# Review of Radar Spoofing Research Papers

Project Authors Name: Farris Nefissi
Project Evaluator Name: Vedran Beganovic

- Guidelines to review the report for Question 1-3 below: https://dl.acm.org/journal/dgov/reviewer-guidelines
- Guidelines to review the code artifacts for Question 4-8 below: https://conferences.sigcomm.org/sigcomm/2022/cf-artifacts.html

Field Code Changed

## 1. Summary

Provide a brief summary of the project in your own words.

This paper explored the similarities and differences of spoofing approaches in two papers:
*mmSpoof: Resilient Spoofing of Automotive Millimeter-wave Radars using Reflect Array (Vennam 2023)*
*MadRadar: A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars (Hunt 2023)*
Additionally, a spoofing simulation was implemented in the report, initially as a part of a URP with Professor Jain. mmSpoof was described, which uses a novel reflector array that allows the attacker to avoid needing perfect synchronization with the victim. MadRadar was defined as using a “black box” approach for real-time parameter estimation. The maximum median error for mmSpoof was <0.05% and <0.03% for chirp slope in MadRadar. Both mmSpoof and MadRadar demonstrate that spoofing is effective against automotive FMCW radars and emphasize the need for countermeasures.

## 2. Strengths

Provide strengths or positive aspects of the project.

The report is very well organized. The strengths and weaknesses between mmSpoof and MadRadar were well described. The simulation was well done, and spoofing is clearly shown in Figure 8. The report addresses a topic that is highly relevant in the current era, as radars are increasingly used in autonomous driving applications. Spoofing can create dangerous conditions on the road, and by developing spoofing techniques, effective anti-spoofing methods can be discovered.

## 3. Weakness

Provide any weakness or aspects that can be further improved.

One aspect that could be improved is the better integration of the simulation with the rest of the report. It is not clear what function the simulation serves beyond serving as a proof-of-concept (Of the 12 figures in the paper, Figures 5 and 8 are from the simulation). An implementation that addressed a weakness in mmSpoof or MadRadar would have been more insightful for spoofing applications.

## 4. Documentation: Is the artifact/code sufficiently documented?

Rate from 0% to 100%, where 0% means "documentation is completely insufficient" and 100% means "documentation is absolutely sufficient". If you need to assess both a dataset and tools, please take the average and comment below. In assessing tools, please consider if they are easy or difficult to install/set up and get to run. In assessing datasets, please consider if the meta data is sufficient.

Choices are:

- **1.** 0%
- **2.** 20%
- **3.** 40%
- **4.** 60%
- **5.** 80%
- **6.** 100%

### Documentation: Comment on/explain your choice above:

The code is very clearly documented. There are function header comments, and many calculation steps have comments. Also, there are useful print statements, such as “Simulation complete.”

## 5. Completeness: Do the submitted artifacts/code include all of the key components described in the report?

Rate from 0% to 100%, where 0% means "does not include any key components" and 100% means "includes all key components".

Choices are:

- **1.** 0%
- **2.** 20%
- **3.** 40%
- **4.** 60%
- **5.** 80%
- **6.** 100%

### Completeness: Comment on/explain your choice above

The code includes all necessary components in the main script. The code also includes graphing capabilities. However, I would modularize the code and parcel out plotting, different spoofing approaches, etc., into separate files.

## 6. Exercisability: Do the submitted artifacts/code include the scripts and data needed to run the experiments described in the paper, and can the software be successfully executed?

Rate from 0% to 100%, where 0% means "the scripts/software cannot be successfully executed and/or no data is included" and 100% means "the artifact includes all necessary scripts/software and data, and scripts/software (if present) can be successfully executed".

Choices are:

- **1.** 0%
- **2.** 20%
- **3.** 40%
- **4.** 60%
- **5.** 80%
- **6.** 100%

### Exercisability: Comment on/explain your choice above

The code environment is in Python, specifically scientific Python, with libraries such as NumPy. The user must have a Python interpreter and the correct libraries installed. Otherwise, it might have been better to package the code into an .exe file or an Electron app.

7. **Results attainable: Does the artifact/code make it possible, with reasonable effort, to obtain the key results from the artifact/code?**

   Rate from 0% to 100%, where 0% means "no results can be obtained" and 100% means "all results can be obtained".

   Choices are:
   - **1.** 0%
   - **2.** 20%
   - **3.** 40%
   - **4.** 60%
   - **5.** 80%
   - **6.** 100%

   **Results attainable: Comment on/explain your choice above**

Figures 5 and 8 in the paper can be generated using the provided code. Additionally, the range and velocity spoofing calculations are printed at the end of the simulation.

8. **Results completeness: How many key results of the paper/report is the provided code meant to support?**

   Rate from 0% to 100%, where 0% means "the artifact is meant to support no key results" and 100% means "the artifact is meant to support all key results".

   Choices are:
   - **1.** 0%
   - **2.** 20%
   - **3.** 40%
   - **4.** 60%
   - **5.** 80%
   - **6.** 100%

   **Results completeness: Comment on/explain your choice above**

The simulation component accounts for about 20% of the report. The code supports those specific key results.

Reviewer Team Name: Vedran Beganovic, Signature: Vedran Beganovic

Reviewer Team member2 Name, Signature: N/A