms, the modulation scheme can be determined directly. The data transmission utilizes an amplitude shift keying in the 433 MHz band. The sensors employ Manchester encoding, which is a binary signaling mechanism that combines data and clock into bit-symbols.

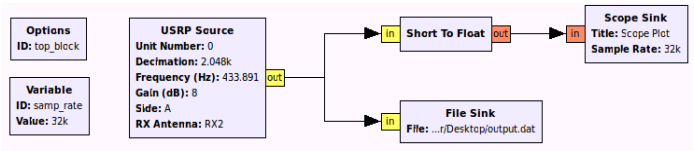

Fig 3: GNU Radio configuration

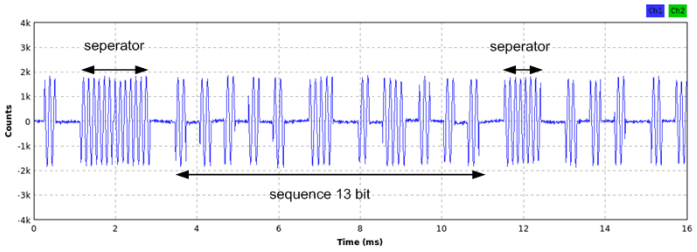

Fig. 4 Part of a TPMS communication message

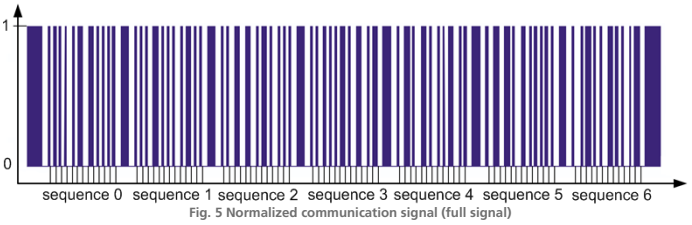

Fig. 5 Normalized communication signal (full signal)

sequence 0	0	0	0	0	1	1	0	1	0	0	0	0	Sensor ID
sequence 1	0	0	0	1	0	0	0	0	1	1	0	0	
sequence 2	0	0	1	0	1	0	1	1	0	0	1	1	
sequence 3	0	0	1	1	1	1	0	0	1	0	1	1	
sequence 4	0	1	0	0	1	0	0	1	1	1	0	1	Battery residue
sequence 5	0	1	0	1	0	0	1	0	0	0	0	0	Temperature
sequence 6	0	1	1	0	0	0	1	0	0	0	1	1	Pressure

Fig. 6 Decoded sequences of the communication signal

Decoding sequences 0 to 3 enables detection of vehicles at two different points to measure travel times.

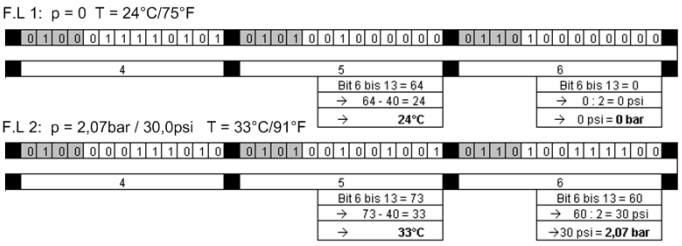

Fig. 7: Understanding the message's bit field

Outlook

- Antenna amplifiers will be tested to extend detection range,
- Different sensors of key manufacturers (e.g. VDO, Schrader, Beru) will be reverse engineered,
- A TPMS travel time demonstrator will be developed being able to trigger TPMS sensors.

Fig. 7: Typical TMPS sensor mounted inside a tire

Workshop is supported & funded under the 7th Framework Programme of the European Commission