Sensor Jamming Detection and Mitigation Techniques

Dana Lombardi
School of Engineering and
Computer Science
Oakland University
Rochester, Michigan
Email: lombardd@mail.gvsu.edu

Justin Gluck
School of Engineering and
Computer Science
Oakland University
Rochester, Michigan
Email: justin@awesome.com

Brett McIsaac
School of Engineering and
Computer Science
Oakland University
Rochester, Michigan
Email: geekman3454@gmail.com

***Abstract*—The abstract goes here.**

I. Introduction

The autonomous vehicle or the 'self-driving car', once thought to be a distant technology of the future, is fast becoming a soon to be reality as a form of transportation. The technology promises to make driving safer, lessen traffic in busy cities and to improve upon the general driving experience, to name just a few of the benefits.

One of the crucial aspects that make autonomous vehicles a possibility is sensor technology. Sensors allow a vehicle to become aware or "see" their surroundings. Sensor technology necessary for autonomous driving will likely vary from manufacturer to manufacturer but would probably include ultrasonic, radar, LIDAR, GPS, camera sensors and light sensors at the very least. These sensor types are not only limited to self-driving cars, this technology is used in many other areas such as unmanned aerial vehicles(UAVs) or drones, use a lot of similar technology in order to sense its surroundings and location.

Autonomous vehicles must not only keep the passengers of the car safe but also not cause harm to any other cars, pedestrians or anything a vehicle could come into contact with. Due to this fact, there is a heavy burden placed upon this technology to function without fail. This means that sensor technology within the vehicle cannot be defective and this includes not being susceptible to malicious attacks or accidental attacks. One of the biggest threats sensors face in autonomous vehicles is *sensor jamming*.

It is necessary to first have a clear idea of what sensor jamming is. Sensor jamming is typically defined as any outside party or entity that is intentionally sending or causing interference to signals being sent or received to sensors during autonomous sensor communication[1][2]. Although there are different types of jamming attacks that are possible, they will likely fall under this broad definition [2]. Jamming is typically done with a device that will send signals flood the sensor with false data that misrepresents the surroundings or overwhelms the sensor causing it to fail. Additionally, jamming can be done through blocking the signals to and from the sensor. Various types of sensor jamming will be discussed in a later section.

A. Mission Statement

For this paper, our initial research goals were to determine possible sensor jamming *detection* and *mitigation* techniques for sensors within autonomous vehicles. Stopping or mitigating the effects of sensor jamming is crucial for functionality, safety, and widespread adoption of autonomous technology. Throughout our research, we wanted to also put into practice and perform testing and analysis of techniques ourselves in addition to analyzing other researched sensor jamming detection and mitigation techniques.

B. Context of Research Area

The focus and context in which we performed our research was on sensors and their usage within autonomous vehicles. Although many of the jamming detection and mitigation techniques are applicable to many types of sensors, we focused upon ultrasonic sensors, especially in our own testing and analysis.

There are a few reasons for this, the first being that autonomous vehicles use ultrasonic sensors for close range detection of objects to assist with parking, adaptive cruise control and traffic jam assist[3]. These are very important features to for safety in autonomous vehicles, as well newer non-autonomous vehicles that include some variation of these features, and if these are sensors are jammed, functionality is severely impacted. Failure can cause danger to passengers and vehicle surroundings. A second reason ultrasonic sensors had more focus was due to the relative low price and availability of these sensors to use for testing. In this paper, we will discuss further how an ultrasonic transducer(HC-SR04) used with an Arduino Uno was used during testing to gather data and provide a proof of concept to our hypothesis that jamming attacks that cause objects around a vehicle to be hidden from ultrasonic sensors can be done with cheap and readily available equipment.

In addition to the testing that was done, several types of jamming detection and mitigation techniques were researched and analyzed. Detection and mitigation techniques studied were *frequency hopping*[1][4], *signal verification protocols*[5][2], and the *filtering/extraction of jamming signals*[4][6].

C. Terminology

This section defines commonly used terminology throughout the paper.

II. Sensor Jamming Attack Models

There are various ways in which a sensor can be jammed. Because of this jamming attacks can be split up into subcategories. This section includes some of the most common types jamming came across throughout the research process.

- **Constant Jamming:** A constant jamming attack is one that operates by emitting a constant stream of random interfering signals the target sensor. This type of attack typically doesn't wait for any communication from the sensor, the attack is consistent and constant while it is happening. This type of attack can block any legitimate signal traffic from communicating with the sensor[6].

- **Deceptive Jamming:** A jamming device tricks the sensor by sending packets or signals to the sensor. The sensor believes this to be a real packet and will switch into a receiving state. By continuously sending these normal signals to the sensor, the sensor is unable to send signals because it is falsely stuck in a receive state[6].

- **Random Jamming:** A random jamming attack will oscillate between states of sleeping and awake. When a random jamming device is awake, it can operate as a constant jammer or a deceptive jammer. This is done to conserve energy and not have the jamming device powered on at all times[6].

- **Reactive Jamming:** The three previous jamming attacks typically target the entire frequency or channel the sensor is operating on. A reactive jamming attack is different in that it will remain idle while listening and scanning traffic until there is activity on the operating frequency band and the jammer will then be able to match and attack that sensor's signals[1][6].

III. Related/Previous Works

Orient readers with most relevant studies.
Explain how it's related to our approach
How our Study builds upon previous works.
There have been numerous studies on sensory jamming within autonomous technology. Three of the top studies include, frequency/channel hopping, signal verification algorithms, and filtering of the jamming signals. Each is discussed further below.

IV. Problem Overview

A. Problem Statement

B. Challenges of the Problem

1) Adversary Goals and Capabilities: **Unsure where to fit this in as of now, maybe won't need it's own section**

V. Our Contribution

A. Research Goals for Solutions

1. Detect when sensor is being jammed 2. Immediately work to mitigate any jamming 3. Allow sensor to continue to function despite attacks

B. Running our own Simulation/Testing

1. Proof of Concept 2. Proof of Interference of sensors(does the way this works affect its reliability?)

C. Analysis and Evaluation

1.How do we sense an attack or interference is happening? 2. What is the best way to alert drivers? 3. What is a consequence of such an attack?

VI. Jamming Detection and Mitigation Techniques

Description of different types of jamming detection and prevention from research. How we were able to simulate or evaluate it's effectiveness.

A. Group Experimentation and Testing

1) Proof of Concept:
2) Computer Experiment:
3) Setup:
4) Results:

B. Frequency Hopping

Frequency Hopping(FH) is the process by which the sensor continuously changes or 'hops' the frequency channel signals are being sent or received on. Hopping patterns will be unknown to attackers and likely unpredictable as well[6]. If FH is happening quickly, jamming devices will be unable to react quickly enough to match to the current operating frequency, thus evading any jammers that were scanning the sensor such as reactive jammers[6].

FH can also help prevent jamming that happens when there is 'cross-talk' between sensors. This occurs when sensors of the same type, operating on the same frequency are close enough that they are sending signals to or receiving signals from the nearby sensors accidentally[8]. This causes sensors to receive false data or accidentally jam other sensors. If these near-by sensors have signals FH enough it is unlikely they would interfere with each other. Meng. et. al. proposes a strategy to mitigate this type of jamming by transmitting ultrasonic signals in pseudo-random pulses within varying frequencies. The sensor then waits on an expected, returned signal corresponding to the pseudo-random pulse and frequency that was sent out[8].

C. Signal Verification Algorithms

-How is it detected -How do we mitigate -does sensor continue to function?

1) Signal to Noise Ratio:

2) Send to Delivery Ratio:

3) Measuring Signal Strength:

D. Filtering Techniques

-How is it detected -How do we mitigate -does sensor continue to function?

VII. Security Analysis

A. Feasibility

B. Scalability

C. Effectiveness in Achieving Goals

VIII. Conclusion

Best way to alert driver?

IX. Recommendation for Future Research Focus

X. Individual Contributions

Acknowledgment

The authors would like to thank...

[7] [1] [8] [4] [6] [5] [2] [9] [10] [3]

REFERENCES

[1] F. Gringoli, N. Facchi, and D. Berger, "Demo: a testbed to evaluate frequency-hopping anti-jamming techniques in ieee 802.11," *Proceedings of the 9th ACM international workshop on Wireless network testbeds, experimental evaluation and characterization (WiNTECH '14)*, pp. 85–88, 2014.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05)*, pp. 46–57, 2005.

[3] [Online]. Available: https://audi-illustrated.com/media/audi-q2-illustrated-copy-e2e59972-8419-4b52-a382-2ed7a6c67cc5/content_image/3749/teaser_38-Q2-FAS-Sensor-uebersicht-E_4_3.jpg

[4] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Extracting jamming signals to locate radio interferers and jammers," *Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '12)*, pp. 257–258, June 2012.

[5] G. Kar, H. Mustafa, Y. Wang, Y. Chen, W. Xu, M. Gruteser, and T. Vu, "Detection of on-road vehicles emanating gps interference," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*, pp. 621–632, 2014.

[6] M. Liechti, V. Lenders, and D. Giustiniano, "Jamming mitigation by randomized bandwidth hopping." *In Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT '15).*, no. 11, December 2015.

[7] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan., "Understanding and mitigating the impact of rf interference on 802.11 networks," *Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '07)*, pp. 385–396, August 2007.

[8] Q. Meng, Q. Liang, and J. Li, "Frequency-hopping pseudo-random pulse width modulation to eliminate crosstalk of sonar sensors in mobile robots,." Beijing, China: IEEE, October 2006.

[9] [Online]. Available: http://arduino-info.wikispaces.com/file/view/sonarbasic.jpg/495545920/633x284/sonarbasic.jpg

[10] [Online]. Available: https://i.stack.imgur.com/X2dK8.jpg