EE 6900 – Software Defined Radio and Networking for the IoT

Kennesaw State University

Feb 23, 2023

Term Project: Proposal

Topic:

Usage of SDR to Decode Tire Pressure Monitoring System (TPMS)

Team:

Kevin Hardin

Koffi Onipoh

Instructor:

Dr. Billy Kihei

1. Project Overview:

The aim of this project is to design and implement a generic tire pressure monitoring receiver using a software defined radio (SDR) module (Nooelec NESDR Mini SDR & DVB-T USB Stick) and MATLAB. The scope of the project includes:

* Investigating frequency modulation schemes and data coding used in vehicles’ tire pressure monitoring systems (TPMSs)
* Implementing a TPMS receiver as a proof of concept
* Performing TPMS data capture
* Evaluating security risks associated with TPMS usage

1. Problem Statement

Maintaining the tires’ designed operating pressure is imperative to safety and fuel economy. Most modern cars are equipped with a TPMS which consists of tiny battery-powered wireless sensors mounted in the vehicle’s wheels and a base station embedded in the car’s control system. The tire pressure information collected by the sensors is wirelessly transmitted to the base station and displayed on the vehicle’s dashboard. TPMSs typically transmit on license free bands, such as 315 MHz, which can easily be received by an SDR module [1]. However, this raises security concerns: since the TPMS transmits over radio link, hackers can snoop the communications and send false tire pressure readings to motorists, which may reduce safety margins and increase the chance of a tire blowout [2].

Prior works have shown that TPMS communication interceptors can be built using advanced SDR devices such as the Universal Serial Radio Peripheral (USRP) receiver and trigger, which costs approximatively $2,000, or using a combination of a radio frequency (RF)-front end integrated circuit, microcontroller, and a demodulation circuit, averaging approximately $500 [3, 4]. Further findings have also demonstrated that TPMSs lack rigorous security and represent one of the entry points for automotive cyberattacks [5]. While these threats were validated in controlled lab environments, researchers have not proved that TPMS data can be captured while the vehicle is in motion at different speeds. Hence, sensor node mobility is yet to be considered, but is required to fully substantiate TPMS security threat concerns.

1. Proposed Approach

In this project we propose the design and implementation of a generic TPMS receiver using the low cost Nooelec Software Defined Radio device (NESDR, approximately $20) and MATLAB. Furthermore, we will investigate the capability of the receiver to pick up packets not only on idle vehicles in close proximity but also at a distance, as well as on moving vehicles at different speeds. The hardware setup and source code will be shared with the open-source community via outlets such as GitHub and Hackaday.

1. Design Method
2. Design Concept and System Architecture

There are 2 different types of TPMSs: indirect and the direct [6]. The indirect method uses the wheels’ speed variation as a basis to determine the pressure of the tires. Per the Ideal Gas Law (pv=nRT), pressure (p) and volume (ν) are directly proportional to each other. Hence, a tire with low pressure decreases in size (smaller diameter) and is forced to roll faster to maintain speed with the other tires. This speed discrepancy is measured and used to alert the driver to the low tire pressure. The sensors used with indirect TPMSs are typically less accurate and hardwired to the car’s control system. The direct TPMS method on the other hand, is achieved by embedding a pressure sensor in the tire and measuring the pressure of the air inside it. The data collected by the sensor is sent to the vehicle control system wirelessly. In this project, we are solely concerned with the direct TPMS (Fig 1). Capturing TPMS data requires knowledge of the individual electronic components involved the system, mainly the sensor, and the control system’s interface with the vehicle communication protocol, CANBUS.

A picture containing timeline

Description automatically generated

Figure 1: System Architecture

1. Sensor

TPMS sensors are often designed for low-power operation. They wake up periodically to measure and to transmit data using a periodic wake-up interrupt [7]. For testing purposes, we will investigate a way to trigger the sensor or wake-up it up from deep sleep when needed. There are also no standard TPMS communication protocols. Therefore, we will examine different communication protocols used by TPMS manufacturers and evaluate how well they interface with our NESDR receiver.

1. Data Processing

Depending on the TPMS sensor manufacturer, we anticipate different modulation and demodulation schemes will be used, with the most notable ones being Amplitude Shift Keying (ASK) and Frequency Shift Keying (FSK). Post-processing data will reveal the message frame and format used for the TPMS sensors considered. MATLAB will be used to process, filter, and decode the data captured by implementing all the necessary signal processing circuits in software, such as demodulators and comparator circuits with positive feedback (Schmitt triggers) to clean up noisy signals and convert them to digital signals.

1. Sensor Node Mobility

As discussed earlier, being able to capture and process TPMS data with a minimal cost design is one of main targets of this project. Our second focus is to investigate and implement how TPMS data can be captured while the vehicle is in motion using the low-cost NESDR receiver. Although the receiver is equipped with a small antenna, we anticipate a higher performance antenna and power amplifier may be needed to intercept TPMS data at a distance and on moving vehicles. We foresee this step being challenging since prior works on wireless sensor’s network mobility have only shown promising results when mobile relays are included in the network, or when all network elements - sensors and receivers - move together [8]. In our case, the receiver will be stationary and ready to capture TPMS data from the moving vehicle. If successful, beyond TPMS security concerns, we see many positive applications for this feature, including V2X (vehicle-to-everything) uses.

1. Limitations:

The scope of the project does not include transmitting packets. Hence, it will not be possible to spoof TPMS packets, nor transmit false readings to vehicles’ TPMS receivers to further evaluate security threats. Packet capture is the focus of this project and will constitute proof that TPMS data can be easily obtained within different environmental contexts (i.e., moving vehicle, close vs. far proximity, etc.).

1. Assessment and Contingency Plans

One risk to this project is that there are no standard TPMS communication protocols. We will examine different communication protocols used by TPMS manufacturers and evaluate how well they interface with our NESDR receiver. However, both the transmitting frequencies and the encoding schemes used are unknown at this time. Additionally, should wireless security features exist, diligence and care must be taken to ensure that a failure to decode the signal is due only to the presence of those security features and not to a failure of the hardware or software to successfully detect and decode the information. This risk may be mitigated by sampling multiple types and makes of vehicles, which may use different direct TPMS sensors and therefore different wireless transmission schemes.

Another risk is the difficulty with which a TPMS sensor may be manually woken-up or triggered when needed. If unable to be manually triggered, this risk can be mitigated by running multiple trials to ensure that devices are automatically transmitting during the time when the NESDR receiver is actively recording data.

One final risk identified is that of detecting the TPMS data under different environmental conditions. In a worst-case scenario, this risk can be mitigated by narrowing the testing scope to only those cases during which data can be reliably captured.

1. Project Organization and Management
2. Work Distribution

Since we are situated in different geographic locations, all work will be done concurrently. We will meet online one day a week to discuss our findings and steer the project to meet its defined goals. We will submit regular updates to our instructor Dr. Kihei for his review and feedback.

1. Deliverables
   * Final report documenting all design and implementation work
   * Software or MATLAB code
   * Pictures and video recording of experimental setups
   * Power point presentation of the work
2. Cost

* Noolec NESDR $20
* TPMS sensor $35
* Miscellaneous $45
* MATLAB software Free (students’ privilege)

1. Gantt Chart



1. References:

[1] N. N. Hasan, A. Arif, M. Hassam, S. S. Ul Husnain and U. Pervez, "Implementation of Tire Pressure Monitoring System with wireless communication," 2011 International Conference on Communications, Computing and Control Applications (CCCA), Hammamet, Tunisia, 2011, pp. 1-4, doi: 10.1109/CCCA.2011.6031524.

[2] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity Attacks in Vehicular Sensors," in IEEE Sensors Journal, vol. 20, no. 22, pp. 13752-13767, 15 Nov.15, 2020, doi: 10.1109/JSEN.2020.3004275.

[3] D. K. Kilcoyne, S. Bendelac, J. M. Ernst and A. J. Michaels, "Tire Pressure Monitoring System encryption to improve vehicular security," MILCOM 2016 - 2016 IEEE Military Communications Conference, Baltimore, MD, USA, 2016, pp. 1219-1224, doi: 10.1109/MILCOM.2016.7795497.

[4] S. Malipatlolla, T. Feller and S. A. Huss, "An adaptive system architecture for mitigating asymmetric cryptography weaknesses on TPMs," 2012 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), Erlangen, Germany, 2012, pp. 221-226, doi:10.1109/AHS.2012.6268654.

[5] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, USA, 6.

[6] J. Han, X. Tang, C. Meng and Y. Liu, "Research on ABS and TPMS System Merging Technology," 2009 International Conference on Intelligent Human-Machine Systems and Cybernetics, Hangzhou, China, 2009, pp. 141-144, doi: 10.1109/IHMSC.2009.43.

[7] S. Y. Kim, C. S. Chae, I. Hwang, S. Lim, H. W. Choi and D. J. Kim, "Design of low power operational TPMS system," 2015 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), Victoria, BC, Canada, 2015, pp. 344-347, doi: 10.1109/PACRIM.2015.7334859.

[8] Basagni, S., Carosi, A. and Petrioli, C. (2008). Mobility in Wireless Sensor Networks. In Algorithms and Protocols for Wireless Sensor Networks (eds A.Y. Zomaya and A. Boukerche). https://doi.org/10.1002/9780470396360.ch10