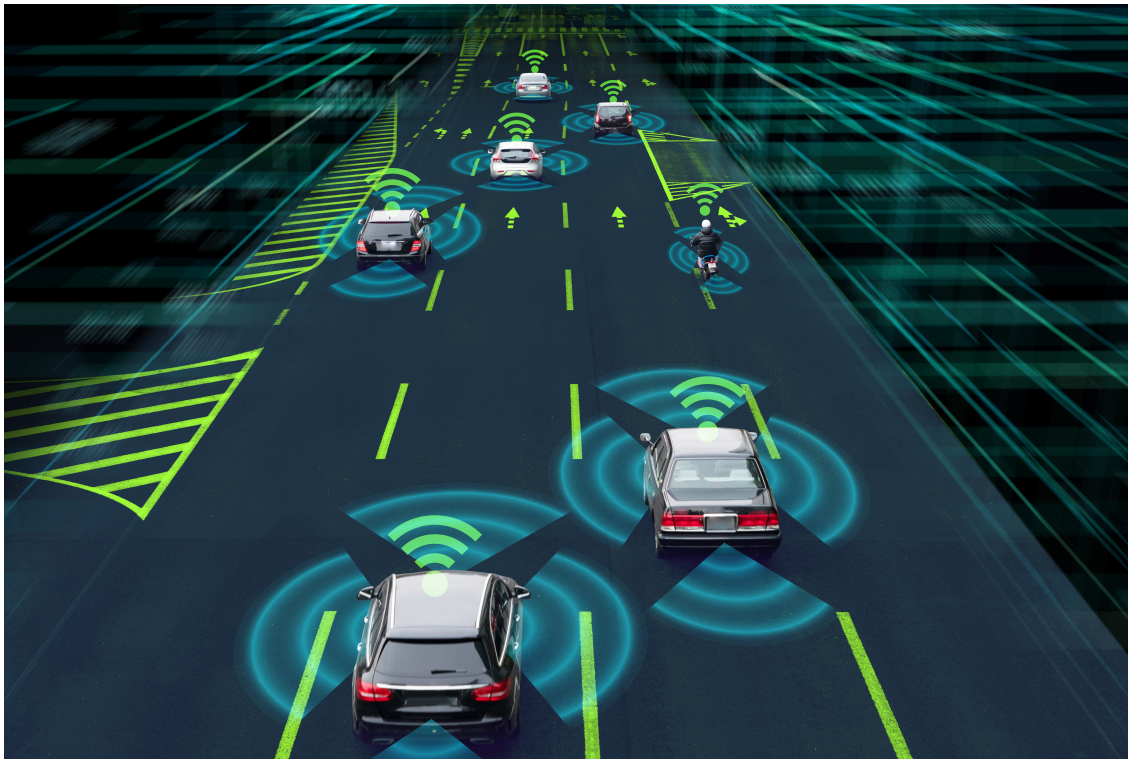


Secure Joint Radar Communications and Risk Assessment for Autonomous Driving

Master's thesis in Computer science and engineering

JOHN SANDELL, QINGYUN GU

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2021

Master's thesis 2021

Secure Joint Radar Communications and Risk Assessment for Autonomous Driving

JOHN SANDELL, QINGYUN GU

UNIVERSITY OF
GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2021

Secure Joint Radar Communications and Risk Assessment for Autonomous Driving

JOHN SANDELL, QINGYUN GU

Supervisor: Canan Aydogdu, Department of Electrical Engineering
Advisor: Tomas Olovsson, Department of Computer Science and Engineering
Examiner: Henk Wymeersch, Department of Electrical Engineering; Andreas Abel, Department of Computer Science and Engineering

Master's Thesis 2021
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: Vehicles using Vehicle-to-Vehicle communication and Radar detection on a highway. Image taken from Shutterstock with permission.

Typeset in LaTeX
Gothenburg, Sweden 2021

Secure Joint Radar Communications and Risk Assessment for Autonomous Driving

JOHN SANDELL, QINGYUN GU
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

Both radar and Vehicle-to-Vehicle (V2V) communication systems in autonomous vehicles are vulnerable to security threats. However, combining radar and V2V communication systems has the potential to overcome the threats to both systems. This report performs a risk assessment of frequency modulated continuous wave (FMCW) radar and dedicated short range communications (DSRC), analyzing the difficulty of performing attacks and the resulting impacts, and presents RadSec, a joint radar communication protocol with sensor data sharing and authentication. The assessment result shows that RadSec has great potential in overcoming automotive security threats against current automotive radar and V2V communication systems. RadSec is shown to improve automotive security for two simulated and three qualitatively discussed use cases. We conclude that joint radar communications should be considered as a technology for enhancing autonomous driving security.

Keywords: Automotive radars, Autonomous driving, V2V, Risk assessment, Joint radar communication, DSRC, FMCW, Automotive security, RadCom.

Acknowledgements

First of all, we want to thank our supervisor Canan for her guidance and knowledge about radars and communication. We also want to thank our examiner Henk Wymeersch and advisor Tomas Olovsson for providing advice about Radars and Security. Finally, we want to thank Mustafa Mete for allowing us to use some of the figures and tables from his thesis.

John Sandell, Qingyun Gu, Gothenburg, June 2021

Contents

List of Figures

List of Tables

1
Introduction

Future autonomous transportation systems will come with severe security risks. Autonomous vehicles can be used as weapons or high-impact bombs for terrorist attacks, making it easy to kidnap or harm certain individuals or attack/impact large groups of people by disrupting the traffic.
The first line of defense in automotive security is to protect the wireless interfaces of an autonomous vehicle. The vehicle-to-vehicle (V2V) wireless communication unit (DSRC or C-V2X) and automotive radar constitute the most vulnerable wireless electromagnetic attack surfaces[1] since they have a more extensive range compared to near field or Bluetooth type attack points.

1.1 Problem Description

Both radar and V2V communication systems are vulnerable to attacks from a reasonable distance away on the order of hundreds of meters. For example, a demonstration of a jamming attack against FMCW automotive radars revealed that it was possible to completely hide a car in front of the automotive vehicle radar[3], where radar signals were jammed by projecting a radar signal with sweeping frequency using separate modified radar equipment. A spoofing attack with the same equipment was theorized in the same study but not tested. However, it is stated that spoofing can create ghost vehicles/objects[2], which might force the vehicle to stop in the best case and result in a collision in the worst-case scenario. V2V security attacks vary from customer annoyance to long-lasting outages of the vehicle, extending to kidnapping the vehicle [4, 5]. For example, a spamming attack annoys drivers by sending junk messages while raising transmission latency in the network. A denial-of-service (DoS) attack, on the other hand, causes many risks to the security since the entire communication channel would be forced to turn off, blocking the vehicle from receiving any information, including accident warnings. The lack of spotting neighbor vehicles also increases the handover load. Vehicles keep broadcasting connection requests and waiting for replies, causing waste of vehicle systems and traffic resources. A black hole attack could be performed when a malicious driver refuses to reply to the connection requests.
One possible way to enhance security is combining these two vulnerable systems. Radar and wireless communications are complementary. The former is about re-

[1] Attack surface is defined as the sum of the different points an unauthorized user can attack the system[2]

[2] A ghost vehicle/object is a target sensed by a radar, which physically does not exist.

ceiving a known signal from an unfamiliar environment, whereas the latter is about receiving an unknown signal from a known environment. The complementary nature of radar sensing and V2V communications, together with the convergence of both technologies [6], suggests the possibility of using joint radar communications for secure autonomous driving in the future. Joint radar communications replace both technologies, i.e., radar and V2V communications, with a radar communications unit (RCU) in a cooperative or co-designed manner [7].

1.2 Related Work

1.2.1 Risk assessment

Other researchers provide the radar and V2V threat analysis, following different standards and frameworks. However, most of them evaluated were only by the impacts they will cause. No details were exposed, nor the possibility of performing the attacks.
Christine et al. listed the threats to DSRC with vague explanations and a general view on security [5]. Irshad et al. introduced main threats in a vehicular network in their article [8], including the impacts they cause and the availability requirement. Other researches like [9] mentioned several threats as examples to their topic, providing valuable opinions about their security. Researches like [10] focus on a particular threat. This kind of researches provides the conduction of our risk assessment.
Our risk assessment is based on the framework described in [11] and the threat analysis from other papers. This framework evaluates each threat from many degrees, leading to a more objective judgment and more precise understanding.

1.2.2 RadChat

RadChat is a cooperative[3] radar communications protocol that uses a single hardware for both radar and communications. RadChat is shown to solve the automotive radar interference problem both in single-hop [12] and multi-hop [13] vehicular networks while providing reasonable V2V communication data rates and latencies [14] to both types of networks. However, the security aspect of joint radar communications has not been investigated and it is not known what other security threats can be eliminated by a joint radar communications protocol design. This study aims to figure out if a joint radar communications system can be more secure than using the stand-alone radar or V2V communication and we aim to design a protocol that has a stronger defense to security threats for the automotive radar and V2V communications.
The complementary nature of both technologies also exists in terms of security. A security comparison among the automotive radar versus DSRC against jamming, spoofing, interference and confidentiality. [15] reveals that V2V communications are more vulnerable to jamming attacks compared to automotive radar (due to the omnidirectional communications). In contrast, radar is more vulnerable to spoofing

[3]Radar and communication cooperate, i.e., exchange data among themselves.

attacks (loss of authentication and encryption). By combining radar and communications, there is a possibility to use the advantages of V2V to eliminate the disadvantages of radar and vice versa. For example, after receiving a signal from radar, we can confirm it with other vehicles via the V2V communication technique to verify a forged signal. Therefore, the security of the vehicle can be enhanced. On the other hand, the heavy handover load of V2V communication can also be decreased by using radar. With the radar detecting vehicles nearby, V2V only needs to connect with the vehicles shown by radar and saves bandwidth and other resources.

1.3 Contributions

In this article, we perform a detailed comparative security risk assessment among radar and V2V. Base on the results of the risk assessment, we add security functions to RadChat. Therefore, we propose a secure joint radar communication protocol - RadSec. It is designed to overcome the threats associated with radar and V2V communications. Following the proposal, a risk assessment on RadSec and some simulations are performed to evaluate RadSec security.

1.4 Thesis Outline

The thesis is structured as follows: After the introduction, we provide some background theory about security and radars and automotive communication basics in Chapter 2. Then we explain the system model and simulation setup for testing RadSec protocol in Chapter 3. In Chapter 4, we explain the basics of the underlying RadChat protocol as well as the new security additions added with our new RadSec protocol. Then we go through the results of the risk assessment and the simulations in Chapter 5. Finally, the results are discussed in Chapter 6.

2

Background Theory

This research covers a vast majority of different disciplines, including computer systems security analysis, electrical engineering radar signal processing, radar communications and transportation. Hence, this chapter covers a risk assessment framework, radar basics, V2V communication basics, radar communication basics, threats to radar systems, threats to V2V communication systems and knowledge of public key cryptography.

2.1 Risk Assessment

We follow the security risk assessment guidelines presented in [11] due to its comprehensiveness in terms of both threat level and impact level of every vulnerable component. The risk assessment includes the following steps:

1. For each potential threat, its threat level is determined by four factors required to attack: expertise, knowledge, the window of opportunity and equipment. The threat values are obtained from Table 2.1 and summed up to obtain a threat parameter sum (T_{sum}), which is used to obtain the treat level (TL) by Table 2.2.
2. For each potential threat, its impact on safety, financial, operational and privacy and legislative aspects is calculated. The impact values are obtained from Table 2.3 and summed up to obtain an impact parameter sum (I_{sum}), which is used to obtain the impact level (IL) by Table 2.4.
3. Security level (SL) for each threat is calculated by using Table 2.5.

The security level can be one of five possible levels: Quality Management, Low, Medium, High, Critical. Other than quality management, all levels suggest that some form of security requirement for a threat/asset pair must be formed.

Table 2.1: Threat Level Parameter Values

Expertise	**Value**	**Knowledge about target**	**Value**	**Window of opportunity**	**Value**	**Equipment**	**Value**
Layman	0	Public	0	Unlimited	0	Standard	0
Proficient	1	Restricted	1	Large	1	Specialised	1
Expert	2	Sensitive	2	Medium	2	Bespoke	2
Multiple Experts	3	Critical	3	Small	3	Multiple bespoke	3

Table 2.2: Threat Level Calculation

Parameter Sum (T_{sum})	**Threat Level**	**TL Value**
>9	None	0
7-9	Low	1
4-6	Medium	2
2-3	High	3
0-1	Critical	4

Table 2.3: Impact Level Parameter values

Impact Level	**Value**
None	0
Low	1
Medium	10
High	100

Table 2.4: Impact Level Calculation

Parameter Sum (I_{sum})	**Impact Level**	**IL Value**
0	None	0
1-19	Low	1
20-99	Medium	2
100-999	High	3
$\geq$ 1000	Critical	4

Table 2.5: Calculation of Security Level from Impact and Threat Level

Security Level (SL)	**Impact Level (IL)**					
Threat Level (TL)		0	1	2	3	4
	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

2.2 Radar Basics

Radar is a device that uses electromagnetic waves to detect objects. The Radar device transmits a signal and if it is reflected from an object, then the distance and location of the object can be calculated using the reflected signal. Radars can operate in different frequency ranges depending on the purpose. Automotive Radars typically operate around 76-81 GHz or 21-26GHz [16].
Radars are classified as either primary or secondary. A primary radar does not depend on other radars and simply receives reflection signals from objects, whereas a secondary radar instead receives a stronger reflected signal transmitted by another radar [17]. Another radar can then receive the transmitted signal and transmit a

reflection signal back, resulting in a stronger signal than merely reflected. Since automotive radars need to be able to detect vehicles without radar transmitters, they are generally primary. Although they can be used as secondary radars together with other automotive radar systems, we use radar units as both primary and secondary in our thesis.

Radars are configured differently to suit different applications. Some of the configurations include Continuous-Wave (CW) radar and pulse-Doppler radar [18]. We will mainly focus on the CW radar in this report and a subset of the CW radar known as Frequency Modulated Continuous-Wave (FMCW) radar [19]. With a normal CW radar that does not change the frequency of its transmitted signal, the direction of an object can be calculated, but the range can not be calculated. This is because there is no way to measure the time delay of when the signal was reflected. However, the relative speed of the target can be calculated using the rules of the Doppler Effect[20]. The speed calculated using the difference in frequency of the signal caused by either the transmitter or reflector moving relatively to the other. Distance to reflected objects can be calculated by measuring the time it takes for the signal to return from being transmitted and then reflected. Using this formula, we can get the distance in meters: $R = \frac{c\Delta t}{2}$, where c is the speed of light and δt is the time difference measured [1].

FMCW is commonly used for automotive systems due to its good range and highly accurate estimations of relative velocity. FMCW radars are also preferred due to their low cost while still being efficient radars. Instead of continually transmitting a signal with constant frequency, the FMCW radar modulates the frequency to calculate distance using the previous formula. Since the frequency is different at different moments in time, we can match the reflected signal with the moment in time that it was transmitted. FMCW radars can be modulated in many different ways. For the purpose of this study, the sawtooth waveform was used. The sawtooth waveform is useful for detecting objects in large ranges. Unlike a sinusoidal waveform, it linearly rises from its base minimum frequency until it reaches the maximum of its modulation, then it drops back to minimum and sweeps back up to maximum, repeating the process. One such transmission from maximum to minimum frequency is called a chirp.

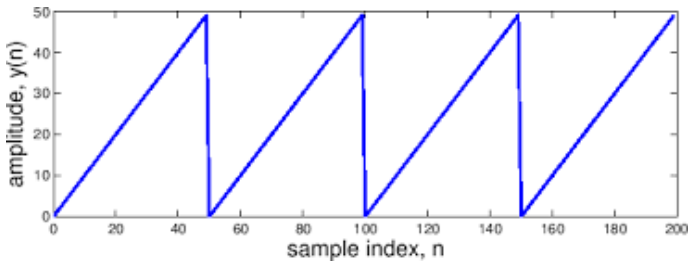


Figure 2.1: Sawtooth waveform

Radar detection systems can be evaluated in several ways. Common metrics for automotive radar are range resolution direction estimation, velocity resolution, maximum

range and maximum velocity measurement. These measurements change depending on the radar properties like sampling frequency, carrier frequency, chirp duration and bandwidth. The sampling rate, i.e., how many samples can be taken a second and the slope of the modulated radar signal determines the maximum range at which objects can be detected. The time it takes between a signal to be transmitted and then be received back can be expressed as time = 2*distance/c, where c is the speed of light. The maximum range can then be given by max_distance = $cf_s/2S$, where S is the slope of the signal and f_s is the sampling rate. The slope of the signal can be calculated given the bandwidth and the length of the chirps, such as (S=B/T), B is the bandwidth.

Instead, the range resolution is a metric of how close two objects can be until the radar can no longer tell them apart. A higher range resolution is therefore desired. The resolution depends only on the bandwidth and is expressed as follows: c/2B. The velocity resolution similarly expresses how accurate the radar is at telling different velocities apart. It depends on the wavelength of the carrier signal λ and the frame duration of the chirps (T_f), i.e., the sum of the chirps duration and time for processing. It can be expressed as such velocity resolution = $\lambda/2T_f$. The maximum velocity that can be measured is calculated with maxVelocity = $\lambda/4T$. One thing that can be taken away from these metrics is that both chirp bandwidth and duration significantly impact them and therefore need to be considered. As there is a trade off with range and velocity metrics, the balance needs to be considered.

2.3 V2V Communication Basics

Vehicular communication has risen in popularity recently when it comes to keeping the roads safe. As proof of this, the 5.9 GHz band has been dedicated to both Vehicle-to-Vehicle (V2V) and Vehicle-to-anything (V2X) communication [21]. This frequency is also known as DSRC. Together with DSRC, the IEEE 802.11p technology has been specifically developed to allow V2V and V2X communication. Currently, the Max data rate is at 27 Mbps. This vehicular communication technology allows vehicles to communicate different attributes to other vehicles, such as position and speed. However, this technology has its flaws, such as the possibility of a signal being blocked by another vehicle or, as will be discovered further in the risk assessment, vulnerable to attacks.

One of the technologies suggested to combat some of the flaws in 802.11p is the Vehicular ad hoc Network (VANET). VANET is a wireless distributed network without any central unit that controls it. The MAC protocol therefore requires heavy allocation [22]. With the combination of the IEEE 802.11p MAC protocol and the Carrier Sense Multiple Access (CSMA) algorithm, listening to channel activity is enabled. In this case, when the channel is busy, a vehicle will stay in the queue in order to prevent congestion. If it senses this, it then randomly calculates a value that determines how long it will wait until it tries to communicate again [12].

2.4 Radar Communications Basics

Radars and V2V communication have valuable functions on their own but have some flaws, such as V2V having a problem with the scarcity of usable frequencies [23] and problems related to security such as denial of service attacks. However, it is possible that they can fix some of these problems by cooperating. In particular, Joint Radar Communications (RadCom) combines radar and communication units into one, transmitting radar signals and using V2V communication on the same radio spectrum [24]. RadCom technology leads to better efficiency in spectrum use and less energy consumption. More importantly, it can help to mitigate some attacks that target either of the systems. This project is built on the joint radar communications protocol RadChat [12], which uses a scheduling algorithm to prevent radars from transmitting simultaneously.

2.5 Automotive Security

An automotive vehicle relies on many systems such as Global Navigation Satellite System (GNSS), heating/cooling systems, cruise control, radar and many more systems that rely on software to work correctly. It is therefore important that all of these systems are secure to keep the passengers safe. A secure automotive vehicle needs to be able to protect itself mainly against malware and against other attacks that can confuse the car's systems. In this thesis, the focus is on wireless attacks to V2V and radar.

2.5.1 Radar Security

The possible threats against automotive radar are jamming, spoofing, denial of service (DoS) and black hole. A detailed explanation is given below for each threat.

2.5.1.1 Radar spoofing

With spoofing, vehicles or other objects can be made to appear to the radar to be there despite not having a physical shape. In the best case, this might make a vehicle come to a stop, but this might make a vehicle collide with an object not visible to the radar in the worst-case scenario. In a study [25], spoofing attacks against FMCW radars were presented. They showed that not only was it possible to attack these sensors but it was possible to do so with commercially available equipment. USRP N210 units were used in the study, which cost around 16 560 DKK per piece [26].

2.5.1.2 Radar jamming

Automotive radars are shown to be vulnerable to jamming attacks. [3] demonstrates an example of a jamming attack against FMCW radars, where radar signals were jammed by projecting a radar signal with a sweeping frequency using separate modified radar equipment. As a result, they were able to completely hide a car in front of the automotive vehicle's radar.

2.5.1.3 Denial of Service (DoS)

This is a theorized attack where attackers target many radars at the vehicle's radar transceiver to make it challenging to handle all signals at once. The radar 2D map will now see many dots around the vehicle, which may be confusing, causing the vehicle to stop or blocking the vision of objects behind the attacking lasers.

2.5.1.4 Black Hole/Signal absorption

This attack represents the case where radar signals are blocked or absorbed by innovative materials like military chaff. Similar to radar jamming, it can cause the vehicle not to see what is in front of the vehicle. Although the black hole attack has not been considered as a threat against automotive radars in the literature before, it might become a threat for autonomous driving in the future.

2.5.2 Vehicular Communication Security

Threats to vehicular communication occur against two essential security attributes: availability and authenticity. Availability is to have all components functional or accessible, whereas authenticity is proof that an entity is whom they claim to be. Whereas radar threats are against only availability, communication threats also include the authenticity dimension. The impacts of those threats vary from customer annoyance to long-lasting outages of the vehicle.
Threats against availability disable some functions of the system and include DoS, Malware and spamming. Threats against authenticity are GPS spoofing, masquerading, broadcast tampering, black hole attacks, replay attacks and transaction tampering. For all the following threats except the malware, performing attacks on a specific target in a mobile environment can be tricky. Nevertheless, if mischief randomly attacks vehicles in some crowded areas, the traffic situation can be messy and cause severe results.

2.5.2.1 Denial of Service (DoS)

In a DoS attack, attackers attempt to prevent legitimate users from accessing the network services by jamming the whole channel or causing some problems to the networks. There are several ways attackers can achieve the DoS attacks in the vehicular environment[8].

- Drop communication packets/Flooding: attackers usually send a vast amount of messages to the target vehicle, so they cannot perform any communication [27].
- Network overloaded/Overwhelm vehicle resources: this attack is to overwhelm the vehicle's resources so that the vehicle is not able to perform other necessary tasks. An example is to continuously send warning messages to the victim so that its internal network will be busy verifying the messages. This can be performed by one or more entities (named Distributed Denial of Service attack or DDoS attack) to shut the network of the target vehicle [8].

2.5.2.2 Malware

A malware, such as worms or viruses, will hack into the vehicle's internal network and lead to some operations disabled, causing severe consequences.

2.5.2.3 Spamming

Spamming is to send messages that are irrelevant to transportation to the vehicle. It will increase the transmission latency in the network.

2.5.2.4 GPS Spoofing

Attackers use a GPS satellite simulator to generate radio signals stronger than those received from the genuine GPS satellite. This can lead nodes to believe they are in a different location than they are [28]. Attackers may also modify a real GPS signal to deceive GPS receivers (also known as GPS manipulation) [10] or send a stronger power signal to cover the real one [27]. This threat endangers human beings both inside and outside the vehicle, especially those GPS-dependent vehicles.

2.5.2.5 Masquerading

Masquerading is an attack that uses a fake identity to gain unauthorized access through legitimate access identification.

2.5.2.6 Broadcast Tampering

Attackers inject false traffic safety messages into the inter-vehicle network to mess up the transportation, for example, suppressing traffic warnings to cause accidents or manipulating traffic flow to clear a chosen route. Moreover, a malicious vehicle would add some time delay to the messages it received and forward the modified messages to other vehicles. For example, not informing the position of one vehicle to another in time and cause an accident between them. Attackers can also declare themselves as multiple nodes (vehicles), eventually leading to extensive damage to network topologies and consuming large amounts of bandwidth [9].

2.5.2.7 Black Hole

A black hole in a network causes propagating messages to fail. Other vehicles may not be able to receive the messages from a specific node (vehicle).

2.5.2.8 Replay

A replay attack is also called an alteration attack, which occurs when an attacker employs any previously generated frames to send and communicate with other nodes, with or without alteration. GPS manipulation can be regarded as a replay attack.

2.5.2.9 Transaction Tampering

This is another threat to message integrity. Attackers modify the messages exchanged in V2I to falsify transaction application requests or forge the associated replies.

2.5.3 AES-CMAC

In cryptography, authentication is a method to ensure that a party is whom they claim to be. The purpose of authentication is to make sure that messages are received from the correct place. One such Authentication algorithm is Advanced Encryption Standard-Cipher Based Message Code (AES-CMAC) [29]. The algorithm is based on block ciphers and only requires one key for signing and authenticating messages. The size of the ciphertext and key it creates are 128 bits each. Due to it using a symmetrical cipher and being of small size, it is relatively fast.

3
System Modelling

3.1 Automotive Radar Model

We assume that all vehicles are equipped with identical RCU units, where all vehicles have the same radar and communication parameters (radar frame time, radar slope, radar bandwidth/carrier frequency, communication bandwidth/carrier frequency/-modulation scheme, etc.). The units are able to transmit and communicate but cannot transmit both signals simultaneously.

3.1.1 Radar Deployment on a Vehicle

We choose to classify FMCW radars by their maximum range and field of view capabilities. The three different types are long-range radar (LRR), medium-range radar (MRR) and short-range radar (SRR) [30]. Table 3.1 shows how they can be classified and what they are most commonly used for.

Table 3.1: Classification of Automotive Radars Based on Range

Radar Type	**Long-Range (LRR)**	**Medimum-Range (MRR)**	**Short-Range (SRR)**
Range(m)	$10 - 250$	$1 - 100$	$0.15 - 30$
Azimuth FoV(deg)	± 15	± 75	± 80
Elevation FoV(deg)	± 5	± 5	± 10
Applications	Automotive cruise control	blind-spot detection	obstacle detection

In our system, we used six radars, two LRR for the vehicle's front and back, and four MRR for the four corners of the vehicle. A Volvo XC90 was chosen as the model of the vehicle. More exact details of the range of each radar as well as their FoVs can be seen in Table 3.2.

The placement of the radars and their FoVs were simulated in MATLAB with their autonomous driving toolbox. Multiple cars with the same configuration were used in the simulations. Tables 3.1, 3.2 along with Figure 3.1 and the angles and positions of the radar were provided from [1].

Table 3.2: Technical Details of Automotive Radars Used in Our Design. [1]

Location	Front	Back	Front Right	Front Left	Back Right	Back Left
Type	LRR	LRR	MRR	MRR	MRR	MRR
Range(m)	$10-200$	$10-200$	$1-80$	$1-80$	$1-80$	$1-80$
Azimuth FoV(deg)	± 10	± 10	± 75	± 75	± 75	± 75
Elevation FoV(deg)	± 5	± 5	± 5	± 5	± 5	± 5
Yaw Angle(deg)	0	-180	-60	60	-120	120

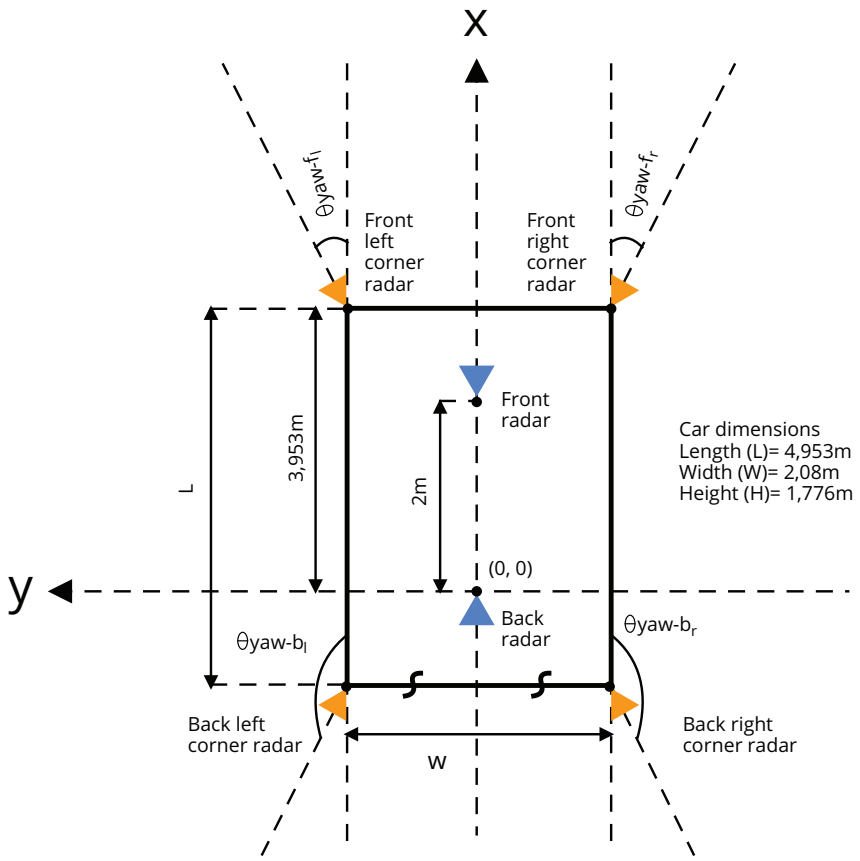


Figure 3.1: Illustration of the radars' placement on a vehicle

3.2 Identifying LoS paths between vehicles

In the simulation, we wanted to test jamming and denial-of-service attacks using RadCom technology. Therefore there was a need to determine the line of sight (LoS) between different RadCom units. Since this was not provided with the autonomous driving toolbox, we needed to provide our own functions to calculate this. To calculate a possible link between two sensors, we used the vehicle's positions, the sensors' position relative to the vehicle, the sensors' angles, and the sensors' FoVs.

First, we add the relative position of the sensors to the vehicle's positions to get their real positions. Second, we compare the ranges of the sensors with the distance between the two cars to see if they are in a range. Third, using trigonometry, we then calculate the angle between the two sensors to get the angle between them relative to the x-axis. Finally, for each sensor, we check if the angles of the sensor plus the FoV align with the angle between the sensors. If all these conditions are true, then there is a link between the two vehicles. Since communication signals and radar signals have different ranges, we do these calculations for both ranges to see a radar link and a communication link. Code for this can be found in Appendix A.1.1.

3.2.1 Link Blockage check

Another function was needed to make sure that links were not blocked by another vehicle. To do this, we first check if a vehicle is closer to the first vehicle than the

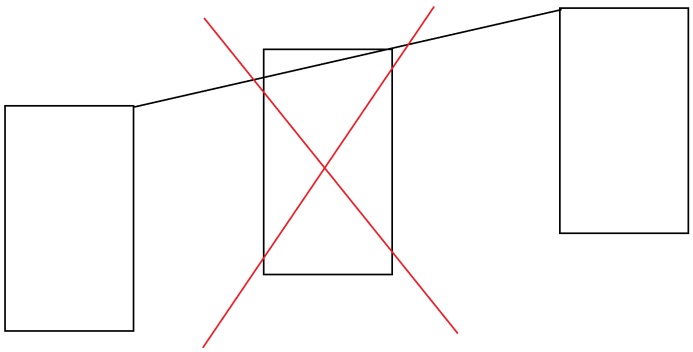


Figure 3.2: Radar blocked by another vehicle

one we are checking the link with. If so, we then calculate the positions of the corners of the possible blocking car by adding its width and length to its position. We then calculate the angles between the sensor and the four angles of the middle car. By sorting the angles, we then determine which corners determine the FoV of blocked sight, as shown in Figure 3.3. We then simply check if the 2nd sensor falls in that blocked area or not to determine if the link is blocked. Code can be found in Appendix A.1.2.

3.3 Wireless Channel Propagation Model

Ray-tracing was used to model the communication channel of the simulations. In the simulations, we assume that radar and communications only propagate via LoS links and use geometry to check if links are there. To simplify the model, reflections from other vehicles and the environment were ignored.

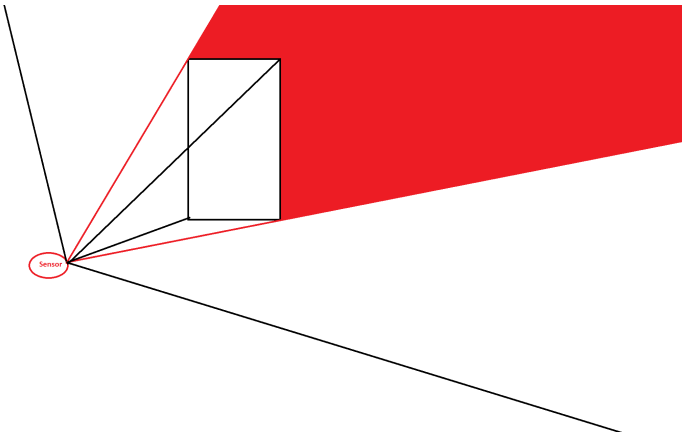


Figure 3.3: FoV of blocked radar vision

This simplification allows for three signals to be received by RadCom unit r_i from another r_j : the reflected radar signal, radar interference and the communication signal. We assumed that there were free space propagation conditions. In other words, we assume that the environment is empty except for the signals stated here. We can then calculate the effective range of these signals using the radar range equation [31].

$$R_{\mathrm{r}} = \frac{P_r G^2 \lambda_r^2 \sigma}{N_r (4\pi)^3 d_{\mathrm{r}}^4}, \tag{3.1}$$

$$R_{\mathrm{int}} = \frac{P_r G^2 \lambda_r^2}{N_r (4\pi)^2 d_{\mathrm{int}}^2}, \tag{3.2}$$

$$R_{\mathrm{c}} = \frac{P_c G \lambda_c^2}{N_c (4\pi)^2 d_{\mathrm{c}}^2} \tag{3.3}$$

$_r$, $_{int}$ and $_c$ represent radar, interference and communication, respectively. P_r is the power of the reflected radar signal, while P_c is the power of the transmitted signal from the RCU unit. G is the antenna gain of the signal. Since the reflected radar signal and radar interference signal are reflected or interfered with by other signals, the antenna gain is squared. λ represents the wavelength of the signals. σ is the radar-cross section which shows how well objects are at reflecting radar signals. d represents the range where signals can be detected. Since the radar signal is reflected in the first equation, it travels twice as far (to the reflected object and back) and therefore has double the exponent 4, compared to d_c and d_int, which has the exponent 2 due to only having to travel to an object. N represents the Noise of the signal and can be calculated with the following equations:

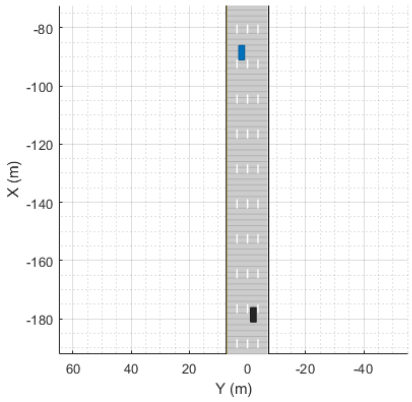
$$N_r = B_r K T F \tag{3.4}$$

$$N_c = B_c K T F \tag{3.5}$$

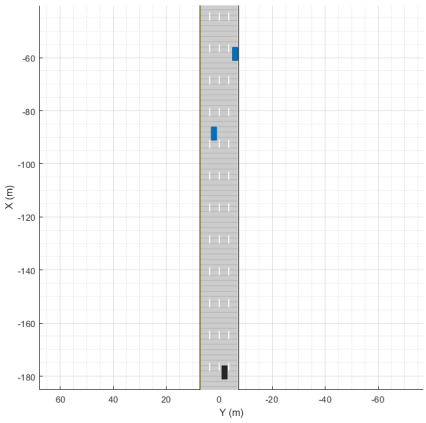
K is Boltzmann's constant, T is the standard temperature, B is the signal bandwidth and F is the receiver's noise figure.

3.4 Simulation Scenario Setup

Using MATLAB's driving toolbox, two different scenarios were set up. Both scenarios take place on a highway with four lanes. In both scenarios, an attacker car simulates both a jamming attack and a denial of service attack separately. We assume that the attacker uses all six radars on the vehicle for its attacks. In the first scenario, there are two vehicles, an attacker and a victim. The two vehicles, along with the links between them, can be seen in Figure 3.4a. The attacker car is painted black in the figure. In the scenario, both cars move along the x-axis with speeds such that the black car eventually passes the blue car. The attacker starts at (-180, -2) and travels forward at a constant speed of 60 m/s. The blue cars travel at a constant speed of 30 m/s. In the first scenario, the blue car starts at (-90,2), while in the second scenario, they start at (-90,2) and (-60,-6).



(a) Scenario-I: Black car starts at (-180,-2) and travels along the x-axis at a constant speed of 60 m/s. The blue car starts at (-90,2) and travels along the x-axis at a constant speed of 30 m/s.



(b) Scenario-II: Black car starts at (-180,-2) and travels along the x-axis at a constant speed of 60 m/s. The blue cars start at (-90,2) and (-60,-6) and travel along the x-axis at a constant speed of 30 m/s.

Figure 3.4: An Illustration of the scenarios

In the second scenario, there are instead two blue victim cars. The purpose of the second scenario is to see the effect that RadSec can have in helping vehicles when they are being attacked by sharing sensor data with each other. Like the first scenario, the black car travels faster along the x-axis and eventually passes the blue cars. The second scenario, as well as the links between the vehicles, can be seen in Figure 3.4b.

To get an accurate depiction of how much of an effect the attack has on the blue cars, we measure the percentage of RCUs, the percentage of radar and communica-

tion area affected as well as the percentage of area covered by RCUs that is on the road under attack.

4

Radar Communications Security Protocol (RadSec)

The RadCom protocol RadChat which we introduced earlier, solves some of the interference issues related to increasing separate radar units on automotive vehicles [12]. In this chapter, we first explain the multiplexing scheme of radar signals, the Radar Medium Access Control technique and the Communications Medium Access (CSMA) Control technique that make up the cores of the protocol. In addition to this, we present the security changes we suggest to the protocol resulting from the risk assessment 5.3 as the RadSec protocol. Mainly Authentication and Sensor Data Sharing.

4.1 Multiplexing

Analog to Digital Conversion (ADC) has restraint on the possible waveforms used. Since we use the same hardware for radar and communications, it is important to consider what should be used. Since FMCW signals result in a low communication data rate [32], multiplexing is used. Multiplexing in the frequency domain allows the system to gain better spectral efficiency and adaptability. Therefore the radar bandwidth is split into four parts. The bandwidth is 15 MHz for communications and the bandwidths for long-range and medium-range radar units are 800 and 250 MHz respectively.

4.2 Radar Medium Access Control

When multiple vehicles with the same type of radar units transmit simultaneously, the effect of interference between signals increases significantly, that is why the communication channel needs to be appropriately shared via some scheduling scheme. The technique used to achieve this is radar time division multiple access (rTDMA). The scheme organizes the radar units by allocating time slots where they are allowed to broadcast. The bandwidth and carrier frequency is kept consistent with reducing receiver complexity.
In Figure 4.1, the frequency and time division of this system is depicted. A radar frame T_f is split into 1/U time slots, of which there are 5 [T_1, T_2,...T_5]. U is the modified radar data cycle expressed as: $U = (N + 1) \cdot T/T_f$. Here (N+1) $\cdot$ T is the duration of one time slot, which is equal to the sum of the duration of N chirps and

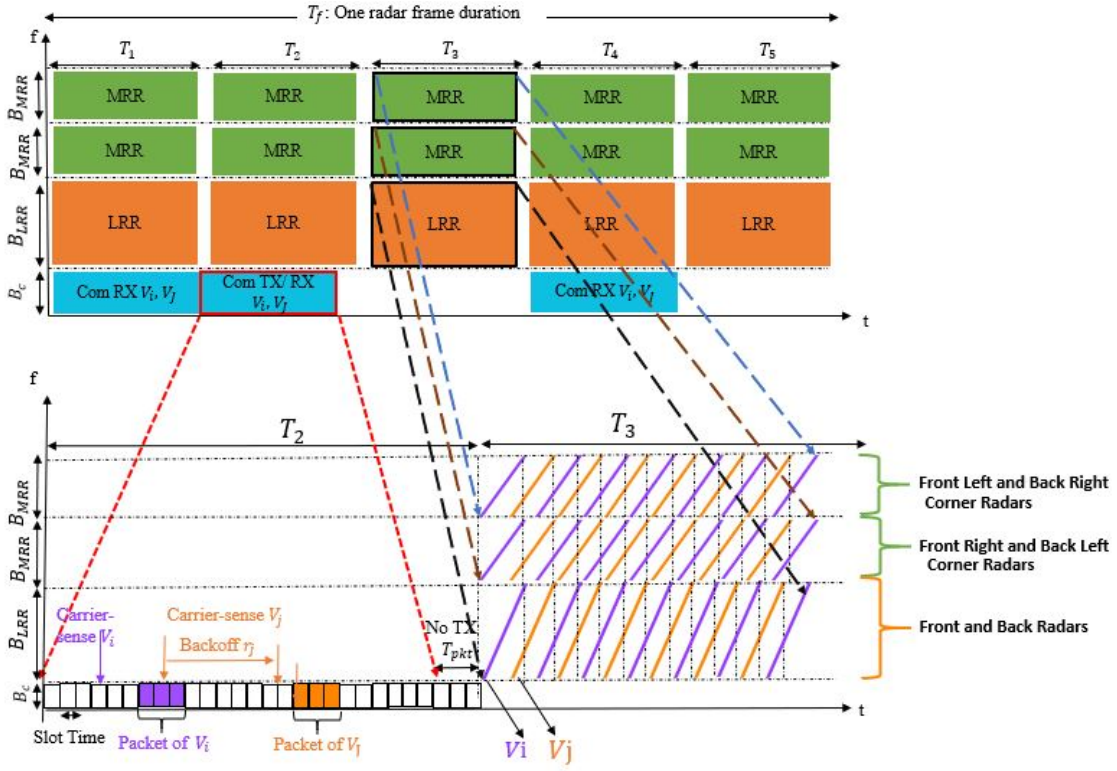


Figure 4.1: Illustration of the RadCom scheduling program. The radars transmit in the T_3 frame [1]

.

then an extra idle waiting chirp to prevent overlap. The idle chirp also allows for radars on different vehicles to fit into one time slot. Due to this, any interference between radar units can be kept to a low but acceptable level.

The maximum number of different radars transmitting in one time slot without interfering can be calculated with: $B_r/((1+\alpha_d)\cdot B_c)$ where α_d is a constant value to express direct links, which could cause interference. This value is separate for LRR and MRR being 10 and 6 respectively. The maximum amount of vehicles that fit into one channel without overlapping can be calculated as such:

$$M_{\max} \leq \frac{B_r}{(1+\alpha_d)\cdot B_c \cdot U} \tag{4.1}$$

The maximum amount of vehicles for LRR and MRR are therefore 25 and 95 respectively. That is, no more than 25 vehicles can be scheduled for one channel using LRR without getting any overlap.

4.3 Communications Medium Access Control (CSMA)

The communication systems of a RadCom unit are on alleviating interference issues since the radars are assigned different time slots. The Communications Medium

Access (CSMA) Control is the protocol that organizes access to the shared communications channel. Since the VANET topology updates dynamically and needs a central unit, CSMA is the only available channel access control option [22].

When a vehicle wants to transmit their radar signals, they broadcast their control communication packets using CSMA with a random binary exponential backoff (BEB) value. This is done over a dedicated communication channel. The control packets are defined as periodic broadcast messages and, as such, do not require RadCom units to send acknowledgment packets. This, therefore, is important in keeping interference low.

First, we can assume that control packets are identical. Let us then assume that vehicle i (V_i) sends a broadcast with a control communication packet (purple coloured rectangle) in T_2. This packet is, in turn, which by a different vehicle j (V_j) as shown in Figure 4.1. A control packet then has a Slot Index (SI), identity (ID) and an id-List. The ID can give the information of the time reference. ID, SI and id-Lists are shared among units on the same vehicle. SI represents a randomly selected slot index and the id-list keeps track of which vehicle has what id. Once a RadCom unit acquires the control communication packets from the neighboring vehicles, it then redefines its ID, SI and id-List accordingly as not to clash with other vehicles. If V_j then wants to do radar transmissions in T_3, it can declare this by sending out another control communication packet (orange coloured rectangle) in T_2. Since the vehicles now transmit at different SI, we prevent overlap.

The RadCom protocol provides unique and compatible SI for each vehicle to ensure a stable schedule for all vehicles involved. If the control packets are transmitted simultaneously by other vehicles, it is solved in another radar frame with the help of [32]. The clock used is synchronized with GPS.

4.4 Sensor Data Sharing

With the many directional RCUs, it is possible for a vehicle to communicate using one or more of its RCUs, even if some are blocked by attacks. This allows for the possibility of sharing useful sensor (angle and distance), location and velocity data to other cars to better judge a situation where they would not otherwise have all of the critical information. This way, a vehicle, which receives information that conflicts with its own radar sensor data, can switch to another radar frequency band preventing further jamming or spoofing.

Another case might be this: if the front-RCU of vehicle A is jammed by attacker B, vehicle A is forced to turn off its front-RCU to stop being attacked. Without RadSec, vehicle A cannot obtain the information its front-RCU could have detected. But with RadSec, a friendly neighbor vehicle can send its sensor data to vehicle A's corner-RCU, potentially rendering the attack useless by providing the sensor information of what vehicle A can not see.

4.5 Authentication

Since the RadSec protocol both schedules transmissions and shares sensor data via V2V communication, there must be some way for vehicles to authenticate these communications. Otherwise, an attacker could easily trick the scheduling protocol or send fake sensor data to confuse vehicles. This also has the upside that attackers can be logged and reported in case they try to attack using encryption keys, making the attackers easier to trace for the relevant authorities.

The most common option for authentication is the AES standard, as mentioned in Section 2.5.3. In [33], NXP suggests using AES-128 bit CMAC keys for signing and authentication. They furthermore suggest using AES-128 CBC for encryption and decryption when updating the key pairs to prevent any attacker from listening in on the updates and retrieving the keys.

5
Results

In this chapter, we give the risk assessment along with the motivations of all the assigned security levels. Then we show the results of the simulations that showcase the benefits of RadSec.

5.1 Risk Assessment

General Risk Assessments of automotive systems can be found in [34], [35], [36]. The basics of Risk Assessment can be found in section 2.1. In [34], a threat assessment similar to the one type of Risk Assessment we use was made. For some of the attacks where this is relevant, we assign the appropriate value of each threat in 2.1 to get correct threat values. We state so in the cases where this is done. Otherwise, it is our own assessment of the attacks.
The threat sum (T_{sum}), impact sum (I_{sum}) and security level for all asset/threat combinations for the automotive radar are summarized in Table 5.1, 5.2 and 5.3, consecutively.

5.1.1 Threats to radar systems

In this subsection, we assess the following radar threats: spoofing, jamming, interference, DoS, and black hole attacks. The first three threats are more commonly known, while the two latter ones are more based on theory.

5.1.1.1 Radar spoofing

The threat levels for radar spoofing were assigned like this in [34]:

- Expertise: Proficient, The attacker needs to know radar sensing parameters (range, chirp formats, etc.) for a successful attack and this requires a 'proficient' level of expertise. Proficient is equal to threat value 1.
- Equipment Required: Light transceivers/pulse generator. We can assume that the equipment needed can be classified as Specialised as it can't be found in everyday stores but can still be purchased without too much effort.Specialised equipment has a threat value of 1.
- Window of Opportunity: Small. Very specific since one needs to know the frequency of radars being used. A small window has a threat value of 3.
- Knowledge: This was not mentioned in the paper, but since knowledge about FMCW Radars is restricted as the manufacturers do not reveal chirp pa-

rameters, we can assume that restricted is a correct level here. Restricted Knowledge has a threat value of 1.

According to [11], $T_{sum} = 1 + 1 + 3 + 1 = 6$ and TL = Medium.

In [35], a similar assessment was made, albeit with a different scale, so it is not easy to apply in our case. Their scale is based on the one used in [37], which has less uniformity in numbers for one. Some categories have values from 0-5, while some go from 0 to infinity. Their conclusion from the assessment was that radar jamming and spoofing were highly risky.

The impact level was assessed in [36] as such:

- Safety: High, the reason being that spoofing and jamming attacks could potentially cause a collision. This corresponds to an impact value of 100.
- Operational: Medium, since this can have serious consequences for the vehicle's operational functions, such as causing it to stop suddenly. This corresponds to an impact value of 10.
- Privacy: None, as we can find no direct privacy violation impact from this attack. This corresponds to an impact value of 0.
- Financial: None. However, we argue that the manufacturers who produce the vehicles are somewhat likely to take financial damage from the news of attacks against their vehicles. Therefore it should be at least Low, which corresponds to an impact value of 1.

Hence, the impact parameter sum becomes $I_{sum} = 10(100 + 1) + 0 + 10 = 1020$, which corresponds to a critical impact level.

Finally, a medium threat level and a critical impact level results in a high security level, according to Table 2.5.

5.1.1.2 Radar jamming

The threat levels for radar jamming were assigned like this in [34]:

- Expertise: Proficient. The attacker needs to know radar sensing parameters (range, chirp formats, etc.) for a successful attack and this requires a 'proficient' level of expertise. Proficient is equal to threat value 1.
- Equipment Required: Light transceivers/pulse generator. We can assume that the equipment needed can be classified as Specialised as it can't be found in everyday stores but can still be purchased without too much effort(UniqueSec AB, www.uniquesec.com). Specialised equipment has a threat value of 1.
- Window of Opportunity: Small. Very specific since one needs to know the frequency of radars being used. A small window has a threat value of 3.
- Knowledge: This was not mentioned in the paper, but since knowledge about FMCW Radars is restricted as the manufacturers do not reveal chirp parameters, we can assume that restricted is a correct level here. Restricted Knowledge has a threat value of 1.

According to [11], $T_{sum} = 1 + 1 + 3 + 1 = 6$ and TL = Medium.

In [35], a similar assessment was made, albeit with a different scale, so it is difficult to apply in our case. Their scale is based on the one used in [37], which has less uniformity in numbers for one. Some categories have values from 0-5, while some

go from 0 to infinity. Their conclusion from the assessment was that radar jamming and spoofing were highly risky.
The impact level was assessed in [36] as such:

- Safety: High, the reason being that spoofing and jamming attacks could potentially cause collision. This corresponds to an impact value of 100.
- Operational: Medium, since this can have serious consequences for the operational functions of the vehicle, such as causing it to stop suddenly. This corresponds to an impact value of 10.
- Privacy: None, as we can find no direct privacy violation impact from this attack. This corresponds to an impact value of 0.
- Financial: None. However, we make the argument that the manufacturers who produce the vehicles are somewhat likely to take financial damage from the news of attacks against their vehicles. Therefore it should be at least Low, which corresponds to an impact value of 1.

Hence, the impact parameter sum becomes $I_{sum} = 10(100 + 1) + 0 + 10 = 1020$, which corresponds to a critical impact level.
Finally, a medium threat level and a critical impact level result in a high security level according to Table 2.5.

5.1.1.3 Radar interference

Another threat against radar is radar interference, which occurs as radars use the same frequency simultaneously in the same space.
Threat level:

- Expertise: Layman (value 0). Radar interference can be caused by simply using radars at the correct frequency.
- Equipment Required: Specialised (value 1). Other FMCW radars in cars can create interference. Of course, it can still be costly as many radars will be needed to increase the success rate of the attack.
- Window of Opportunity: Medium (value 2). One or many vehicles will have to stay in the range of the moving target vehicle to cause interference.
- Knowledge about target: Public (value 0). As long as attackers know the public frequency to operate in causing interference is possible.

$T_{sum} = 0 + 1 + 2 + 0 = 3$ and TL=High.
Impact Level:

- Safety: High. Interference can hide low radar cross section targets [38] and potentially cause a collision. This corresponds to an impact value of 100.
- Operational: Medium, since interference can have serious consequences for the operational functions of the vehicle, such as causing it to suddenly stop in case of detecting a ghost target [39]. This corresponds to an impact value of 10.
- Privacy: None, as we can find no direct privacy violation impact from interference. This corresponds to an impact value of 0.
- Financial: None. However, we make the argument that the manufacturers who produce the vehicles are somewhat likely to take financial damage from the news of attacks against their vehicles. Therefore it should be at least Low, which corresponds to an impact value of 1.

$I_{sum} = 10(100 + 1) + 0 + 10 = 1020$ and IL=Critical.

5.1.1.4 Denial of service (DoS)

Threat level:

- Expertise: Proficient. Attackers need to be able to operate and target radars at one single point
- Equipment Required: Multiple bespoke. Using many radars is going to be quite costly.
- Window of Opportunity: Small. All the radars need to be targeted at the transceiver while in range of the moving target.
- Knowledge about target: Restricted. All parameters of the radar transceiver are not public.

$T_{sum} = 1 + 3 + 3 + 1 = 8$ and TL = Low
Impact level:

- Safety: Low. While the radar might be confused from this attack it is unlikely to cause any collision
- Operational: Low. Car might get confused and stop
- Privacy: None. This will not affect privacy.
- Financial: Low. This might reflect poorly on the automotive industry causing financial damage to stakeholders.

$I_{sum} = 10(1 + 1) + 1 + 0 = 21$ and IL = Medium.
Security level = Low, since the attack is most likely quite costly and might not cause that many bad consequences.

5.1.1.5 Black Hole/Signal absorption

Threat level:

- Expertise: Expert. Attackers need to understand some material science to understand how to correctly employ the blocking material
- Equipment Required: Bespoke. The kinds of materials needed to do these attacks are either top secret or very expensive to purchase.
- Window of Opportunity: Medium. Attackers need to be in the range of the target vehicle's radar.
- Knowledge about target: Restricted. Knowledge about these materials is not public

$T_{sum} = 2 + 2 + 2 + 1 = 7$ and TL=Low.
Impact level:

- Safety: High. In the worst there could be a collision with the hidden vehicle.
- Operational: Low, The vehicle might not operate correctly when information is hidden from it.
- Privacy: None. No privacy violations are committed here.
- Financial: Low. This might reflect poorly on the automotive industry causing financial damage to stakeholders.

$I_{sum} = 10(100 + 1) + 1 + 0 = 1011$ and IL=Critical.
Security level = Medium, as the likelihood of the threat occurring is very low, but it could be dangerous if the attack works.

5.1.2 Threats to V2V communication systems

We focus on V2V communications, omitting infrastructure-based communications since a distributed ad-hoc wireless communication is more vulnerable
The evaluations of vehicular communication, more specifically, Dedicated Short Range Communications (DSRC), are mostly inspired by three articles: [5], [9] and [27]. These articles use different methodology for threats analysis: [5] and [9] follow the Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) created by European Telecommunications Standards Institute (ETSI) [40]. [27] uses a formula $Risk = Asset \cdot Vulnerability \cdot Threat$. In our risk assessment, we evaluate each factor based on these articles and some other papers that research on a certain threat.

5.1.2.1 Denial of Service (DoS)

Threat level:

- Expertise: Expert (value 2). For flooding attacks, attackers repeatedly drop communication packets or warning messages that are standard and do not require much security knowledge. However, for other types of attacks such as jamming, attackers want to interfere with specific components (for instance, the control channel of the vehicle or roadside unit), more security knowledge is required.
- Knowledge about target: Public (value 0). Knowledge of standard protocol is public and easy to find online. Attackers can use standard message types to forge messages. Overall, this is an attack that has low technical difficulty, especially in a traffic jam.
- Window of Opportunity: Medium (value 2). To perform DoS attacks, attackers should maintain a certain distance from the target vehicle. If there are devices that attackers can stick to the vehicle and control remotely, then attackers need to have physical access at least once to install a device. This will be another attack type that requires attackers to be familiar with the owner and to maintain the device.
- Equipment Required: Standard (value 0). A standard message sender and a computer should be enough for these attacks, no need for specialization.

T_{sum} = 2+0+2+0 = 4, TL = Medium.
Impact level:

- Safety: High (value 100). Traffic accidents may happen if the driver has no awareness of the dangerous situation.
- Financial: Low (value 1).
- Operational: Medium (value 10). Once succeed, DoS would result in temporary outages on communication, collision warnings, or platoon directives may not be able to deliver (Flooding). Traffic safety applications that depend upon message delivery may be compromised so that attackers may not be identified. [5]
- Privacy: Low (value 1).

I_{sum} = (100+1)*10+10+1 = 1021, IL = Critical.
Security level = High. DoS is a common attack that can cause severe consequences.

5.1.2.2 Malware

Threat level:

- Expertise: Expert (value 2). Attackers must be a security expert and be familiar with underlying algorithms, protocols, hardware, software, concepts and the vehicle's inner architecture. They should also know techniques and tools of existing attacks to design and implement effective malware. [11]
- Knowledge about target: Restricted (value 1). Some knowledge of internal architecture design is required.
- Window of Opportunity: Medium (value 2). The chance of having physical access to the inner vehicle system is meager. To install the malware remotely, the attacker needs to maintain a relatively short distance from the target vehicle.
- Equipment Required: Standard (value 0). No special equipment is required for this attack.

T_{sum} = 2+0+2+1 = 5, TL = Medium.
Impact level:

- Safety: High (value 100). As a result, long-lasting outages will happen to the system, essential functions such as brake may be blocked and the driver may lose control of the vehicle. In that case, passengers' lives will be threatened.
- Financial: Medium (value 10). Mainly includes indirect financial damages like damages to reputation and loss of market share.
- Operational: High (value 100). Important functions such as brake may be blocked.
- Privacy: Medium (value 10). Since customers' privacy and life are highly risky, a successful malware attack may cause a reputation loss to the company and a loss of market share.

I_{sum} = (100+10)*10+100+10 = 1210, IL = Critical.
Security level = High.

5.1.2.3 Spamming

Knowing the communication protocol, attackers wrap the messages as they are from normal users. It will be difficult to spam a specific target, but it could make drivers annoyed if attackers broadcast to the environment since they can attack many targets at once in a busy area or during a traffic jam. As an impact, a high transmission latency may lead to a late response, but the system is still functional. Customers would complain about the annoyance, but there will be no discernible effects or appreciable consequences for the stakeholders.

5.1.2.4 GPS Spoofing

Although GNSS simulations can be found on the market, it is not easy to perform this attack in a mobile environment. Also, some areas have the law to forbid over-the-air retransmission of GPS signals without prior authorization. [10]
GPS spoofing targets on interfering with the navigation. Other functions in the vehicle will not be affected. However, when the driver has no knowledge of the area

they are going to, they may get annoyed not being able to reach the destination. Also, the driver panics once they found the environment different from the GPS map, increasing the possibility of accidents. A worse situation will happen in self-driving since the system relies on GPS to navigate the vehicle. A misleading signal may guide the vehicle to turn in a direction that it should not be, therefore, cause collisions. However, autonomous vehicle navigation not only depends on GPS. With other sensors such as precision mapping, cameras, radar and LiDAR, GPS spoofing can be easily detected. [41]

5.1.2.5 Masquerading

By compromising integrity, this threat has a high impact on the user and the network. However, according to [5], there is a very significant technical difficulty in forging a certificate that can bypass the authentication protocol. Once it succeeds, it may cause information leakage on the customers' side.

5.1.2.6 Black Hole

Attackers may disable their message sender to hide their activities and approach the target silently. There was no privacy leakage in this attack, but customers' safety would be threatened as they could not see an approaching vehicle or receive some traffic warnings. The report of Christine et al. [5] ranks this threat as critical, but in our assessment, considering the knowledge required to the target vehicle and the window of opportunity, it decreases to high in rank.

5.1.2.7 Replay

The potential gain of this attack is to fool other nodes (vehicles) in the network, therefore, manipulate the network. However, similar to GPS spoofing, the technical difficulties in carrying out a replay attack are substantial.

5.1.2.8 Transaction Tampering.

As a result, attackers may manipulate the traffic as expected. Although, this attack is not easy to perform due to the encryption of transaction messages and a mobile environment.

5.1.2.9 Broadcast Tampering

Similar to transaction tampering, this attack is not easy to perform. This attack's threat level evaluation is based on [5], while the impact level is concluded from [27].

Table 5.1: Threat Level Assessment (*X = Expertise, K = Knowledge about target, W = Window of opportunity, Q = Equipment*)

Asset	**Threat**	**X**	**K**	**W**	**Q**	T_{sum}	**TL**
V2V	GPS Spoofing	3	2	3	0	8	1
	Masquerading	3	2	2	0	7	1
	Broadcast Tampering	3	2	2	0	7	1
	Black Hole	1	2	1	1	5	2
	Replay	3	2	3	0	8	1
	Transaction Tampering	3	2	2	0	7	1
	DoS	2	0	2	0	4	3
	Malware	2	1	2	0	5	2
	Spamming	0	0	2	0	2	3
Radar	Radar Interference	0	0	2	1	3	3
	Radar Spoofing	1	1	3	1	6	2
	Radar Jamming	1	1	3	1	6	2
	DoS	1	1	3	3	8	1
	Black Hole	2	2	2	1	7	1
RadSec	GPS Spoofing	3	2	3	0	8	1
	Masquerading	3	2	2	0	7	1
	Broadcast Tampering	3	2	2	0	7	1
	Black Hole	1	2	1	1	5	2
	Replay	3	2	3	0	8	1
	Transaction Tampering	3	2	2	0	7	1
	DoS	2	0	3	0	5	2
	Malware	3	2	1	0	6	2
	Spamming	1	0	2	0	3	3
	Radar Spoofing	3	1	3	1	8	1
	Radar Jamming	3	1	3	1	8	1
	Radar Interference	0	1	2	0	3	3
	Radar DoS	1	1	3	3	8	1
	Radar Black Hole	2	2	2	1	7	1

Table 5.2: Impact Level Assessment(*S = Safety, F = Financial, O = Operational, P = Privacy and Legislative*)

Asset	**Threat**	**S**	**F**	**O**	**P**	**Isum**	**IL**
V2V	GPS Spoofing	10	1	1	10	121	3
	Masquerading	100	1	1	10	1021	4
	Broadcast Tamp.	1	1	0	10	30	2
	Black Hole	100	1	1	10	1021	4
	Replay	10	1	0	1	111	3
	Transaction Tamp.	1	1	1	10	31	2
	DoS	100	1	10	1	1021	4
	Malware	100	10	100	10	1210	4
	Spamming	1	0	1	0	11	1
Radar	Radar Interference	100	1	10	0	1020	4
	Radar Spoofing	100	1	10	0	1020	4
	Radar Jamming	100	1	10	0	1020	4
	Radar DoS	1	1	1	0	21	2
	Radar Black Hole	100	1	1	0	1011	4
RadSec	GPS Spoofing	1	1	1	1	22	2
	Masquerading	100	1	1	10	1021	4
	Broadcast Tamp.	1	0	0	1	11	1
	Black Hole	1	1	1	1	22	2
	Replay	1	1	0	1	21	2
	Transaction Tamp.	1	1	1	1	22	2
	DoS	1	1	1	1	22	2
	Malware	100	1	100	100	1210	4
	Spamming	1	0	1	0	11	1
	Radar Spoofing	100	1	10	0	1020	4
	Radar Jamming	100	1	10	0	1020	4
	Radar Interference	0	1	0	1	11	1
	Radar DoS	1	0	0	1	11	1
	Radar Black Hole	100	1	1	0	1011	4

Table 5.3: Full Assessment With Asset/Threat Pairs(*SA = Security Attribute, TL = Threat Level, IL = Impact Level, SL = Security Level*)

Asset	**Threat**	**SA**	**TL**	**IL**	**SL**
V2V	GPS Spoofing	Authenticity	1	3	Low
	Masquerading	Authenticity	1	4	Medium
	Broadcast Tampering	Authenticity	1	2	Low
	Black Hole	Authenticity	1	4	Medium
	Replay	Authenticity	1	3	Low
	Transaction Tampering	Authenticity	1	2	Low
	DoS	Availability	3	4	High
	Malware	Availability	2	4	High
	Spamming	Availability	3	1	Low
Radar	Radar Spoofing	Authenticity	2	4	High
	Radar Jamming	Authenticity	2	4	High
	Radar Interference	Availability	3	4	High
	DoS	Availability	1	2	Low
	Black Hole	Authenticity	1	4	Medium
RadSec	GPS Spoofing	Authenticity	1	2	Low
	Masquerading	Authenticity	1	4	Medium
	Broadcast Tampering	Authenticity	1	1	Low
	Black Hole	Authenticity	2	2	Medium
	Replay	Authenticity	1	2	Low
	Transaction Tampering	Authenticity	1	2	Low
	DoS	Availability	2	2	Medium
	Malware	Availability	2	4	High
	Spamming	Availability	3	1	Low
	Radar Spoofing	Authenticity	1	4	Medium
	Radar Jamming	Authenticity	1	4	Medium
	Radar Interference	Availability	3	3	Low
	Radar DoS	Availability	1	2	Low
	Radar Black Hole	Authenticity	1	4	Medium

Table 5.4: Simulation Parameters

Parameter	Value
Chirp duration (T)	**77.5 μs**
Frame duration (T_f)	**50 ms**
LRR Bandwidth	**800 MHz**
MRR Bandwidth	**250 MHz**
Radar Cross Section	**10 dBsm**
Radar power (P_c)	**10 dB**
LRR FoV Azimuth	**20 degrees**
MRR FoV Azimuth	**150 degrees**
Carrier frequency	**79-80 GHz**
Antenna gain (G)	**13-30 dB**
LRR Range	**197 m**
LR Communication Range	**979 m**
MRR Range	**96 m**
MR Communication Range	**130 m**
Thermal noise temperature (T_0)	**290K**
Receiver noise figure	**10 dB**
Communication Bandwidth (B_c)	**15 MHz**
Communication Power (P_c)	**23 dB**
Packet Size	**4800 bits**

5.2 Simulation Results

Two different scenarios were detailed in Section 3.4. The attacker vehicle starts at (-180, -2) and travels forward at a constant speed of 60 m/s. The victim vehicle travels at a constant speed of 30 m/s. In the first scenario the victim vehicle starts at (-90, 2). In the second scenario, a helper car starts at (-60, -6) is added, which also travels at a constant speed of 30 m/s. In the simulations, we test both radar jamming and communication DoS attacks. Our security metrics are the fraction of secure RCUs and the percentage of the secure area. The fraction of secure RCUs refers to the amount of RCUs not affected by an attack. As an example in scenario 1, if the victim vehicle is attacked on three of its RCU units then the percentage of secure area would be 50% as 1 - 3/6 = 0.5. We define the fraction of secure RCUs as f_{sec} for simplification.
$f_{sec} = \frac{RCU_t - RCU_a}{RCU_t}$, where RCU_t is the total number of RCUs and RCU_a is the number of atttacked RCUs.
The percentage of secure area is similar but instead of counting the number of attacked RCUs we calculate the area that each RCU could cover for each attacked RCU and then divide by the maximum possible area (when no RCU units are attacked). We define the percentage of secure area as A_{sec} for simplification.

First of all we have the graphs that show f_{sec}, Figure 5.1 and 5.2. The distance between the attacker and the victim is denoted by d_{av}. On the y-axis we have f_{sec}.

As we can see in the beginning of Scenario-I when the attacker is further away from the victim vehicle it seems like more RCU units are affected by the attack. In the beginning of Scenario-I we can observe that f_{sec} is low at the start when the attacker is far away and able to target both the back radar, the two back corner radars and the front corner radar on the same side as the attacker vehicle. Then more units become secure when the attacker vehicle is between or by the side of the victim vehicle. However there is also a point at $d_{av} = 0$ where the attacker car is just at an angle where it is able to target another corner radar unit. In the end when the attacker passes the other vehicle the amount of secure RCUs decreases once more. This is due to the attacker vehicle not being able to attack the front or back radars when it is on the side of or in between the victim vehicles, therefore the corner radars that face the attacker vehicle are insecure at that point but the other units should be secure at that point of distance.

Scenario-II is slightly different, in the beginning of the scenario there is a difference in the amount of secure units from Rad and Com attacks due to the difference in range of the signals. Otherwise it is similar in that the vehicles become more secure when the attacker vehicle is close and between the victim and helper vehicles. The attacker vehicle is between them at $d_{av} = 0$ to 50.

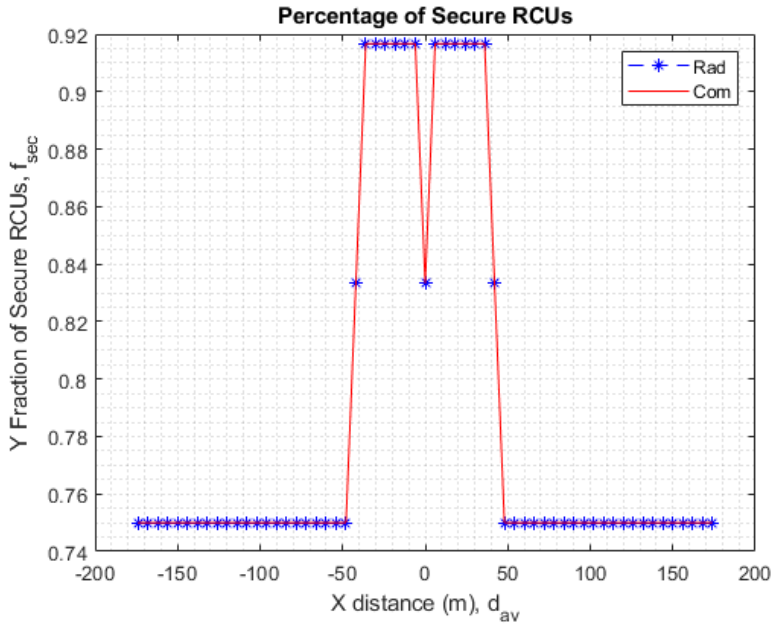


Figure 5.1: Percentage of RCUs not attacked in Scenario-I. The fraction of secure RCUs f_{sec} is on the y-axis while the distance in m from the victim vehicle to the attacker vehicle, d_{av} is present on the x-axis.

Figures 5.3 and 5.4 shows A_{sec}. On the y-axis we have A_{sec}. On the x-axis we have d_{av}. Figure 5.1 shows a similar shape to the RCU unit graphs but we can also notice that the area for the communication part seems to be more affected. This is related to the area calculation formulas. Since the areas are circle sectors they can be calculated by $Area = r^2 \cdot FoV/2$. The Azimuth angle of the FoV stays the same for both

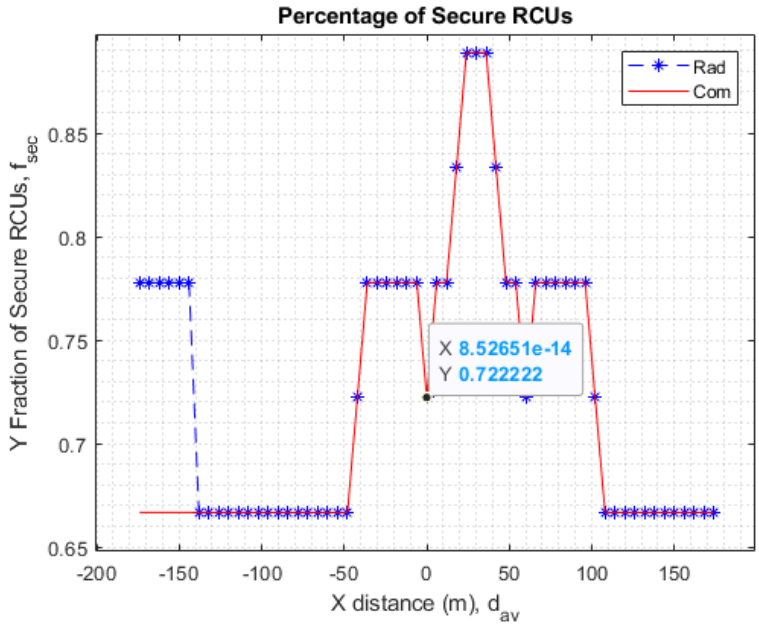


Figure 5.2: Percentage of RCUs not attacked in Scenario-II. The fraction of secure RCUs f_{sec} is on the y-axis while the distance in m from the victim vehicle to the attacker vehicle, d_{av} is present on the x-axis.

signals , however since the range for the communication is much longer for the front radars compared to the radar range there therefore becomes a difference in the area percentage since the corner radars do not share the same proportional difference. Essentially with Com signals one corner RCU unit might take up around 10% of the area for a vehicle while for a radar signal it is around 15%. Those are not the exact percentages and are simply meant to give understanding of the underlying principles of how the metric works. Figure 5.4 compares A_{sec} with and without RadSec. It is observed that the amount of secure area stays higher than when RadSec is not used for all of the scenario as sensor data is shared between the victim vehicle and the helper vehicle. Other than that we see a similar shape to Figure 5.2.

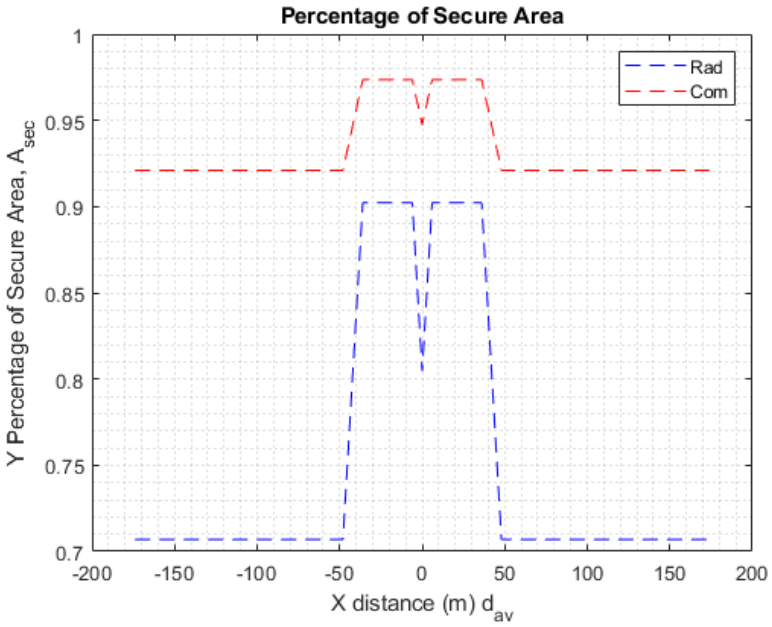


Figure 5.3: Percentage of Secure radar/com area, A_{sec} in Scenario-I,The percentage of secure area A_{sec} is on the y-axis while the distance in m from the victim vehicle to the attacker vehicle, d_{av} is present on the x-axis.

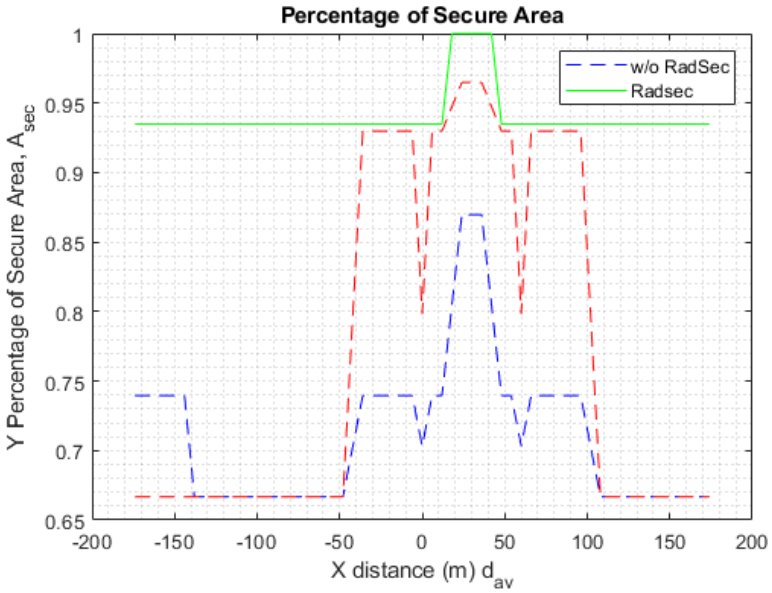


Figure 5.4: Percentage of Secure radar/com area, A_{sec} in Scenario-II,The percentage of secure area A_{sec} is on the y-axis while the distance in m from the victim vehicle to the attacker vehicle, d_{av} is present on the x-axis.

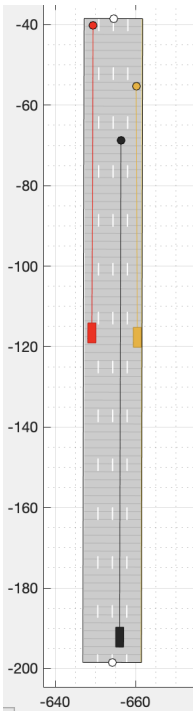


Figure 5.5: A possible use case for RadSec in the case of a V2V DoS attack. Here the black vehicle sends out a DoS Attack towards the red and yellow vehicles. Since they are linked with their front corner radars they can still communicate.

5.3 A Qualitative Discussion of Use Cases with RadSec

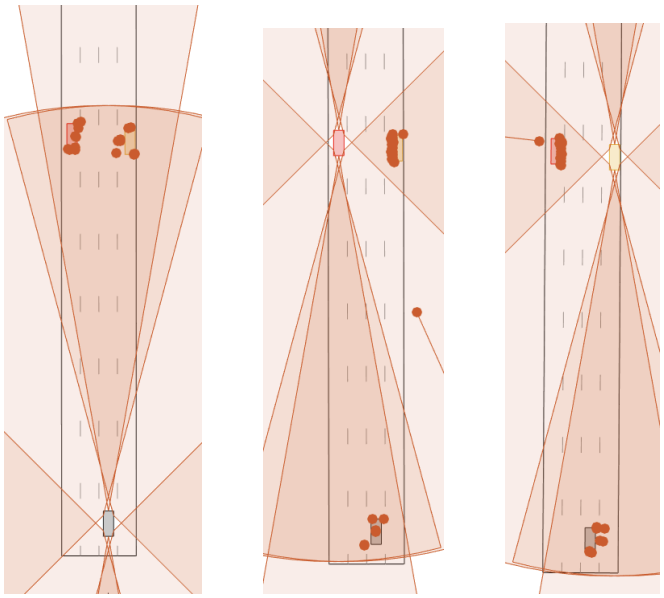
5.3.1 Use Cases for Communication

This use case is illustrated in Figure 5.5, the black vehicle is performing a DoS attack, and both the red and yellow vehicles are within the attack range. With DSRC only, the two vehicles need to turn off their DSRC, and then they are not able to send or receive any message. In Figures 5.6a, 5.6b and 5.6c, we can observe the vision of radars for each vehicle. Note that each vehicle has a visual of the other two vehicles.

With RadSec, vehicles have directed radar-communication units (RCUs). So they only need to turn off the units communicating with the black vehicle - their back RCU, back left corner RCU, and back right corner RCU, and keep their front RCU, front left corner RCU, and front right corner RCU working. In this case, the red vehicle and the yellow vehicle are still able to communicate with each other.

5.3.2 Use Cases for Radar

The first radar use case is illustrated in Figure 5.7a. In this case, the black vehicle sends a jamming signal in all directions. The radar vision cones of the black vehicle

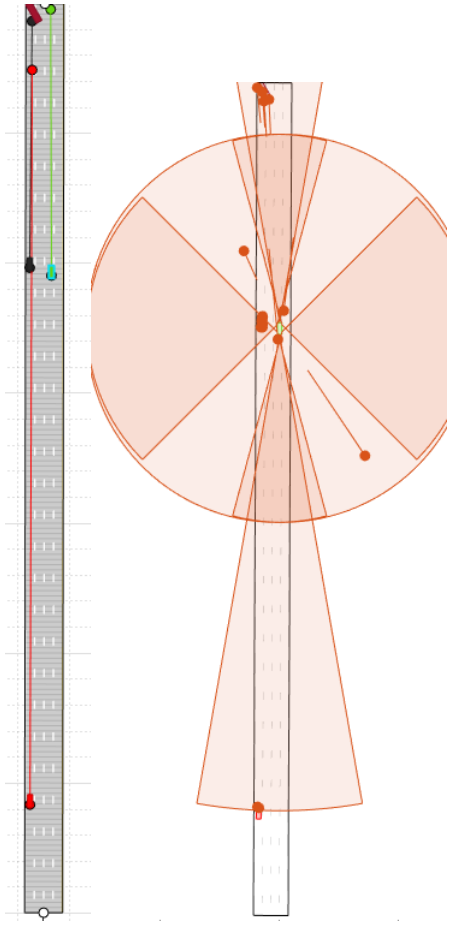


(a) (b) (c)

Figure 5.6: Vision cones for the three vehicles in the V2V RadSec use case. In (a) we can observe the vision cones for the black attacker vehicle. (b) and (c) contain the vision cones for the other two vehicles.

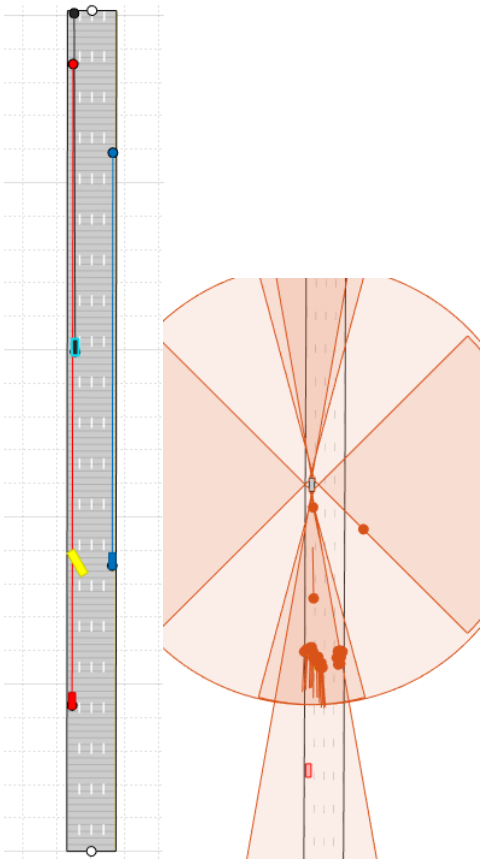
are illustrated in Figure 5.7b. However, the green vehicle next to it will still have unblocked radar sensors forward and backward. It will therefore be able to see the truck blocking the path further ahead and will be able to pass that information backward with the unjammed sensors. The red vehicle, which is far behind, will be able to get this information as it is outside the range of the black vehicle.

The second radar use case is illustrated in Figure 5.8a. Here the black vehicle sends a spoofing signal, making the red vehicle see an obstacle in front of it (yellow box). The radar vision cones of the black vehicle are illustrated in Figure 5.8b. The blue vehicle next to the obstacle can see through it with its backward corner radar and can communicate that there is no obstacle there, thereby preventing the spoofing attack.



(a) **(b)**

Figure 5.7: Here are illustrations for the first radar use case of RadSec. The black vehicle sends a jamming signal in all directions. The green vehicle has unblocked front and back radars and can therefore communicate in both of those directions to show that there is an obstacle ahead. The vision cones of the green vehicle can be seen in (b).



(a) (b)

Figure 5.8: This second use case illustrates how RadSec can be useful in spoofing attacks. Here the black vehicle sends a spoofing signal with its back radar which causes the red vehicle to see an obstacle (yellow box). With the help of communication signals of the blue vehicle it can understand that there is no obstacle in front of it.

6
Conclusion

Here we summarize the work done in the thesis and also discuss possible future work that could be done.

6.1 Summary

We started the project by performing a risk assessment on radar, V2V and RadCom automotive technologies. We investigated the different risks and possible impacts of each threat to determine which ones should be prioritized when it comes to security. As a result, we found that some of the threats to radar and V2V could be mitigated using RadCom. Specifically, High Risk threats such as spoofing, jamming and DoS could be solved using the directional RCUs by sharing sensor data. We also suggested adding authentication to prevent various tampering attacks and black hole attacks.

Furthermore, we discussed how the authentication and sharing of sensor data could be added to the already existing protocols to enhance security. We then proceeded to design simulations to test some of the possible attack scenarios with radar jamming and DoS attacks. To do this, we set up a MATLAB simulation and calculated links between sensors of different vehicles while gathering metrics about the attacks. From this we could notice that in cases where multiple cars are being attacked using radar or V2V attacks, the attacks could be slightly mitigated using the new RadSec protocol. In Scenario-II we could clearly see that the percentage of secure radar/communication area when using RadSec was much higher than when simply using radar or V2V communication separately. This does not remove the attacks entirely, but since the attacks themselves rely on denying the victims information, we can state that the protocol successfully mitigates the some of the attacks. We also discussed some other use cases where RadSec helps mitigate attacks that would otherwise work on separate radar/communication systems.

6.2 Future Work

The first thing that should be prioritized for any future work should be to think of more scenarios using a wider range of attacks. Not only would it be useful to simulate other attacks such as radar spoofing attacks, but it would also be interesting to observe what happens when multiple different attacks are used at the same time. What happens when one attacker car sends jamming signals and another

sends spoofing signals to confuse sharing of sensor data?

Another important part that we could not fit into the scope of this thesis would be to test the performance of RadSec compared to RadChat to see if the new security additions negatively affect performance. This will be to see if the protocol gets slowed down noticeably.

Another possible addition to security could be zone encryption [42]. This is a fairly new technology that does not seem very popular, yet the addition of encryption based on geographical zones could be helpful as it would prevent attackers from listening to V2V broadcasts. This would help prevent replay attacks, but in general, withholding information from attackers is a good thing.

Bibliography

[1] M. Mete, "FMCW-based automotive radar communications for intersection and real-traffic scenarios," 2020.

[2] T. van Eoermund, "Secure connected cars for a smarter world," tech. rep., Whitepaper, NXP Semiconductors, 2015.

[3] J. Liu, C. Yan, and W. Xu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles." DEF CON, 2016. https://doi.org/10.5446/36252 $Lastaccessed : 11Feb2021$.

[4] A. Karahasanovic, "Automotive cyber security," Master's thesis, Chalmers University of Technology, Computer Systems and Networks, 2017.

[5] B. M. Laurendeau C., "Threats to security in DSRC/WAVE," 2006.

[6] B. Paul, A. R. Chiriyath, and D. W. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. 5, pp. 252–270, 2017.

[7] A. R. Chiriyath, B. Paul, and D. W. Bliss, "Radar-communications convergence: Coexistence, cooperation, and co-design," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 1, pp. 1–12, 2017.

[8] I. Sumra, H. Hasbullah, and J.-L. Ab Manan, "Effects of attackers and attacks on availability requirement in vehicular network: A survey," pp. 1–6, 06 2014.

[9] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[10] M. Ball, "GPS Spoofing Test System Developed for Autonomous Vehicles," May 2019.

[11] M. Islam, A. Lautenbach, C. Sandberg, and T. Olovsson, "A risk assessment framework for automotive embedded systems," in *CPSS '16*, 2016.

[12] C. Aydogdu, M. F. Keskin, N. Garcia, H. Wymeersch, and D. W. Bliss, "RadChat: Spectrum Sharing for Automotive Radar Interference Mitigation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 1, pp. 416–429, 2019.

[13] C. Aydogdu, M. F. Keskin, and H. Wymeersch, "Automotive Radar Interference Mitigation via Multi - Hop Cooperative Radar Communications," in *2020 17th European Radar Conference (EuRAD)*, pp. 270–273, 2021.

[14] C. Aydogdu, H. Wymeersch, and M. Rydström, "Can Automotive Radars Form Vehicular Networks?," in *2020 IEEE Radar Conference (RadarConf20)*, pp. 1–6, 2020.

[15] E. R. Yeh, C. Bhat, R. Heath, J. Choi, and N. G. Prelcic, "Security in automotive radar and vehicular networks," *Microwave Journal*, vol. 60, pp. 148–164, 2017.

[16] everythingRF, "Automotive radar frequency bands."
[17] C. A. S. Authority, "Primary and secondary radar."
[18] M. I. Skolnik, *Radar Handbook*. New York: McGraw-Hill Education, 3 ed., 2008.
[19] C. Wolff, "Frequency-modulated continuous-wave radar."
[20] NASA, "Doppler shift."
[21] P. Kumari, J. Choi, N. González-Prelcic, and R. W. Heath, "Ieee 802.11ad-based radar: An approach to joint vehicular communication-radar system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3012–3027, 2018.
[22] V. D. Khairnar and K. Kotecha, "Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment," *International Journal of Network Security & Its Applications*, vol. 5, Mar 2013.
[23] Y. Han, E. Ekici, H. Kremo, and O. Altintas, "Automotive Radar and Communications Sharing of the 79GHz Band," in *Proceedings of the First ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, CarSys '16, (New York, NY, USA), p. 6–13, Association for Computing Machinery, 2016.
[24] Y. Zeng, Y. Ma, and S. Sun, "Joint radar-communication with cyclic prefixed single carrier waveforms," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4069–4079, 2020.
[25] R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," 2014.
[26] "USRP N210," tech. rep., Ettus Research, 2021.
[27] R. Q. Qiyi He, Xiaolin Meng, "Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles," *ournal of Advanced Transportation*, vol. 2020, 2020.
[28] J. S. Warner and R. Johnston, "GPS Spoofing Countermeasures," 2003.
[29] T. Iwata, J. Song, J. Lee, and R. Poovendran, "The AES-CMAC Algorithm." RFC 4493, June 2006.
[30] S. M. Patole, M. Torlak, D. Wang, and M. Ali, "Automotive radars: A review of signal processing techniques," *IEEE Signal Processing Magazine*, vol. 34, no. 2, pp. 22–35, 2017.
[31] C. Wolff, "The radar range equation."
[32] C. Aydogdu, N. Garcia, and H. Wymeersch, "Radar communication for combating mutual interference of fmcw radars," in *IEEE Global Communications Conference (GlobeCom)*, 2018.
[33] R. Soja, "Automotive security - white paper," 2014.
[34] A. Bolovinou, U. Atmaca, A. T. Sheik, O. Ur-Rehman, G. Wallraf, and A. Amditis, "Tara+: Controllability-aware threat analysis and risk assessment for l3 automated driving systems," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, pp. 8–13, 2019.
[35] A. Le and C. Maple, "A simplified approach for dynamic security risk management in connected and autonomous vehicles," in *Living in the Internet of Things (IoT 2019)*, pp. 1–8, 2019.

[36] S. van Winsen, "Threat modelling for future vehicles: on identifying and analysing threats for future autonomous and connected vehicles," February 2017.

[37] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*, pp. 641–646, 2009.

[38] C. Aydogdu, N. Garcia, and H. Wymeersch, "Improved pedestrian detection under mutual interference by FMCW radar communications," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Workshop on 5G V2X Communications for Connected Autonomous Driving*, Sept. 2018.

[39] C. Aydogdu, M. F. Keskin, G. K. Carvajal, O. Eriksson, H. Hellsten, H. Herbertsson, E. Nilsson, M. Rydstrom, K. Vanas, and H. Wymeersch, "Radar interference mitigation for automated driving: Exploring proactive strategies," *IEEE Signal Processing Magazine*, vol. 37, no. 4, pp. 72–84, 2020.

[40] " Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON systems; Part 7: Design guide for elements of a TIPHON connection from an end-to-end speech transmission performance point of view. ETSI TR 101 329-7 V2.1.1 (2002-02)," report, European Telecommunications Standards Institute, 2002.

[41] P. Cleveland, "Why GPS spoofing is no threat autonomous navigation," June 2019.

[42] J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, and P. Towa, "Zone Encryption with Anonymous Authentication for V2V Communication," pp. 405–424, 09 2020.

A

Appendix 1

A.1 Code

A.1.1 CheckLink

```
function [linkstatus, location1, location2] = checkLink(car1
    , car2, sensor1, sensor2, sensorRange) %checks if sensor
    1 is can link to sensor 2.
location1 = car1.Position + sensor1.MountingLocation;
location2 = car2.Position + sensor2.MountingLocation;

range1 = 0;
range2 = 0;
if sensor1.RangeLimits(2) <= 80
    range1 = sensorRange(2);
else
    range1 = sensorRange(1);
end

if sensor2.RangeLimits(2) <= 80
    range2 = sensorRange(2);
else
    range2 = sensorRange(1);
end

linkstatus = false;

sensorAngle1 = mod(car1.Yaw + sensor1.MountingAngles(1),
    360);
sensorAngle2 = mod(car2.Yaw + sensor2.MountingAngles(1),
    360); %reverse the second angle to compare with dAngle
if pdist([location1; location2], 'Euclidean') < range1 &&
    pdist([location1; location2], 'Euclidean') < range2 %are
    the sensors in range
    dAngle1 = getAngle(location1, location2); %calc angle
        between sensor around x-axis
    dAngle2 = getAngle(location2, location1);
```

```
    if betweenAngles(sensorAngle1, sensor1.FieldOfView(1),
       dAngle2) %check if sensor1 is pointed in the right
       direction
        if betweenAngles(sensorAngle2, sensor2.FieldOfView
           (1), dAngle1)%check if sensor2 is pointed in the
           right direction
            linkstatus = true;
            return;
        end
    end

linkstatus = false;
end
end
```

A.1.2 CheckSensorOccluded

```
function [occluded] = checkSensorOccluded(car1, car2,
   obstacle, sensor1, sensor2) %check if obstacle is between
    sensor1 and sensor2
location1 = car1.Position + sensor1.MountingLocation;
location2 = car2.Position + sensor2.MountingLocation;
location1 = location1(1:2);
location2 = location2(1:2);


if pdist([location1; location2], 'Euclidean') > pdist([
   location1; obstacle.Position(1:2)], 'Euclidean') %Is the
   obstacle closer than the 2nd car?
    corners = [ [obstacle.Position(1:2) + [ obstacle.Length
       /2, obstacle.Width/2]] ,...
                [obstacle.Position(1:2) + [ obstacle.Length
                   /2,-obstacle.Width/2]] ,...
                [obstacle.Position(1:2) + [-obstacle.Length
                   /2, obstacle.Width/2]] ,...
                [obstacle.Position(1:2) + [-obstacle.Length
                   /2,-obstacle.Width/2]] ];
    angles = [getAngle(location1, corners(1:2)),...
              getAngle(location1, corners(3:4)),...
              getAngle(location1, corners(5:6)),...
              getAngle(location1, corners(7:8))  ]; %get
                 angle between sensor and all the corners of
                  the obstacle
```

```
    maAngle = max(angles);
    miAngle = min(angles); %might need to check if there is
       some reverse here
    dAngle = getAngle(location1, location2);
    if maAngle - miAngle > 180
        if dAngle < miAngle && dAngle > 0 || dAngle >
           maAngle && dAngle < 360
            occluded = true;
            return;
        end
    elseif dAngle > miAngle && dAngle < maAngle
        occluded = true;
        return;
    end
end
occluded = false;
end
```