Cybersecurity in Vehicular Networks: Enhanced Roll-Jam Attack and Jamming Detection

A Thesis

Presented in Partial Fulfillment of the Requirements for the Degree Master of Science in the Graduate School of The Ohio State University

By

Zachary David Depp, B.S.

Graduate Program in Electrical and Computer Engineering

The Ohio State University

2023

Master's Examination Committee:

Can Emre Koksal, Advisor

Eylem Ekici

Abstract

Over the past several decades, vehicle manufacturers have been increasingly adding technological improvements to the vehicles they release to the public. While these advancements are well-intentioned, especially in regards to vehicular safety and security feature upgrades, they have dramatically increased the cyber attack surface for malicious actors. These attackers are taking advantage of software-defined radios to assist in their methods. In this thesis, we aim to improve upon a well-known vehicular replay attack, the roll-jam attack, as well as develop an machine learning-assisted algorithm to allow a target vehicle to detect if it is being jammed.

The traditional vehicular roll-jam attack is an effective means to gain access to the target vehicle by jamming and recording key fob inputs from a victim. However, it requires specific knowledge of the attack surface, and delicate tuning of software-defined radio parameters. We have developed an enhanced version of the roll-jam attack that uses a known noise signal for jamming, in contrast to the additive white Gaussian noise that is typically used in the attack. Using a known noise signal allows for less strict tuning of the software-defined radios used in the attack and allows for digital noise removal of the recorded input to enhance the replay attack.

Next, we focus on jamming detection from the perspective of the target vehicle. If the vehicle is able to detect that it is being jammed and takes appropriate countermeasures, then the roll-jam attack and other attacks like it would be thwarted. We

have created a jamming detection algorithm that is able to use physical layer data to accomplish detection. Our first algorithm focuses on estimating the approximate distance from a potential attacker using received signal power as the primary metric. Our second method involves collecting empirical data and training a machine learning algorithm to perform the jamming detection.

To my wife Maggie, and our daughter, Reagan. You are my biggest supporters and motivators, and none of this would be possible without you.

Acknowledgments

I have to give my outstanding thanks to my advisor, Dr. Can Emre Koksal. Coming from a non-traditional undergraduate experience, he gave me the ability to explore my interests in a way that was profoundly refreshing. No idea was too unorthodox, and no stone was left unturned. My gratitude goes out to Dr. Halit Bugra Tulay, who I was lucky enough to shadow in his final semester of his PhD program and learned the basis for my own research. Thank you for continuing to support me even after your graduation. I would also like to extend my thanks to Dr. Eylem Ekici, for his valuable feedback and serving on my thesis committee.

I thank the Transportation Research Center (TRC) for funding my research, and for their valuable support in validating our research through our meetings and conversation.

Vita

June 22, 1992 ..... Born - Ohio, USA

2014 ..... B.S. Department of Electrical Engineering and Computer Science, United States Military Academy

Publications

Research Publications

Zachary Depp, Halit Bugra Tulay, C. Emre Koksal "Enhanced Vehicular Roll-Jam Attack using a Known Noise Source". Symposium on Vehicles Security and Privacy (VehicleSec) 2023 , 27 Feb 2023.

Fields of Study

Major Field: Electrical and Computer Engineering

Table of Contents

List of Tables

Table **Page**

List of Figures

Chapter 1: Introduction

As the automotive industry continues to innovate and integrate technology into vehicles, the need for robust cybersecurity measures becomes increasingly vital. As a result, vehicle cybersecurity has become a critical area of research and development. The rapid advancement of connected cars and autonomous vehicles has created new challenges, as these vehicles are susceptible to cyber-attacks that can potentially compromise the safety of passengers, vehicles, and the public at large.

1.1 Software-Defined Radio and Vehicles

Software-defined radio (SDR) is a powerful tool that can be used to analyze wireless communication between components in a vehicle, and between vehicles themselves. SDR technology allows for the capturing and decoding of wireless signals, enabling researchers to investigate the behavior of various components and identify potential vulnerabilities. One of the key advantages of using SDR is its flexibility. With the ability to change frequencies and protocols on the fly, we can quickly switch between different wireless communication standards to capture and analyze data. This flexibility is essential when dealing with modern vehicles, which often use a wide range of communication standards such as Wi-Fi, Bluetooth, and cellular networks. Another advantage of SDR is its ability to capture and decode wireless signals in

real-time. This enables us to perform live analysis, allowing for the identification of potential vulnerabilities as they occur. By analyzing the behavior of wireless communication in real-time, we can detect anomalies that may indicate the presence of an attack, allowing for timely responses to mitigate the risk of compromise.

1.1.1 Attacking Vehicles with SDR

While SDR technology can be used for analyzing wireless communication in vehicles, it can also be used by attackers to compromise the security of these vehicles. SDRs have been demonstrated to be incredibly threatening to Internet of Things (IoT) devices, and modern vehicles with their abundant wireless systems are no exception [1].

One common attack is the man-in-the-middle (MITM) attack, where an attacker intercepts and alters communication between two devices. In the vehicular context, this could involve an attacker intercepting communication between a car's sensors and its control unit, allowing them to manipulate sensor readings and potentially cause dangerous malfunctions. SDR technology can be used to perform this attack by capturing and altering wireless signals in real-time.

Another attack is the denial-of-service (DoS) attack, where an attacker floods a vehicle's wireless communication channels with high volumes of traffic, causing the vehicle's systems to become unresponsive or malfunction. This type of attack can be particularly dangerous when directed at safety-critical systems such as the vehicle's brakes, steering, or tire pressure management systems (TPMS).

A third attack is the replay attack, where an attacker captures a legitimate signal and replays it to perform unauthorized actions. For instance, an attacker could

capture the signal from a key fob and replay it to unlock a car's doors without the owner's knowledge. This attack is particularly effective against modern vehicles that use rolling code encryption, which can be easily bypassed using SDR technology. This type of attack is commonly known as the roll-jam attack, because it uses an SDR to jam the target vehicle to bypass its rolling code security. Enhancing this attack in particular will be the first focus of this thesis.

1.1.2 Defending Against SDR Attacks on Vehicles

Defending against SDR attacks on vehicles requires a multifaceted approach that includes both technological and organizational measures. With the increased availability of SDRs to the general hobbyist and consumer population, many of these attacks are becoming more prevalent and harder to detect and defeat.

One of the key strategies for defending against SDR attacks is to use strong encryption methods. Modern encryption standards such as AES or RSA are much more difficult to bypass using SDR technology, making it much harder for attackers to capture and replay signals without the use of more advanced techniques. Such encryption methods have been presented as a potential means to secure the otherwise exploitable TPMS messages [2]. Additionally, manufacturers can use secure communication protocols such as TLS or SSL to protect wireless communication channels from attacks such as MITM attacks.

Organizational measures can also be effective in defending against SDR attacks. Manufacturers can establish strong security policies and procedures, including regular

security audits and penetration testing, to identify and mitigate potential vulnerabilities. Additionally, manufacturers can collaborate with security researchers and experts in the field to identify new threats and develop effective countermeasures.

Another strategy is that manufacturers can design vehicles with physical security measures that can prevent attackers from gaining physical access to critical components. This may involve using tamper-resistant components or designing systems with redundancy and fail-safes that can prevent unauthorized access or manipulation. Without physical access to these components, attacks could be easily defeated.

One of the key strategies is to implement intrusion detection and prevention systems that can detect and respond to attacks in real-time. These systems can be designed to monitor wireless communication channels for unusual or suspicious activity and automatically block or quarantine any potential threats. Intrusion detection systems can be particularly effective when combined with machine learning algorithms that can learn to recognize patterns of behavior and identify new threats as they emerge, which will be the second focus of this thesis.

Chapter 2: The Enhanced Roll-Jam Attack

Fundamentally, the vehicular roll-jam attack works by having an adversary target a victim whose vehicle they want to access without authorization. In the attack model, the adversary jams and records the signals transmitted from a key fob to access a target vehicle. It was developed specifically to defeat the rolling code security measures that modern vehicles use to protect against normal replay attacks. The vehicular roll-jam attack has been around publicly since at least 2015, and has proven to be situationally effective at gaining unauthorized access to modern vehicles that use key fob rolling code security [3]. The increased availability of SDRs to hobbyists have made this attack well-known, although it has not fundamentally changed since it first emerged, and car manufacturers have yet to implement any kind of real mitigation strategy against it.

The attacker uses one or more SDRs to send a jamming signal to the vehicle to block the reception of legitimate key fob inputs, while simultaneously recording that legitimate input, typically an unlock signal, with the intention of replaying it at a later time to gain access to the vehicle, as seen in Figure 2.1. This attack bypasses the rolling code security of the key fob, which synchronizes key fob inputs with a cryptographic counter that is shared with the vehicle's onboard computer. The vehicle will interpret the replayed input as legitimate since it has yet to receive

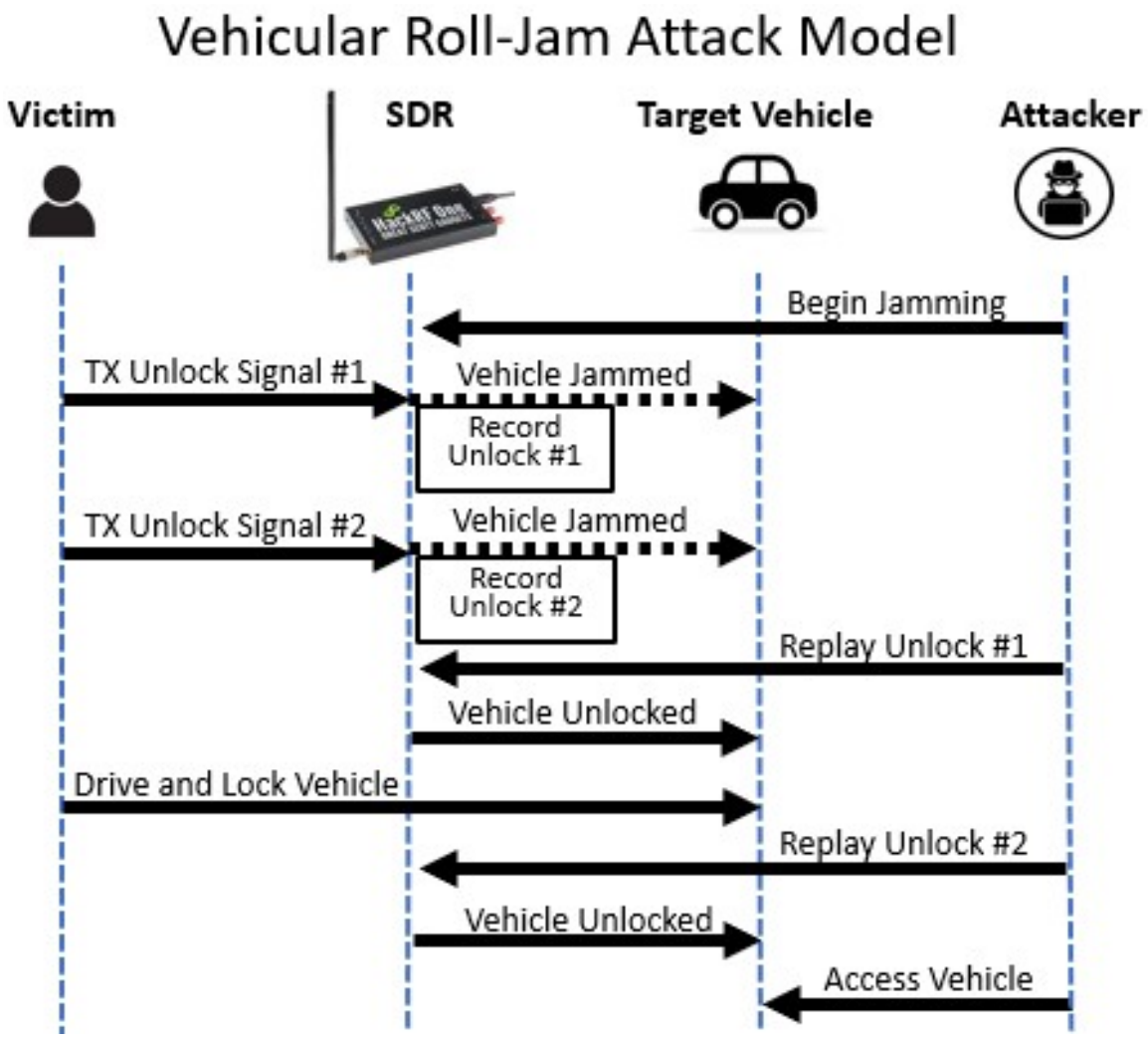


Figure 2.1: Roll-Jam Attack Model.

that message, and unlock the vehicle. There have been several proposed defense strategies against this attack, including adding timestamps to the rolling code, but vehicle manufacturers have yet to make any widespread changes [4], [5].

While the roll-jam is a well-known attack, it still requires information from the victim before the adversary can execute the attack. The attacker needs to know the exact frequency that the vehicle key fob operates at, and then must adjust their SDR

to jam either slightly above or below that frequency and then must find an appropriate level of transmit gain for the noise signal such that the vehicle is jammed, but not so much that it renders the captured key fob signal unusable in the subsequent replay attack. Certain modern vehicles are also starting to incorporate anti-theft security features which can prevent the vehicle from receiving any key fob inputs if it receives an already used code. This means if the attack is not executed perfectly the first time, further attempts are blocked. This tuning and configuration of the SDR can take a significant amount of time, during which the attacker could lose their window of exploitation.

In this paper, we propose an enhanced roll-jam attack that uses a known noise sequence at the exact same frequency as the key fob. Unlike the traditional roll-jam, our new attack does not require prior knowledge of the key fob signal. It conceptually works for any signal, and even those with modern encryption practices with rolling codes. Our new attack method allows us to jam the vehicle at the exact frequency with even higher transmit power than the traditional roll-jam attack. Subsequently, we record the key fob input and perform noise removal techniques to obtain the original input signal. The obtained signal is later replayed to gain access to the target vehicle.

2.1 Enhancing the Roll-Jam Attack

One of the biggest setbacks with the traditional roll-jam attack is that it requires simultaneous jamming and recording within a relatively narrow bandwidth, usually 1.5MHz, in the spectrum of either 315MHz or 433MHz [6]. The jamming signal is usually additive white Gaussian noise (AWGN), as it is effective at jamming over

a narrow bandwidth and is easy to generate with most SDR software [7]. If the attacker jams at a frequency further than 1.5MHz from the key fob operating frequency, however, they run the risk of jamming outside of the receive window of the vehicle, and not jamming the vehicle at all. If the attacker jams too closely to the key fob frequency, they risk distorting the recorded signal to the point of being unable to replay it later.

Modern vehicles have been shown to be incredibly vulnerable to being wirelessly jammed by a variety of techniques [8]. In our approach, the attacker uses a known noise sequence transmitted at the same frequency as the key fob for jamming. Since the noise sequence is known, the attacker uses noise removal techniques to maintain a sufficient signal-to-noise ratio (SNR) that enables the signal to be replayed. By removing the noise component from the recorded message, the attacker could replay the attack from much further away and with greater efficiency. The noise source being known also gives the attacker greater flexibility in the amount of power they use to jam the target vehicle. As the noise signal is known to them, they will be able to identify and digitally remove noise sources transmitted at higher power than the traditional attack. This enables the attacker to have greater confidence that the target vehicle is in fact being jammed from receiving legitimate messages, and potentially interrupting the attack. Figure 2.2 details our enhanced roll-jam model.

The attacker begins jamming the target vehicle with the known noise signal as soon as they are in position to wait for the victim to attempt to unlock their vehicle. Once they capture the unlock signals, they immediately digitally remove the noise component from them, and then carry out the replay attack using the enhanced messages. Due to the noise removal process, the vehicle is more likely to accept the

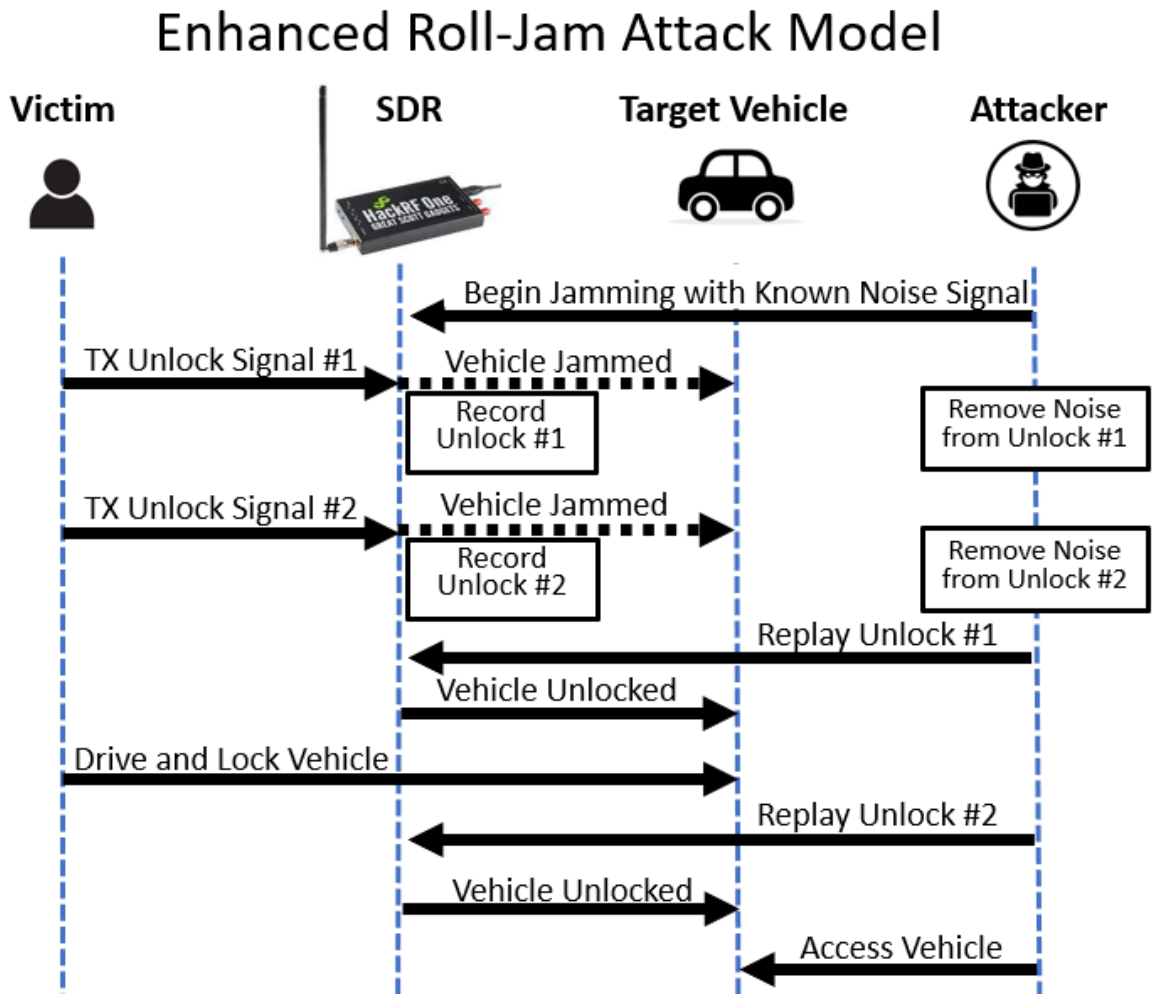


Figure 2.2: Enhanced Roll-Jam Attack Model.

replayed signals as legitimate, and give the attacker access to their target. We propose to use a legitimate key fob message as a template for the noise source. However, simply capturing and replaying old signals multiple times is not a viable option, due to anti-theft security features on certain modern vehicles. These features automatically lock-down the car and its accompanying key fob if the car receives previous rolling code messages. These constraints meant we had to record a legitimate signal, and then modify it sufficiently such that it was efficient at jamming the vehicle and was easily identifiable by the attacker.

2.2 Evaluating the Enhanced Roll-Jam Attack

2.2.1 Creating the Known Noise Source

The first step to generate the known noise signal was to capture several legitimate key fob messages from a modern vehicle that used rolling code security. For the purposes of this research, a 2020 Kia Sorento EX was used, and the software Universal Radio Hacker (URH) was used in conjunction with a Great Scott Gadgets HackRF One as our SDR for collecting, analyzing, and replaying data [9]. Figure 2.3 and Figure 2.4 show several captured and demodulated signals from the target vehicle's key fob in hexadecimal form.

This key fob operates in the 433MHz range, specifically at 433.92MHz, and uses frequency-shift keying for modulation. URH has a helpful auto-detection setting that

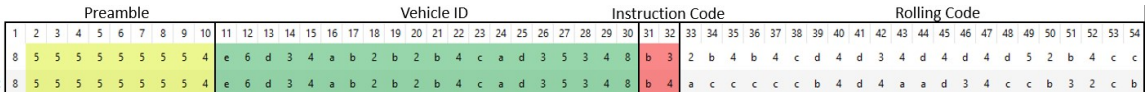


Figure 2.3: Breakdown of demodulated hexadecimal key fob message.

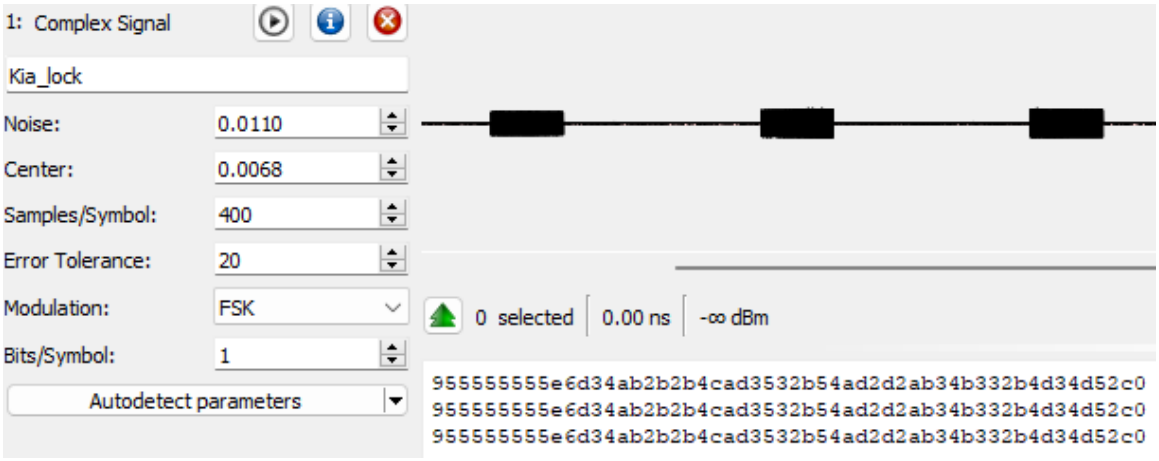


Figure 2.4: Demodulated key fob message from 2020 Kia Sorento.

attempts to determine the signal parameters as long as the SNR is sufficiently high enough.

The key fob transmits three identical message pulses, each separated by approximately 120ms. Figure 2.3 shows the demodulated frames of data consist of a preamble, vehicle ID number, instruction code, and the rolling code. Each individual message is 54 hexadecimal digits long, and each button press on the key fob generates three new identical pulses. From here, URH has a function which allows generation of new data frames by using captured data and copying the modulation technique, carrier frequency, sample rate, and symbol size. Now we are free to change any of the bits in the message, and then compile a brand new payload consisting of specific data. To make visual analysis of the decoded signal easier, we decided on generating a known noise payload consisting entirely of hexadecimal 5, as seen in Figure 2.5. The actual demodulated bit values of the known noise signal do not matter as long as they are

Figure 2.5: Known noise signal generated from legitimate message.

known to the attacker and do not match an old rolling code message from the vehicle. From here, we can transmit this signal indefinitely from the SDR to act as the jamming signal in the enhanced attack.

2.2.2 Executing the Enhanced Roll-Jam Attack

After generating the known noise sequence, we can execute the entire enhanced roll-jam attack. The first part of the attack is carried out almost identically to the traditional roll-jam. The attacker selects a target vehicle, the 2020 Kia Sorento in this case, and transmits the known noise signal to jam the vehicle from one SDR while simultaneously recording the legitimate key fob input. The differences are that instead of a randomly generated noise source, the known noise source is used, and the noise is transmitted at the exact frequency of the key fob, 433.92MHz. The URH

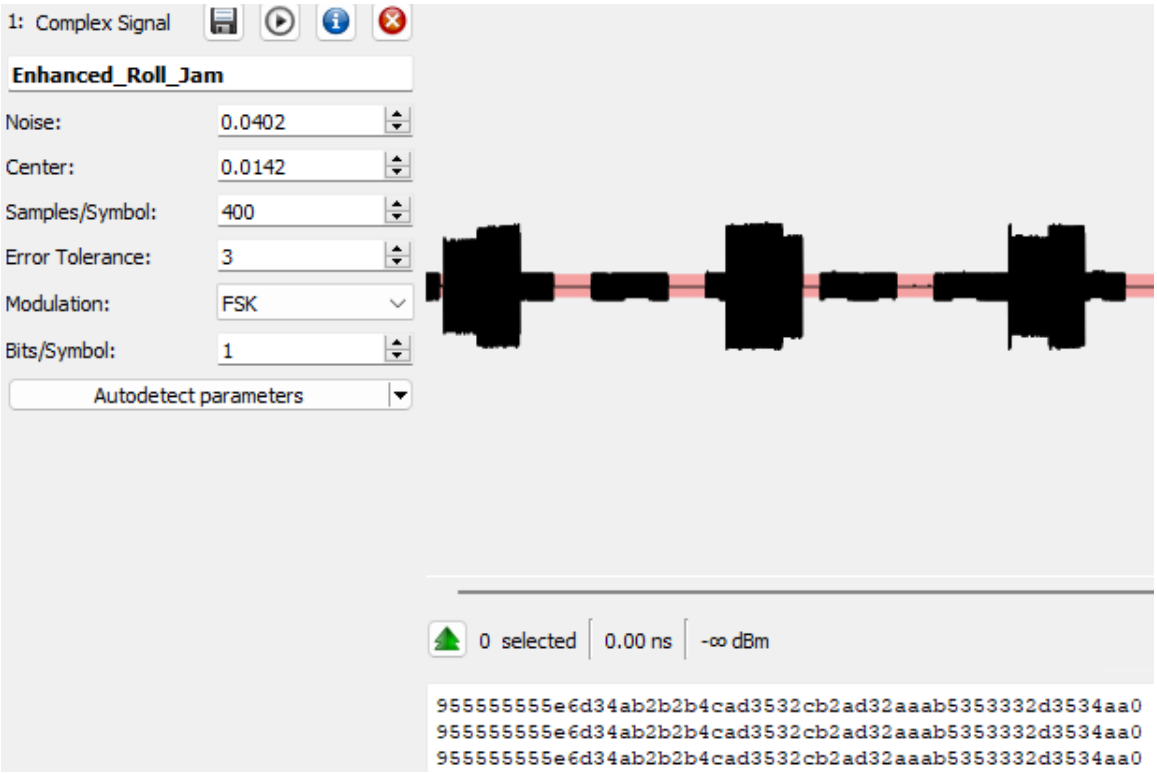


Figure 2.6: Key fob message recorded while jamming with known noise source.

output in Figure 2.6 shows what this captured input looks like alongside the known noise signal.

For our experiments, the jamming SDR was placed directly next to the receiving SDR, and the key fob was placed close to the SDRs in order to keep our transmitting power at a reasonably low level, as seen in Figure 2.7. After recording the key fob input while jamming, the URH autodetect function was able to automatically isolate the key fob message from the known noise signal. Even if the autodetect function had not worked, the attacker would be able to visually locate the captured message and could then manually adjust the parameters to fully isolate the input. With the

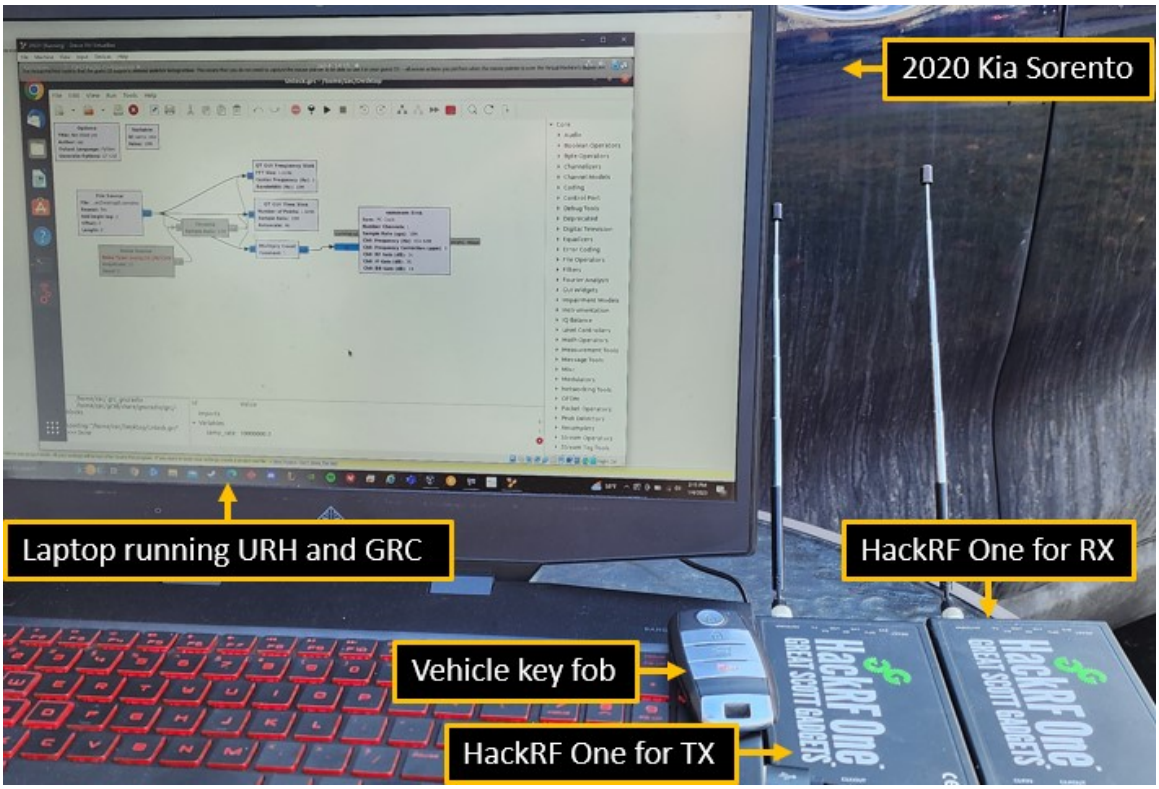


Figure 2.7: Executing the enhanced roll-jam on a 2020 Kia Sorento.

noise floor set to the maximum amplitude of the known noise source, the attacker is left with the key fob message alone in its entirety.

The next step is to generate a new payload for the replay portion of the attack using URH, with a similar method as was used to generate the known noise source. After removing the noise in URH, the outcome is a message signal with the entirety of the noise component removed, as seen in Figure 2.8. The attacker can then transmit this noise-removed signal when they want to access the victim's vehicle. With the noise component completely removed from the payload, the SNR is improved significantly, and the attacker has the ability to replay the message with more flexibility.

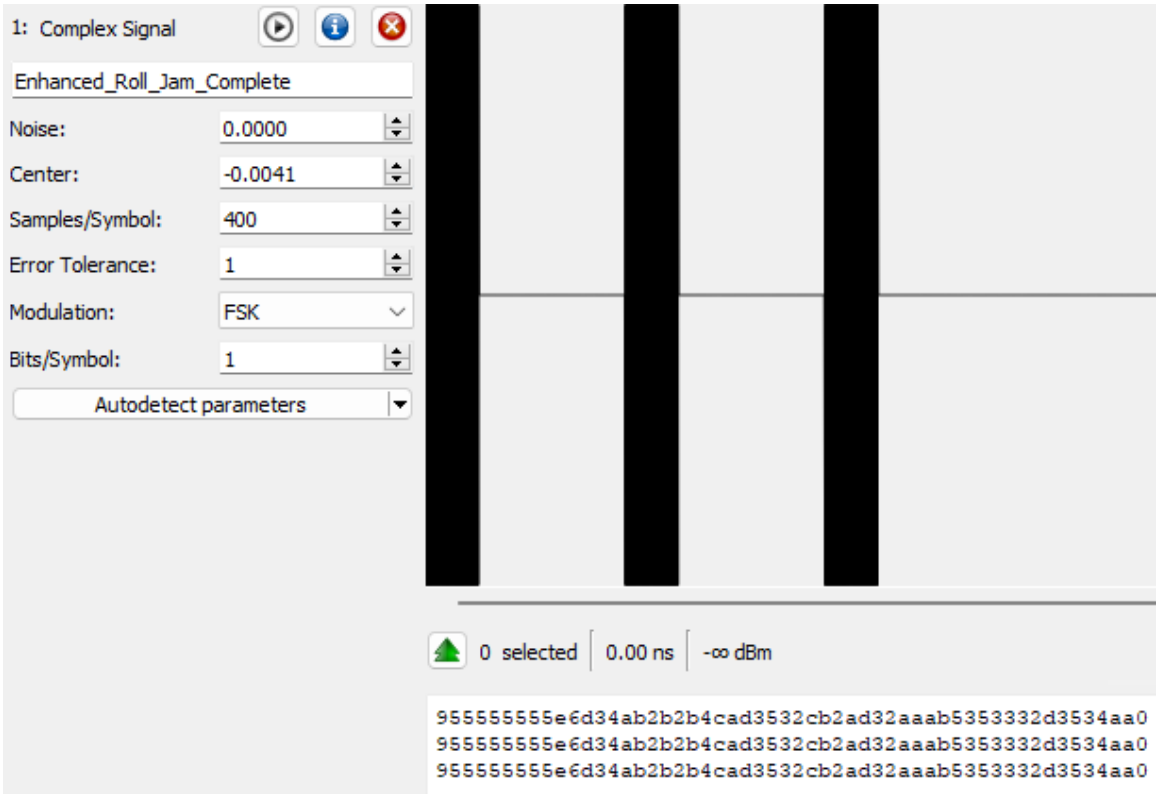


Figure 2.8: Recorded key fob message with noise component removed.

In the traditional roll-jam attack, the replayed message still contains the added noise component that the attacker used to jam the vehicle. While the jamming is at an adjacent frequency to the key fob frequency, the sidebands generated can be significant, and makes the replay attack difficult to alter if the attacker needs to transmit with additional power. The enhanced attack allows for the message to be replayed at even higher power than the original key fob recording, and from a further range than the key fob's operating distance.

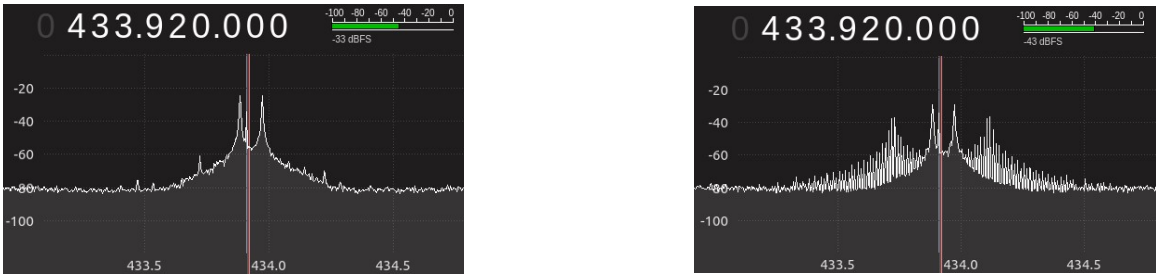
Our experiments have demonstrated that this attack works on every vehicle we have had available for testing. This includes vehicles with key fob frequencies operating in the 315MHz range, and that use amplitude-shift keying for modulation rather than frequency-shift keying. The attack performs with highest efficiency when the jamming SDR is closer in proximity to the vehicle than the recording SDR and key fob, but the attack also works well even when the jamming SDR, recording SDR, and key fob are co-located. Figure 2.9 shows the frequency domain signals before and after jamming. This attack has been tested and verified successful on the following modern vehicles from the United States, Asian, and European markets:

- 2013 Ford F-150
- 2015 Honda HRV
- 2015 Nissan Rogue
- 2015 Audi A3
- 2020 Kia Sorento
- 2020 Toyota Tacoma

The traditional roll-jam works situationally on these vehicles as well, however, significant configuration changes to the SDR are required for every different vehicle. With the enhanced attack, all the adversary needs to know is the key fob frequency and then they can implement the attack with a high rate of success.

2.2.3 Comparing the Traditional and Enhanced Attacks

To directly compare our enhanced roll-jam attack with the traditional version, we used the Linux-based GNU Radio Companion (GRC), a framework that contains



(a) (b)

Figure 2.9: a) Frequency domain key fob signal before jamming b) Key fob signal while jamming with known noise source.

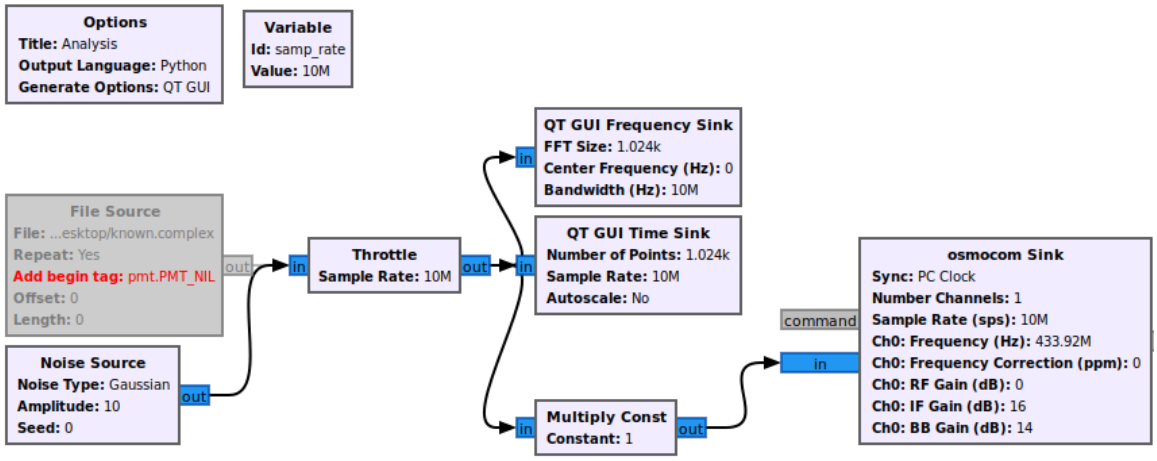


Figure 2.10: GNU Radio Companion Block Diagram used for Analysis.

signal processing blocks for SDRs [10]. Figure 2.10 depicts the flow chart derived for this analysis.

GRC contains a block for generating AWGN, which we use to compare against our generated known noise source. For our first analysis, we measure the average SNR of a captured key fob signal when using AWGN and the known noise sequence to jam. We also measure the SNR of the complete enhanced roll-jam attack after we

have used URH to remove the noise, leaving just the key fob message. While the SNR of the attack is not completely indicative of its success, attacks with a higher SNR have more flexibility to replay the attack under conditions favorable to the attacker, such as being able to unlock the target vehicle from a further distance, and giving the attacker more confidence that the attack will succeed.

The HackRF operates in half-duplex, so two were used to collect this data, one for transmitting the noise source using GRC, and one for collecting the key fob input using URH. Both SDRs used the same low power settings as seen in Figure 2.10 in the osmocom Sink block. For each noise type, ten consecutive unlock signals were sent from the key fob and captured by the SDR connected to URH. An average SNR was calculated using the analysis tools available in URH, and the results are shown in Table 2.1. We observe that using AWGN as the noise source provided slightly better results than when just using the known noise sequence alone. However, when implementing the noise removal in the enhanced attack, the SNR is significantly higher, as the only noise component remaining is the ambient noise of the environment. This allows the attacker to easily replay the signal from further away and with a high degree of confidence.

For the next analysis, we compare the highest level of transmit gain for each noise type that still allows for noise removal in URH. The setup for data collection is the same as the previous analysis, and we simply raise the transmitter power in GRC until URH could no longer automatically detect the captured key fob input apart from the noise.

The HackRF has two transmitter gain settings that can be adjusted, a radio frequency (RF) gain and an intermediate frequency (IF) gain. The RF gain controls

Table 2.1: Signal-to-Noise Analysis

	Attack Type		
	AWGN Noise Source	***Known Noise Source***	***Enhanced Attack***
SNR (dB)	8.786	7.899	40.115

the front-end amplifier of the HackRF, and it is either on or off with gain values of 0dBm and 14dBm, respectfully, and the IF gain can be set from 0dBm to 47dBm [11]. Initial testing confirmed that both the AWGN and known noise sequence begin effectively jamming the vehicle at the same transmit power from the same distance. For this analysis, the front end amplifier was turned on for both noise sources, and the IF gain was adjusted for comparison.

The AWGN source had a maximum transmit gain of 17dBm before the signal became undecipherable by URH. The key fob signal is still visibly recognizable on the recording, but above 17dBm the noise distorts the signal beyond recognition. Any recorded sequence above this gain threshold is not suitable for noise removal in URH. The known noise sequence, however, could be transmitted at up to 26dBm before URH was unable to detect a message, as seen in Figure 2.11. This 9dBm difference represents the ability to transmit the known noise sequence with approximately eight times more power than the AWGN signal. This allows the attacker to jam at higher power and have greater confidence that the vehicle is in fact being jammed.

While executing the entire enhanced attack takes longer than the traditional roll-jam due to the noise removal and signal generation process in URH, attackers would generally perform the collection part of the roll-jam attack first, and then execute

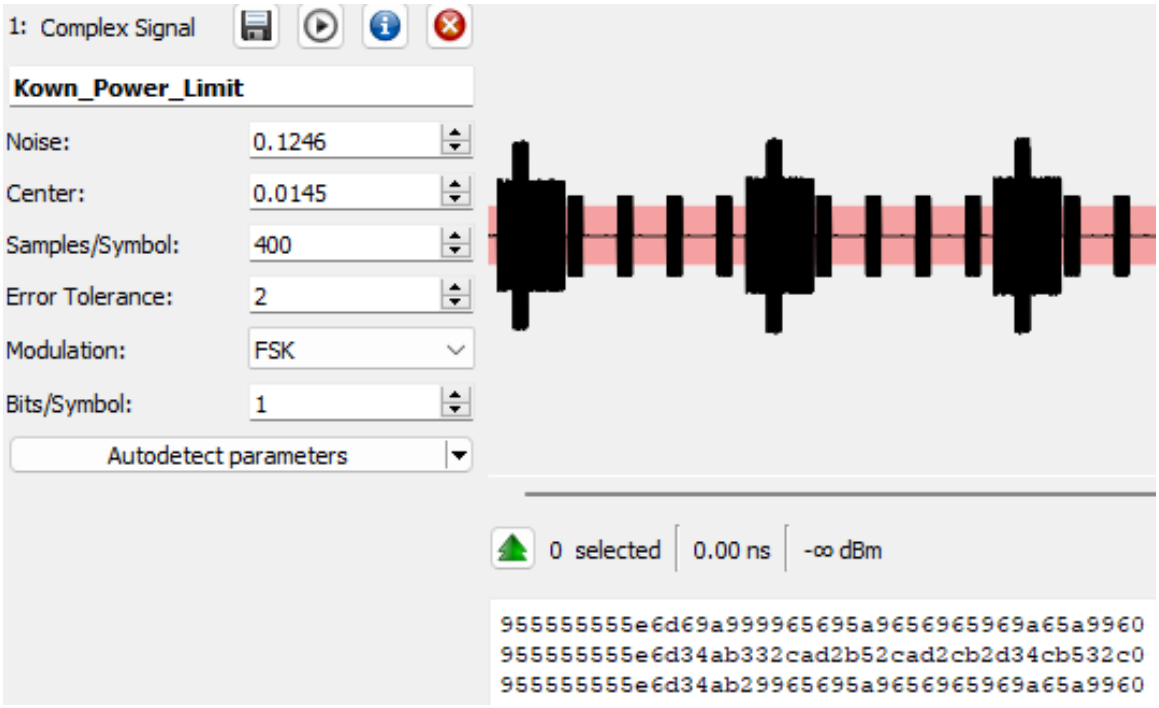


Figure 2.11: URH detects key fob message with known noise transmitted at 26dBm.

the replay portion of the attack at a later time when the vehicle is unattended. This means that there is no loss in attack efficacy as long as the replay occurs sometime after the collection process. The collection process itself is greatly improved by being able to jam the vehicle with an appropriate level of noise as soon as the attacker knows the key fob frequency.

Chapter 3: Jamming Detection

In the previous chapter, we demonstrated that wireless jamming attacks are a common threat to the security of modern vehicles, with attackers using radio frequency interference to disrupt communication between vehicle components and then using that disruption to carry out more advanced attacks. Detecting jamming attacks is essential for maintaining the safety and security of vehicles on the road. In this chapter, we will explore the use of SDR technology paired with machine learning for detecting jamming attacks on vehicles.

SDR technology is well-suited for detecting jamming attacks, as it allows for the monitoring and analysis of wireless signals in real-time. By analyzing wireless signals at the physical layer, we can detect unusual or unexpected patterns of behavior that may indicate the presence of a jamming attack. Additionally, SDR technology can be used to identify the frequency and intensity of the jamming signal, allowing for the identification of the source of the attack.

Detecting jamming attacks using SDR technology typically involves monitoring the wireless communication channels used by different components in the vehicle. In our case, we will be focusing on detecting jamming attacks such as the traditional and enhanced roll-jam attacks which target the key fob to vehicle communication link. Other research has shown that jamming detection and even localization is possible

with SDRs, however, they generally focus on using packet or bit error rate metrics for analysis [12] [13]. Our research is interested in performing the jamming detection while only using physical layer characteristics in order to simplify the detection process at the vehicle.

3.1 Distance-Based Jamming Detection

Our first model is based on calculating a distance estimation between the vehicle and the attacker or legitimate user by using the received signal power. The goal is to set threshold values for received power and then conduct distance estimation that will detect jamming when the estimated distance away remains constant over a period of time, which would be anomalous for a legitimate user. We assume that a legitimate user would either strictly get further away from their vehicle, in the case they had just parked and were pressing the lock button on the key fob, or get strictly closer to their vehicle over a period of time in the case that the owner was returning to their vehicle and was pressing the unlock button while approaching on foot. We also assume that if the vehicle receives more than 5 signals per second, or that the vehicle receive buffer is full for 5 seconds, that jamming is present. Figure 3.1 depicts the jamming detection model.

The basis for our distance estimation is using Friis equation, which is given by:

$$P_r = P_t + G_t + G_r + 20log(\frac{\lambda}{4\pi d}) \tag{3.1}$$

Where P_r is the received power measured at the vehicle, P_t is the power of the transmitted signal, G_t and G_r are the transmitter and receiver gains, respectively, and d is the distance between transmitter and receiver. λ is the wavelength of the

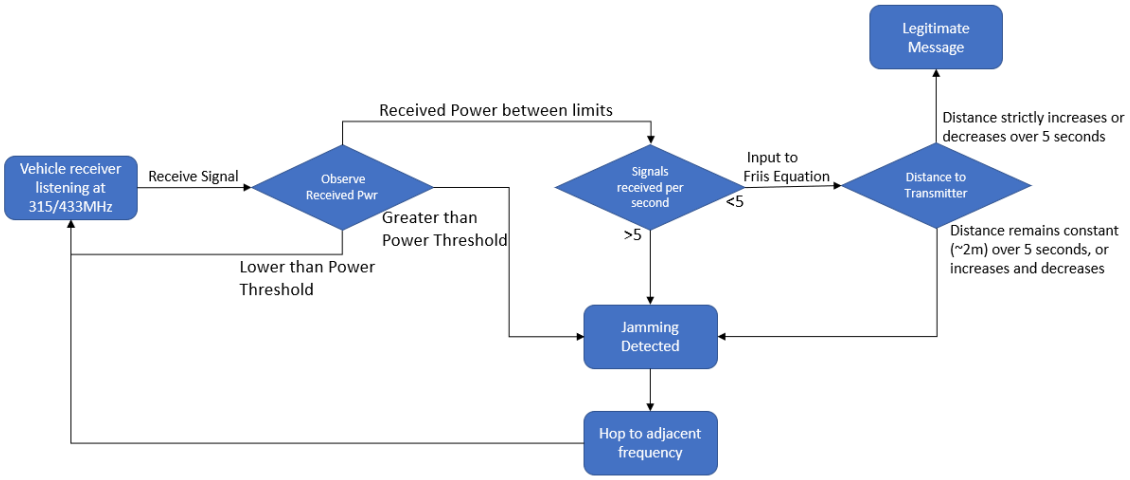


Figure 3.1: Distance-Based Jamming Detection Model.

signal, and for our purposes with signals in either the 315MHz or 433MHz range, the wavelength will be between approximately 0.7 and 1 meter. It has been shown that using Friis equation is a viable way to perform jamming detection and even localization, however, for our purposes we will reorganize the equation in order to solve for distance [12]. This gives:

$$d = (\frac{\lambda}{4\pi})10^{\frac{P_t+G_t+P_r+G_r}{20}} \tag{3.2}$$

While this cleans up the equation, at the vehicle receiver the only values it would have access to naturally are P_r and G_r. We assume that G_r would be roughly equal to G_t, which just leaves P_t to be found. Researchers in [12] used empirical data collection to estimate the received power at a range of distances, and we duplicate this effort for our work. With one HackRF receiving, we collect the SNR from key fob inputs and SDR jamming transmissions from increasing distances and then average them

together. This average will then become the P_t for our model. Table 3.1 shows the results of this empirical data collection.

With these averages we now have all of the data required to perform distance estimation between the vehicle and the unknown signal source. For a complete walk-through of the model, assume the vehicle receives a signal at 433MHz. If the signal falls below a certain SNR threshold the vehicle will continue to wait for a stronger signal. If the signal is greater than a set threshold, we immediately assume that we are being jammed and take appropriate countermeasures. The goal is to set this upper bound such that it would be impossible for a key fob and legitimate user to generate a signal that powerful, no matter how close they are to the receiver.

Assuming the signal then falls between the set upper and lower bounds, the vehicle then detects the rate of signals being received. If this signal rate is greater than 5 messages received per second our model would detect being jammed. The reason is that it is generally beyond human capability to send more than 5 key fob messages in one second, and thus would be more likely a signal generated from a digital source. To calculate this message rate, we use the typical key fob message length as the standard. In the case of the 2020 Kia Sorento from Chapter 2, this message length is 54 hexadecimal characters long, so for every 54 hexadecimal characters received we count one message. In the case of jamming being done with a signal that cannot be demodulated, the model will detect jamming if the vehicle's receive buffer is full for 5 seconds. If the signal passes all of these checks, the received power is then input into our Equation 3.2 to estimate the distance to the source. The last check is to analyze the signals received over a span of 5 seconds. Typically a legitimate user would be approaching or departing their vehicle when they are using the key fob to

Table 3.1: Empirical SNR Data

	SNR of Signal Source (dB)	
Distance (m)	***Key Fob***	***Jamming SDR***
5	-13.97	-22.42
10	-20.47	-23.57
15	-22.06	-25.25
20	-23.54	-26.89
25	-25.07	-28.31
Average	**-21.02**	**-25.29**

send messages. This would lead to either strictly increasing or strictly decreasing distance estimations. If, however, over this 5 second period the estimated distance remains constant within approximately 2 meters, or both increases and decreases, the model detects a jam. A jamming attacker would likely be in a fixed position during their attack, which would lead to a relatively constant distance estimation from the perspective of the vehicle. If the attacker is using more advanced jamming techniques, like modulating the power and frequency of their jamming signal, the estimated distance would not remain constant over the 5 second interval, but would instead both increase and decrease. In both cases our model would detect the presence of jamming and would take countermeasures.

3.1.1 Jamming Countermeasures

The main anti-jamming countermeasure we propose is to use frequency-hopping. Frequency-hopping has been used by the military for several decades and has proven to be incredibly successful at mitigating interference in a communications channel [14]. Two methods of frequency-hopping could be used in this model. In the first,

when the vehicle detects jamming, it either raises or lowers its receive window by a few MHz to attempt to avoid the jamming. For instance if the vehicle normally receives at 433MHz, it could hop to receive at 434MHz. This hop size would be easier to implement on the key fob, but would potentially struggle against a wide bandwidth jamming device. In the second method, the vehicle would instead hop to the alternative industrial, scientific, and medical (ISM) frequency band from the one it is currently using. In the United State both the 315MHz and 433MHz bands are used for vehicle key fobs, so the vehicle would simply swap to the band they are not currently using. This method would be more effective at mitigating a wide bandwidth jamming device, but would also be more difficult to implement between the vehicle and the key fob.

In the end, we determined that this model was interesting and absolutely held applicability, but wanted to create a more advanced model that could perform the jamming detection in a more streamlined manner with the assistance of machine learning.

3.2 Machine Learning-Assisted Jamming Detection

In recent years, researchers have developed advanced machine learning algorithms that can be used in conjunction with SDR technology to detect jamming attacks [1]. These algorithms can learn to recognize patterns of behavior in wireless signals and identify anomalies that may indicate the presence of a jamming attack. By combining SDR technology with machine learning algorithms, we can improve the accuracy and efficiency of jamming detection systems.

As in the first model, we wanted to use physical layer data as the primary input into our algorithm. Other research has been done in this area of jamming detection with machine learning, but have primarily used metrics like packet delivery ratio and bit error rate to train their model [15] [16]. We chose to use in-phase and quadrature (I/Q) data captured with an SDR to serve as the basis for our analysis and training data as is easy to generate and capture in GRC. We decided to create three classes of data to train the machine learning algorithm:

1. Vehicle being jammed
2. Vehicle not being jammed (steady state)
3. Vehicle receiving legitimate key fob message

Next, we set up our HackRF similarly as in Chapter 2.2.3 to collect data for each of these classes. For the jamming case, we put our two HackRFs next to one another and transmitted AWGN at low power from one while recording from the other. Next, for the no jamming or steady state class we simply isolated the HackRF and recorded the ambient noise signals in the spectrum. Finally, for the class where the vehicle is receiving legitimate key fob input we recorded with one HackRF while pressing unlock signals twice per second on the key fob. This data is easily captured in GRC using the block diagram in Figure 3.2.

We sampled at 2MHz for 10 seconds for each class to collect 20 million total I/Q samples each. In order to analyze the I/Q data we had to record the real and imaginary data as individual audio streams as seen in Figure 3.2, which we could then import into Matlab and recombine. From here, we divided each class of 20 million samples into 100 groups of 20 thousand samples in order to reduce the size of our

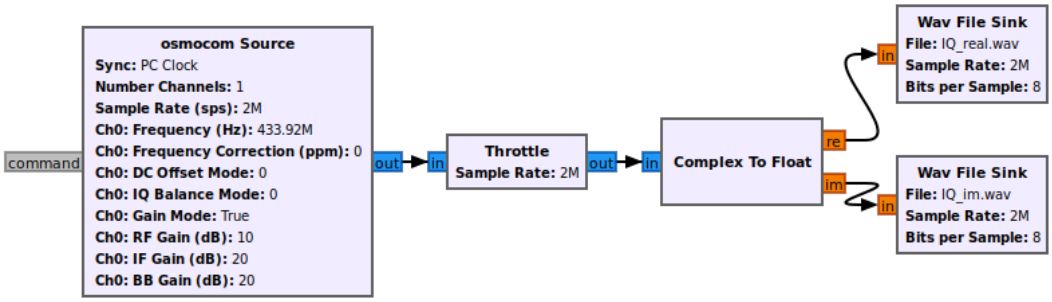


Figure 3.2: GRC Block Diagram for Capturing I/Q Data.

training set. For each of these sets of 20 thousand samples for each class we computed the mean, standard deviation, and variance, and then recorded these values into a 300x3 matrix. A plot of these metrics is in Figure 3.3.

The final step is to then import this training data into python and execute train a multiclass algorithm. For our research we used the open source python library and learning database scikit-learn [17]. After importing our data into python, we then

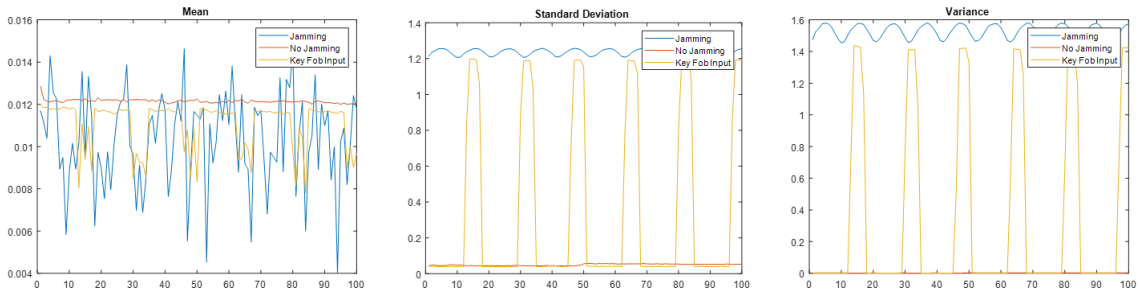


Figure 3.3: Mean, Standard Deviation, and Variance of the Training Data.

Table 3.2: Multiclass Algorithm Accuracy Results

Algorithm	***Accuracy***
AdaBoost	99.67%
Gradient Boosting	100%
Extra Trees	99.67%
K-Nearest Neighbors	94.67%
CART	99.67%
Naive Bayes	83.67%
SVM	99.67%

trained and tested our data using several multiclass algorithms, including one-vs-one, one-vs-rest, linear, and nonlinear algorithms. The top results of these trials are depicted in Table 3.2

Many of these well-known algorithms perform with a high degree of accuracy, but in particular, the gradient boosting classifier boasts a perfect accuracy rating. This is likely due in part to gradient boosting algorithms being adept at regression and classification on unclean data [18]. The high accuracy scores across the board suggests that the data is generally easily classified by many algorithms, however, in the case of vehicular security we want the accuracy as close to perfect as possible. In the real-world case, as in the first model, we would use frequency hopping as a mitigation technique in the event of a jamming event detected by our classifier.

Chapter 4: Conclusion and Future Work

In this thesis, we propose the enhanced vehicular roll-jam attack that uses a known noise source, and a machine learning-assisted jamming detection algorithm. We demonstrate the effectiveness of this enhanced attack on different vehicles using a software-defined radio. Specifically, we show a significant SNR improvement over the traditional roll-jam attack. This provides the adversary incredible flexibility to carry out the attack without requiring prior knowledge of the transmitted signal. While AWGN serves as an appropriate noise source for the attack, jamming becomes significantly more potent when using a noise source created and known by the attacker. Indeed, cryptographic security approaches will not be able to mitigate this new attack, as we have shown that the key fob signal can be decoded simultaneously during smart jamming in a full-duplex like operation. While cryptographic methods will not be able to thwart our new attack, we demonstrate a gradient boosting classifier able to detect vehicular jamming with a perfect accuracy. Once detected, the vehicle jumps to an adjacent frequency and successfully defends against any jamming attack. These types of attacks, however, will remain prevalent in our society as long as vehicle manufacturers are unable to update their security mechanisms to defend against them.

For our future work we would like to continue to develop defense strategies for cyber attacks on vehicular networks. Specifically we would like to continue our work on the machine learning-assisted jamming detection algorithm presented in this thesis. We believe there is room for improvement by adding additional classes of data and further broadening the training data used to train the classifier, as well as using statistical values beyond mean, standard deviation, and variance. We are also interested in the use of neural networks to defend against these attacks. One potential neural network could be trained to perform image processing on spectrograms generated by a vehicle's receiver to detect jamming. Another neural network could study the behavior of a key fob user over time, and develop a model that could detect anomalous behavior that deviates from the user's normal patterns. Ultimately, as the number of wireless vehicular networks increases, it is imperative that manufacturers and researchers continue to work together to identify and address potential vulnerabilities, implement effective defense strategies, and stay ahead of emerging threats, in order to ensure the safety and security of vehicles at rest and on the road.

Bibliography

[1] P. D. Hung and B. T. Vinh, "Vulnerabilities in IoT Devices with Software-Defined Radio," 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, 2019, pp. 664-668, doi: 10.1109/CCOMS.2019.8821711 (accessed Apr. 04, 2023).

[2] 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 (accessed Apr. 04, 2023).

[3] C. Kraft, "Anatomy of the Rolljam Wireless Car Hack," Make: DIY Projects and Ideas for Makers, Aug. 11, 2015. https://makezine.com/article/maker-news/anatomy-of-the-rolljam-wireless-car-hack/ (accessed Jan. 04, 2023).

[4] K. Greene, D. Rodgers, H. Dykhuizen, K. McNeil, Q. Niyaz and K. A. Shamaileh, "Timestamp-based Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems," 2020 IEEE International Conference on Consumer Electronics (ICCE), 2020, pp. 1-4, doi: 10.1109/ICCE46568.2020.9043039.

[5] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh and V. Devabhaktuni, "A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic," in IEEE Consumer Electronics Magazine, vol. 10, no. 1, pp. 101-108, 1 Jan. 2021, doi: 10.1109/MCE.2020.3012425.

[6] G. Nespral, "How to hack a car," Hackaday.io, Mar. 26, 2019. https://hackaday.io/project/164566-how-to-hack-a-car/details. (accessed Jan. 04, 2023).

[7] "Noise and dB — PySDR: A Guide to SDR and DSP using Python," pysdr.org. https://pysdr.org/content/noise.html (accessed Jan. 04, 2023).

[8] Y. O. Basciftci, F. Chen, J. Weston, R. Burton and C. E. Koksal, "How Vulnerable Is Vehicular Communication to Physical Layer Jamming Attacks?," 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), 2015, pp. 1-5, doi: 10.1109/VTCFall.2015.7390968.

[9] J. Pohl, "Universal Radio Hacker," GitHub, Mar. 22, 2022. https://github.com/jopohl/urh/ (accessed Jan. 04, 2023).

[10] "GNU Radio - The Free and Open Source Radio Ecosystem" GNU Radio. https://www.gnuradio.org/ (accessed Jan. 04 2023).

[11] M. Ossmann, "HackRF Documentation," hackrf.readthedocs.io, Sep. 22, 2022. https://hackrf.readthedocs.io/en/latest/index.html (accessed Jan. 04, 2023).

[12] K. Thanakan, K. Sapphaniran, T. Palasarn, P. Supnithi, W. Phakphisut and C. Sakorn, "Real-Time Jamming Detection and Position Estimation via Software-Defined Radio (SDR)," 2021 18th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 2021, pp. 280-284, doi: 10.1109/ECTI-CON51831.2021.9454678 (accessed Apr. 04, 2023).

[13] R. Bhojani, R. Joshi, "An Integrated Approach for Jammer Detection using Software Defined Radio," Procedia Computer Science, vol. 79, pp. 809-816, 2016. https://www.sciencedirect.com/science/article/pii/S1877050916002441 (accessed Apr. 04, 2023).

[14] D. L. Herrick, P. K. Lee and L. L. Ledlow, "Correlated frequency hopping-an improved approach to HF spread spectrum communications," Proceedings of the 1996 Tactical Communications Conference. Ensuring Joint Force Superiority in the Information Age, Fort Wayne, IN, USA, 1996, pp. 319-324, doi: 10.1109/TCC.1996.561099.

[15] O. Puñal, I. Aktaş, C. -J. Schnelke, G. Abidin, K. Wehrle and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, Australia, 2014, pp. 1-10, doi: 10.1109/WoWMoM.2014.6918964.

[16] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," 2020 International Conference on Information Networking (ICOIN), Barcelona, Spain, 2020, pp. 459-464, doi: 10.1109/ICOIN48656.2020.9016462.

[17] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thiron, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrotm, and E. Duchesnay, "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 10, pp. 2825-2830, 2011.

[18] J. H. Friedmann, "Greedy Function Approximation: A Gradient Boosting Machine." The Annals of Statistics, vol. 29, no. 5, 2001, pp. 1189–232. JSTOR, http://www.jstor.org/stable/2699986. (accessed Apr. 04, 2023).