EE 6900 – Software Defined Radio and Networking for the IoT

Kennesaw State University

Apr 03, 2023

Term Project: Milestone 3

Topic:

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

Team:

Kevin Hardin

Koffi Onipoh

Instructor:

Dr. Billy Kihei

**3.1 Setup MATLAB SDR environment**

100% complete

We have both downloaded, installed, and verified MATLAB and Simulink software required for this project. We utilized Exercise 2.1 in the RTL-SDR textbook to ensure that the installation was correct. See below for the installed environment verification:

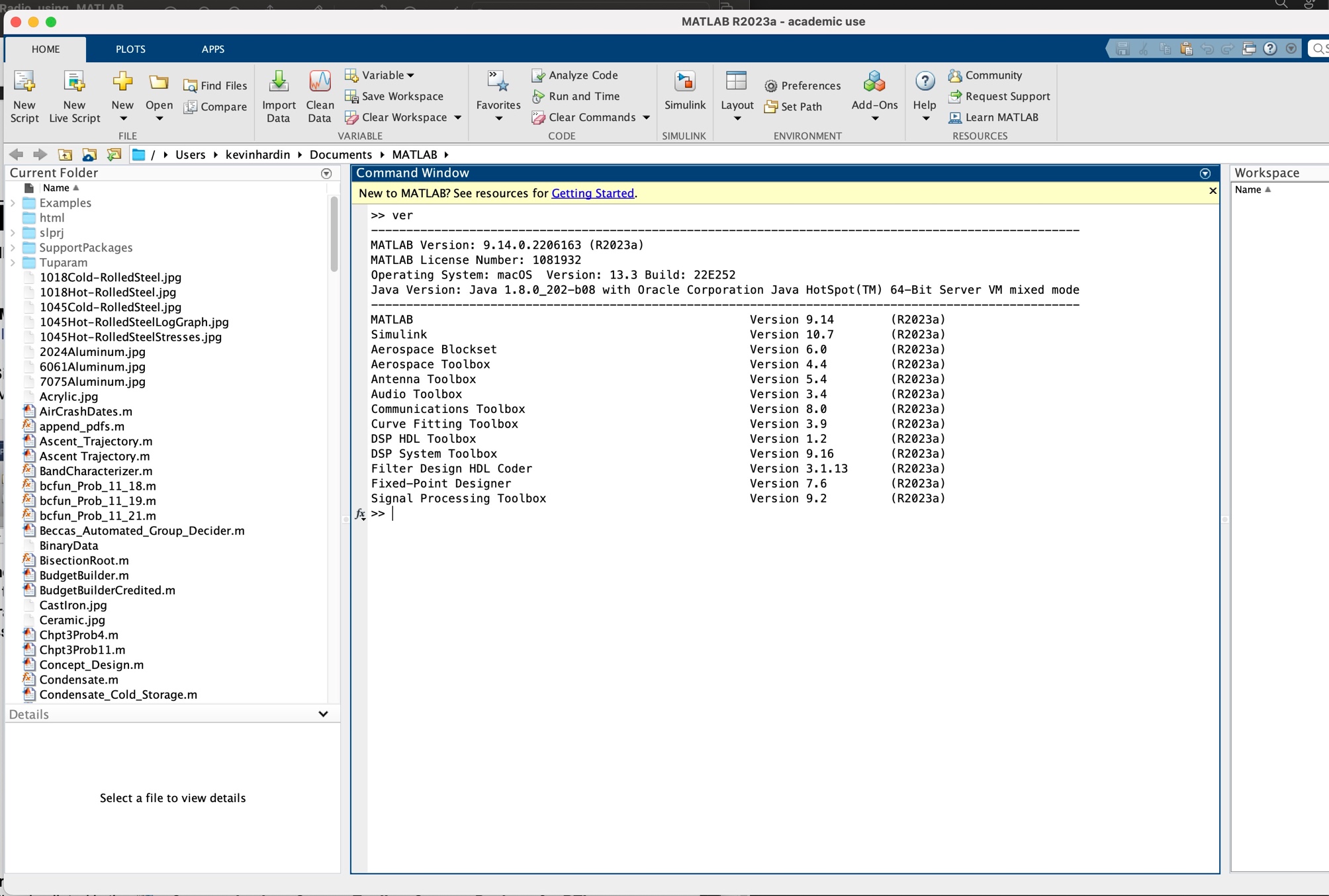


Figure : MATLAB Verification

**3.2 Record Data from Multiple Vehicles**

**80 % complete**

To get a better understanding of the tire pressure data captured by the SDR receiver, we created an initial testbed environment consisting of one vehicle - 2020 Jeep Grand Cherokee, equipped with 4 TPMS sensors, one on each tire. The IDs and frequencies of the sensors were determined by using Thindiag2, an onboard diagnostic and scanning tool (OBD2) for vehicles. The tool also affords the ability to wake up the sensors. The sensor IDs are recorded in below. This information was later used to design a suitable demodulator for converting the captured TPMS data waveforms into bitstream.Using the SDR receiver, the initial TPMS packets were captured by writing a small MATLAB script and setting the SDR tuner frequency to 433 MHz. shows the captured data spectrum.

| Table : TPMS data recorded with Thindiag2, scanning tool | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Vehicle** | **TPMS Sensors** | | | | |
| Jeep GC (2020) | **Type** | **Frequency**  **(MHz)** | **Position** | **ID** | **Tire Pressure**  (PSI) |
| Citroen | 433.92 | Left Front | 938FDE0B | 41 |
| Citroen | 433.92 | Left Rear | 938FDE32 | 40 |
| Citroen | 433.92 | Right Front | 938FE97D | 41 |
| Citroen | 433.92 | Right Rear | 938FDE42 | 41 |

Chart, line chart

Description automatically generated

Figure : FFT spectrogram of captured TPMS data

Additional models of car will be tested, and the data and results conglomerated to bolster the dataset. This will occur in the coming weeks. This task is behind schedule due to testing having taken longer than anticipated. The due date has been extended to 4/10 to enable the thorough use of multiple makes, models, and years of vehicles. However, this is imperative to the project and will not endanger the schedule of the project overall.

**3.3 Begin Data Analysis**

**30% Complete**

We started by creating a Simulink model for analyzing and processing purposes that can also store the data. We used the ‘Save RTL-SDR Data’ block from the receiver’s library in MATLAB. The resulting model is shown in . The raw IQ data recorded will need to be demodulated, filtered, and decoded.

Diagram

Description automatically generated

Figure : Simulink Model

**Demodulation**:

To demodulate the signal, it’s important to know the modulation scheme used. We passed the signal through a few well-known receivers such as Audacity (<https://www.audacityteam.org>). Other applications such as rtl\_433 () allowed us to obtain more complete information on 433 MHz devices transmitting in the area. We determined that FSK (Frequency Shift Keying) was used for the Citroen sensor tested. This means that the symbols are encoded by the change of signal frequency, so we will consider a central frequency with a positive and negative deviation using a binary FSK (BSFK) constellation diagram. However, as shown on , the tire pressure read by the receiver using rtl\_433 did not match the actual pressure values in tires. This will be further explored. This task is on track and due to be completed 4/16.

A picture containing calendar

Description automatically generated

Figure : TPMS sensor signal captured with SDR device using rtl\_433

**4.1 Create Scripts to Extract Data Content**

**50% Complete**

Following, steps described in the “*Software Defined Radio Using MATLAB & Simulink and RTL-SDR*” book, we wrote the following script () to extract the data from the SDR receiver:

%IMPORTING RTL-SDR DATA OBJECT

obj\_rtlsdr = import\_rtlsdr\_data(...

'filepath', 'rtlsdr\_data.mat', ...

'frm\_size', 4096, ...

'data\_type', 'single');

%INITIALIZING SDR OBJECT AND GETTING SAMPLING RATE

rtlsdr\_data = step(obj\_rtlsdr);

rtlsdr\_data\_fs = obj\_rtlsdr.fs;

%CREATING SPECTRUM ANAYZER OBJECT

obj\_spectrum = dsp.SpectrumAnalyzer(...

'SpectrumType', 'Power density',...

'FrequencySpan', 'Full',...

'SampleRate', rtlsdr\_data\_fs);

%SETTING PARAMETERS

rtlsdr\_frmtime = 4096/rtlsdr\_data\_fs;

run\_time = 0;

sim\_time = 10;

%LOOPING WHILE RUNTIME IS LESS THAN SIMULATION TIME

while run\_time < sim\_time

rtlsdr\_data = step(obj\_rtlsdr);

step(obj\_spectrum, rtlsdr\_data);

run\_time = run\_time + rtlsdr\_frmtime

end

Figure : **m-script to extract and read captured TPMS data form the receiver**

**This task is on track.**

**4.2 Create Scripts to Build Graphs**

**30% Complete**

The above script () will also allow us to plot and view a spectrograph of the captured TPMS data. However, more scripts will be needed to show the output signal after it is demodulated, filtered, and decoded. This task is ahead of schedule and due to be completed 4/12.

**4.3 Begin Project Paper**

100% Complete

We downloaded the recommended IEEE paper template. We have added the title, introduction, and are working on additional sections as we complete the work required for them.

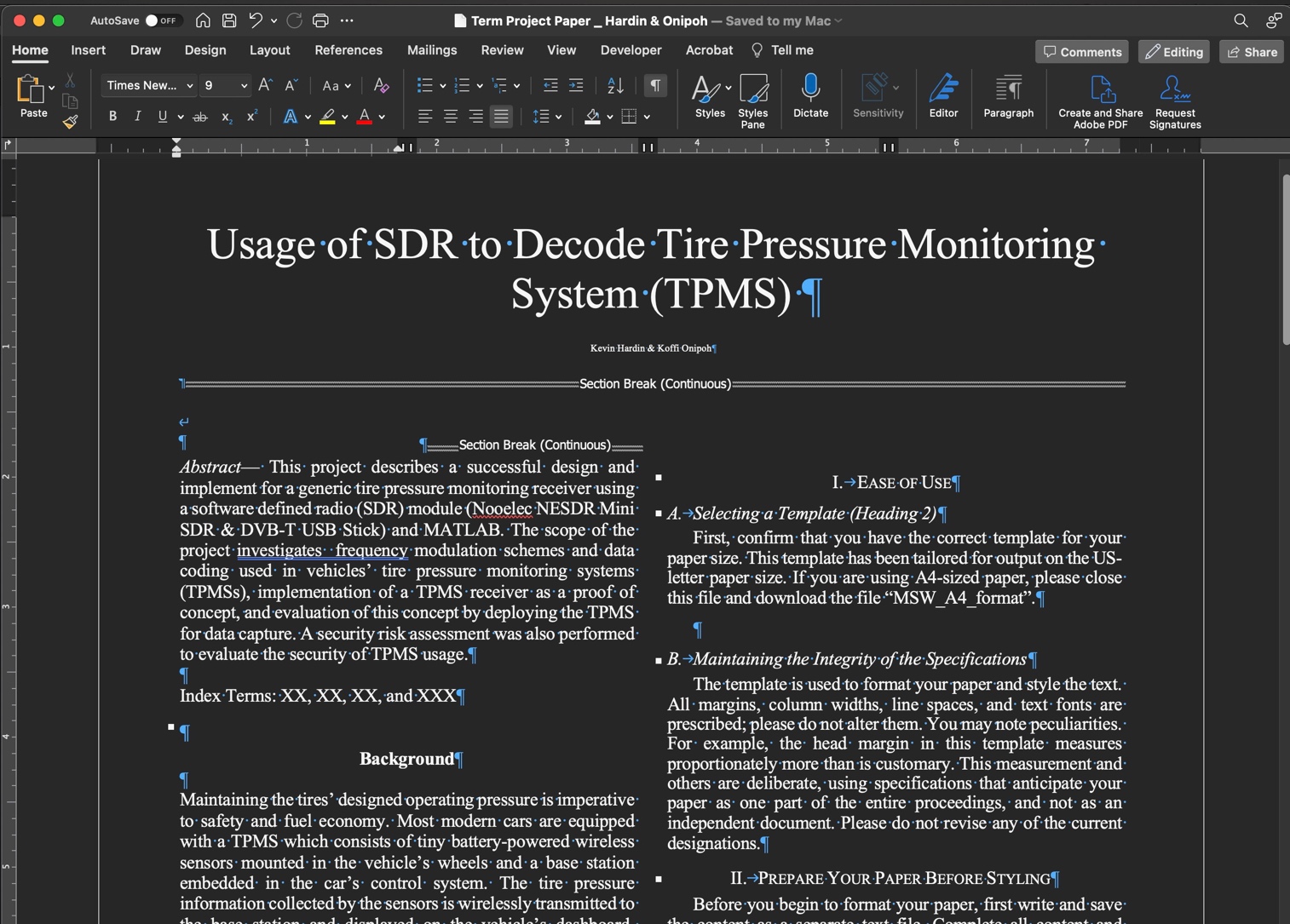
****

Figure : Early Term Paper Draft

**4.4 Begin Project Presentation**

0% Complete

As more data is accumulated and graphed, it will be added to the presentation. This will take place in the next few weeks. This task is not scheduled to begin until 4/13.

**5.1 Project Paper**

15% Complete

See item 4.3. Project paper has been started, and we will continue to write and edit it in the coming weeks, with a final draft being completed on 5/1 as outlined in the updated Gantt chart on the following page ().

**Updates to Proposal Expectations**

Beyond minor corrections to the testing schedule to accommodate additional vehicles and test conditions, most tasking has gone according to the proposal. However, expectations and hopes remain guarded with respect to being able to receive and demodulate a range of TPMS sensors, as well as whether or not some data may be encrypted from certain sensors. Additionally, if different modulation schemes are used beyond FSK, the ease with which we can read the data may be impacted.



Figure : Updated Gantt Chart

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