Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 3, July 2021:1891- 1909

Research Article

Implementation of a Cost Efficient Passive Keyless Entry Device for the Communication Protocol

[*]J Ravindra babu [a], K Srinivas [b], Mohammed Ismail B [c], Aatif Jamshed [d] and Asmita Dixit [e]

Associate professor, P V P Siddhartha Institute of Technology, Kanuru, Vijayawada, India.

Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India.

Associate Professor Department of Information Technology, Mangattupramba campus, Kannur University, Kerala, India.

Assistant Professor, Information Technology, ABES Engineering College, Ghaziabad, Uttar Pradesh, India.

Assistant Professor, Information Technology, ABES Engineering College, Ghaziabad, Uttar Pradesh, India.

jrb0009@gmail.com *

Abstract:

The susceptibility to relay attacks is a major safety risk in modern vehicles, due to the system for responding to challenges, such as those used in the Passive Keyless Entry (PKE) of most commercial cars. This form of attacks requires a long-range contact between a vehicle and its key, which circumvents encryption and unlocks the vehicle without direct access to the key. While a number of defences have in recent years been proposed, many are not robust or realistic. Any feasible system is likely to rely on a non-easily manipulated environmental parameter. The device must also be: cost efficient; simple to implement; and take comfort into account, for example the life of the main battery. This work implements and assesses a Relay Attack-resistant PKE device, analyses several of the suggested feasibility strategies in literature, as well as proposes a new method: Curve matching approach. The most promising methods have been concluded: immobility identification, distance limitation protocols and curve-matching approaches - the first of which is to be implemented in the PKE-system prototype. Instead of traditional RFID, the project introduces a PKE device and uses Bluetooth to implement the communication protocol. Disturbance detection is then applied using an accelerometer. The final device is subsequently checked and measured. It is found to be easily implementable, cost-efficient and can improve the protection of PKE systems, although immobilisation detection is not entirely effective. Finally, the recommendation is that manufacturers should employ immobility detection promptly while exploring techniques that are potentially more successful, though uncertain.

1. Introduction

In India alone there are near five million registered, in use, personal vehicles [1]. Approximately one vehicle for every two individuals [2]. The rapidly increasing connectivity of these vehicles and the shift from mechanical to electronic and wireless systems gives rise to new security vulnerabilities. Modern methods of car theft are a prime example of newly digitalized exploits owing to the spread of digital lock systems. The Remote Keyless System (RKS) has all but replaced the previous mechanical lock mechanism in cars with its Passive Keyless Entry (PKE) variant becoming standard in most high-end brands instead of its active counterpart. The traditional active RKS is a unidirectional system where the user unlocks the vehicle with a remote control, a.k.a. 'key fob'. The PKE System, unlocks the car automatically as the user approaches the vehicle with the key fob - without the need for any interaction with the user interface. It employs bidirectional communication where the car sends a wake-up signal to the key when it is within range (commonly under 1 meter) and the driver takes hold of the handle, proceeded by a challenge response from the key which, if correct, will unlock the vehicle. A similar check may be performed in order to start the vehicle [3, 4].

This system increases user comfort due to the eliminated interaction and with the encryption algorithm and challenge-response technique that is employed in most recent implementations, assures high resistance to many methods of attacks. However, it is not secure against relay attacks - also known as Mafia Fraud - and Signal Amplification Relay Attack (SARA) which are attacks that do not require decryption and are not affected by the encryption algorithm's complexity, nor can they be eliminated using alternative protocols [4, 5]. A review by Gulsever of Up stream's, a cyber security companies, repository consisting of security incidents relating to the automotive industry show 187 exploits related to connected cars with 25 unique attack vectors (paths that allow an attacker to gain access to a system) identified [6]. RKS vulnerabilities accounted for the largest number of them as well as having the largest ratio of 'black hat' (malicious as opposed to 'white hat' - research) attacks. Various suggested security features exist that could protect a PKE System from relay attacks. These include context-based systems using relative position of car and key fob, comparison of Wi-Fi access point lists, Global Positioning System (GPS) coordinates etc [7, 8]. This work analyses these proposed defences as well as suggests a novel way of protection, constructs a prototype system with the chosen method - Immobility Detection and evaluates said system.

2. Background

The following chapter outlines all the required information for complete analyses of the proposed defences. Understanding current PKE implementation - into which any defense must be integrated - both in terms of limitations and potential is crucial for assessing viability of any system. In order to judge the effectiveness of proposed strategies the chapter also presents a high-level overview of relay attacks.

2.1 Passive Keyless Entry

A. Overview

The PKE system, replacing the active remote keyless entry system that preceded it, was first introduced in 1998 by Mercedes Benz and is considered to increase comfort of use as it negates the need for a key press when unlocking the vehicle [9]. Instead, PKE systems allow users to unlock the doors by approaching the vehicle and grabbing the door handle with the key fob on their person. There are variations in protocol and exact implementation, but the following steps demonstrate a typical version [10]:

- The car periodically broadcasts a wake-up message on a Low Frequency (LF) RFID channel, approximately around 130 kHz, probing for nearby keys [11].
- As the key fob approaches the vehicle and enters the LF RFID's effective range it receives the wake-up message and is powered on by inductive coupling from the car's signal. It will respond with an acknowledgement on an Ultra High Frequency (UHF) RFID, around 315MHz (this is done in order to save power).
- The car proceeds to send a challenge (essentially a request for the password) via LF RFID including an identifier to the car.
- The key receives the challenge and, if the identifier matches the key's, responds with the challenge response.
- The car then unlocks - assuming that the challenge response is accepted.

While variations on this system exist, such as omitting the wake-up or requiring double verification, the core functionality is the same across manufacturers [12].

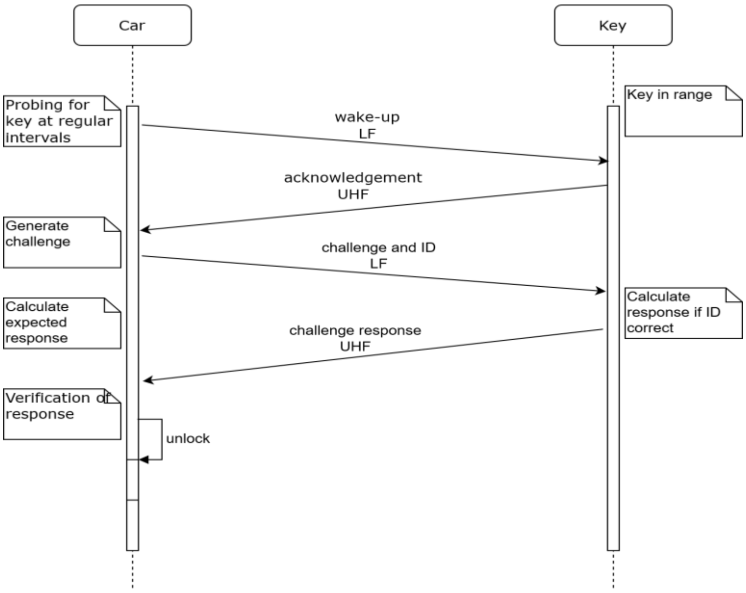

Figure 1: Protocol diagram of typical PKE system.

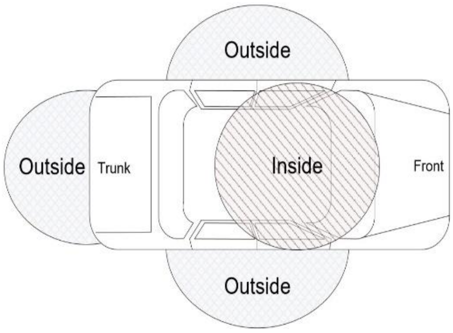

Figure 2: Inner and outer RFID zones.

For this, two RFID zones are required, as depicted in Figure 2, with one reaching outside of the car (generally in a range no more than one meter from the doors) for unlocking and one exclusively on the inside of the vehicle for starting the engine. Note that while the LF zones are strictly in a few meters' radius around the car the range of the UHF transmitter can be significantly larger [13, 14].

B. Encryption

While this paper does not focus on the encryption algorithms used in PKE systems it is briefly summarized as follows: Both the vehicle and the key fob share a secret hardware key unique to a manufactured vehicle. When the key fob has acknowledged that it is in range the car generates a pseudo-random code to be transmitted as the challenge. The key receives the challenge and uses it to generate a response using a cipher such as KeeLoq or DST [8]. During this time the car will also generate the response and compare it to the received response from the key. In theory, this is a one-way operation which can neither be predicted, reverse engineered, or brute forced.

While the cryptography method used in PKE can itself be attacked [15], this goes beyond the scope of this paper; which assumes that the encryption method can be fully relied upon.

2.2 Relay Attacks

A. Overview

Relay attacks, also known as Mafia Fraud, have multiple forms, though all rely on the same fundamental principles. It is a man-in-the-middle attack, a method by which an agent (in this case a relay) steps between two (or more) devices and forwards (a.k.a. relays) signals between them, see Figure 3. This allows the agent to essentially pose as a trusted device without having to know any details of the secure communication. This type of attack is commonly employed with parked cars with the key in a relatively close range, such as inside a house or in the pocket of the driver at a store, cafe, or similar [3].

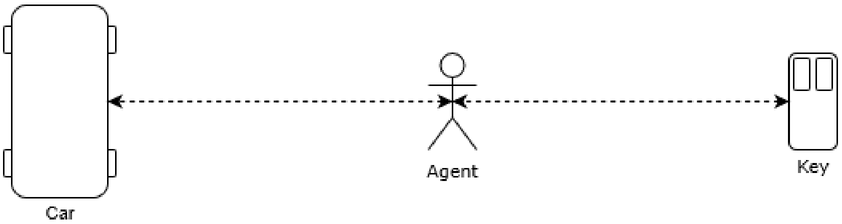

Figure 3: Agent entering between the car and key fob communication.

As mentioned previously, while the LF RFID needed to establish connection between the key and car has a range limited to approximately a meter from the vehicle, the range of the UHF response sent by the key can have a much greater range: analogous to actively unlocking the car with the button. This leads to certain systems being vulnerable to amplification attacks where a signal, in this case the challenge from the car, is amplified to the key. Since the car broadcasts the challenge periodically, without prior verification that the key is in range, this can be picked up by a relay device and amplified. The key receives the signal, verifies that it has the correct ID associated with the key, and responds to the challenge accordingly. If the car and key are within range of the UHF signal, such as in the driveway and inside a house, the car is immediately unlocked.

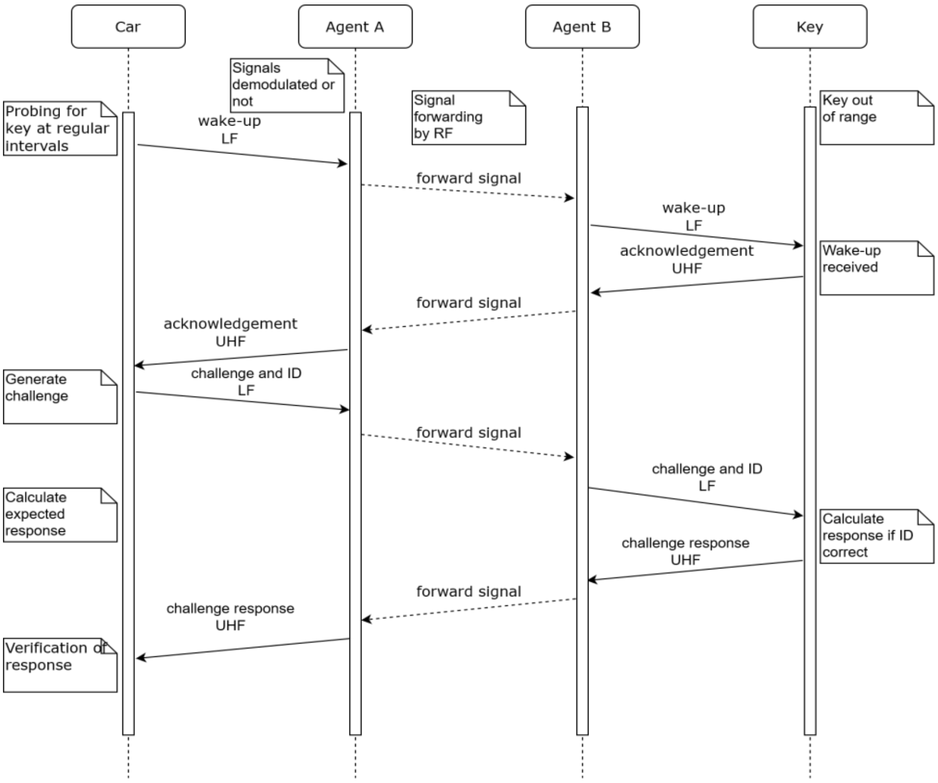

Figure 4: Protocol diagram of relay attack on PKE System.

In cases where the range of the UHF RFID is not sufficient, or where a vehicle with PKES is to be started and driven away, two agents are commonly needed. This is analogous to a SARA but relays bidirectionally. Figure 4 illustrates a modified version of Figure 1 illustrating this attack. Note that the effectiveness of relay attacks is not diminished by increased cryptographic complexity as no cracking of the cipher is needed.

2.3 Key Fob Design

A. Battery

When suggesting potential defenses against relay attacks it is crucial to put these into the context of existing systems and technical limitations. Battery limitations of the key fob are often ignored in otherwise rigorous studies, such as the paper published by J Wang et al. which suggests a combination of various defenses despite their unfeasibility in real-world applications, see Chapter 3 [16]. The main advantage of PKES systems over previous ones is comfort and simplicity which is negated if constant battery replacement becomes an issue.

While it is outside the scope of this paper to provide a detailed analysis of power consumption of key fobs it is necessary to have a basic estimate in order to verify the feasibility of the suggested defences. The 2018 Lexus NX300h is taken as an average vehicle with PKES; it uses a CR2032 button cell battery of 3 V and a capacity of 220 mAh [17]. According to the vehicle's user manual the batteries are generally expected to last one to two years [18,19]. As a very rough estimate for general comparisons it can be said to have a consumption of $220/(365 * 1.5) = 0.4$ mAh per day. This estimate can be used for evaluating the added power consumption of proposed solutions.

B. Wireless Technology

While specific frequencies differ due to regulations, the technology used for communication between the key fob and the on-board computer in the vehicle is generally the same for all manufacturers. An LF channel is used for wake-up while authentication is processed using a UHF channel. The nature of this technology allows for low power usage while idle, inductive coupling for wake-up, as well as a generally simple but robust interface.

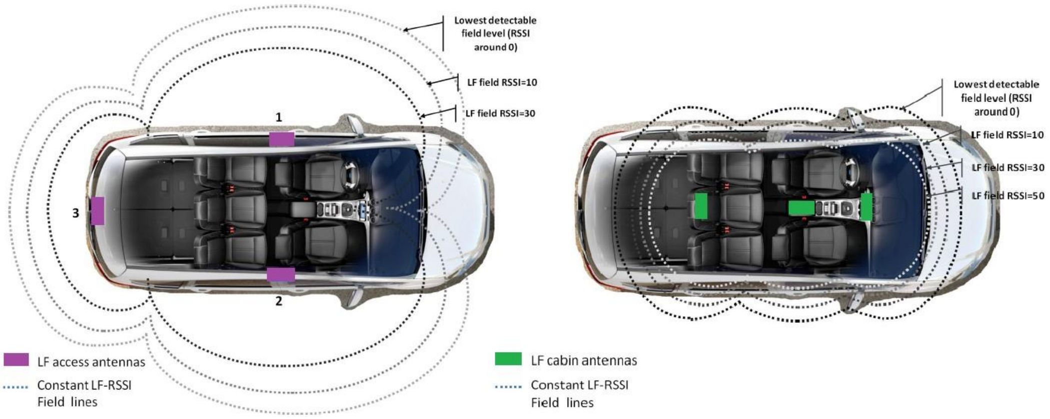
Lowest detectable field level (RSSI around 0)
LF field RSSI=10
LF field RSSI=30
1
3
2
LF access antennas
Constant LF-RSSI Field lines
Lowest detectable field level (RSSI around 0)
LF field RSSI=10
LF field RSSI=30
LF field RSSI=50
LF cabin antennas
Constant LF-RSSI Field lines

Figure 5: RFID beacons placed around the car interior and exterior.

A separate set of RFID transceivers may be present inside and outside of the car so that it can be determined if the key fob is within or without the vehicle, as seen in Figure 5. An alternative may be to simply create different zones in and around the car which can easily be distinguished between.

While most current manufacturers use RFID technology for their PKES systems, BLE is an emerging technology for secure access control and indoor positioning solutions. Unfortunately, distance measurements using Received Signal Strength Indicator (RSSI) or Rx power (received signal power, measured in dBm) have been consistently shown to be inaccurate. Mesh networks and trilateration techniques may increase accuracy, but these are not viable solutions for PKE systems. One study in a static indoor environment showed that due to the multipath interference caused by metallic surfaces distance measurements using BLE RSSI resulted in a mean absolute position error of approximately 1.2 m. While this may be sufficiently accurate for some applications it is not viable for a premium consumer product which is expected to be substantially more consistent.

However, in late 2018 Imec demonstrated a system using BLE that has excellent accuracy of distance measurement and claims to be immune to sophisticated distance manipulation that other defense measures are still susceptible [20,21]. With its low power consumption and potential for high accuracy BLE could come to replace

RFID based PKES systems. Furthermore, it can enable novel access control systems such as those needed for unlocking carpooling vehicles with mobile phones, or other access sharing applications.

3. Proposed Defences

The following defences are potential solutions to the vulnerabilities of PKES systems as proposed by this study and supported by previous research. Many effective defences employ context-based verification where there is an independent verification of an environmental parameter by the key fob and vehicle followed by a mutual authentication. If this parameter is chosen right, it is sufficiently complex and space variant that there exists a clear difference in its value near the car and some meters away. Ideally, the environmental parameter is also resistant to manipulation, or spoofing. While many of the following approaches are effective methods of protection on paper, the implementation of these is often not considered by other studies.

3.1 Received Signal Strength Indicator

Received Signal Strength Indicator (RSSI) is a measure of the approximate power level of a received signal. There exist suggestions to use this to verify proximity to the car, however, this is essentially already what is implemented by the LF RFID wake-up. The key only replies when it detects a signal with enough power. This is however easily duped using a relay attack or signal amplification relay attack.

3.2 Coordinate Tracing

This is a method proposed amongst others by S. Rizvi et al. where either the LF signal's RSSI or a different communication channel such as Bluetooth is used to triangulate the position of the key and compare it to that of the vehicles. There are a multitude of difficulties with this.

The first problem arises already with the implementation on the vehicle side. S Rizvi et al. proposes using the GPS already included in most cars' entertainment systems. This, if possible, at all due to regulations, would require a large overhaul of how access is managed to the vehicle's features while locked. A highly costly and unpractical operation. A further issue is that of accuracy. RSSI can be used for relative positioning but due to its inaccuracy and susceptibility to physical interference it is not suitable for exact positional measurements. Even assuming that the accuracy is sufficient, the solving of simultaneous equations needed for triangulation are extremely demanding and would require a more expensive chip in the key fob and cause greatly increased power consumption. This method, while theoretically sound, is practically impossible to implement. It is far too complex, computationally intensive, and even inaccurate.

3.3 GPS

One suggested defense against relay attacks is location verification using GPS. This proposes using the often already included GPS in the vehicle's on-board computer as well as an added GPS in the key fob for independent location measurements. The measured coordinates of the key can then be transmitted together with the wake-up acknowledgement or challenge response and compared by the vehicle with its known position. This would in theory allow verification of the distance between the devices.

This solution however has several major flaws. Firstly, the accuracy of GPS measurements may not be suitable precisely for this type of close-range application. GPS is intended to provide specific location measurement with a guaranteed accuracy in the United States of under 7.8 meters with 95% certainty. While the reported accuracy is greater than this, hardware quality, interference, weather conditions, and other factors can greatly influence the effective accuracy. This is far from accurate enough for definitive protection against relay attacks where distances of a few meters can be crucial. GPS can furthermore be susceptible to spoofing attacks [22].

A further problem with implementing a context-based verification grounded on GPS technology is the power consumption of the GPS module and accompanying calculations. As an example, the ZOE-M8B, see Appendix A, released in 2019, marketed as a compact low power chip, has a typical power requirement of tens of mAs while active. A consumption far from negligible. Furthermore, it has a long" Time-To-First-Fix" (the time taken to calculate a position after start-up) with around 30 seconds" cold-start" (without previously saved GPS data, used unless previous position is similar). Moreover, this module is rather expensive, costing above 10 Euros. While it claims to possess spoofing detection, a feature enabling it to detect if the GPS signal is manipulated externally such as an attacker might do to bypass the verification system, it does warn that this may not detect all spoofing attempts. Furthermore, the accuracy of this specific module is likely not sufficient, claiming accuracy to around 3 meters.

3.4 Distance Bounding

A potential solution to access control, not only in PKE systems but for any wireless or wired application relying on an untrusted prover needing to prove proximity, is distance bounding. This is a method of determining an upper limit to the physical distance a prover, in this case the key or attacker pretending to be the key, can be from the verifier: the car [24]. This is done by measuring the time for signal propagation from verifier to prover and back. If Radio Frequency (RF) is used then, due to nothing being able to communicate faster than the speed of light, the protocol can establish a physical upper bound for the distance between the devices with the only uncertainty arising from the processing speed of the prover. For every 1 ns delay due to processing, the window for the attacker - assuming they can act in zero-time - increases by 15 cm. This means that both the hardware, the protocol and the underlying function which is needed to guarantee the identity of the prover need to be highly optimised. The function applied to the challenge has a similar purpose as any encryption used for challenge response in current systems but must be significantly faster. Even a simple XOR adds time delays that render the protocol unusable.

The first distance bounding protocol for RFID was introduced in 2005 by Hancke and Kuhn with the first demonstration of a protocol with the required security features - to some degree at least - was done in 2010 by Rasmussen and Capkun [25]. Their implementation achieved processing in approximately 1 ns, resulting in an accuracy only 15 cm outside of the theoretical maximum. While the protocol has been shown to be susceptible to certain types of attacks there have been improved versions proposed. One such proposal and implementation by Hussein et al. is optimized for UHF RFID tokens and has greater security while maintaining a processing speed of 1 ns [26].

While distance bounding protocols are improving rapidly, they are not yet ready to be implemented commercially. The implementations so far have been highly experimental in nature. Furthermore, the effective frequency channels of such protocols are limited. Rasmussen and Capkuns set up for example were effective around 3.5 GHz but admitted to not being functional at lower frequencies. We can conclude that distance bounding as a protection against relay attacks has substantial potential in both PKE systems and other applications such as smart card readers but may not be a viable solution in the near future.

3.5 Immobility Detection

The situation where the vehicle is parked in the driveway with the key left near the door for the night is an ideal and, common scenario for attacks. Immobility Detection, implemented and evaluated in Chapter 4, uses an accelerometer built into the key fob to detect when the key has remained motionless for a given amount of time and enter a" sleep-mode" protecting from relay attacks. This method of protection is in the process of implementation by car manufacturers.

While this does not protect against all instances of relay attacks, such as when the key is in motion, it has several advantages over many alternative proposals. It is simplistic and conclusive. Implementation is trivial, and does not involve much calibration or need for extensive data gathering such as, for example, location-based solutions. It is also clearly and unambiguously defined in its effectiveness. While it does not provide complete protection, the cases it does protect from can easily be outlined. Furthermore, it is not an invasive alteration into the core functionality of the PKES System, with little to no modification needed, making it cost effective.

While the choice of concrete component for commercial implementation is irrelevant for this work, we can consider the AIS2DW12 accelerometer from STMicroelectronics as an example. A summary of the data-sheet can be found in Appendix C. The implementation presented in Chapter 4 uses a more common and easily implemented component, but is otherwise analogous. The above-mentioned accelerometer is, as claimed by the manufacturer, designed specifically for the automotive industry being highly resistant to all forms of abuse. With a current consumption in" power-down" mode of maximum 950 nA, and allowing for the powering down of other components when in" sleep-mode", there is no negative, and perhaps a somewhat positive, effect on battery life.

3.6 Approach Curve Matching

A potential defense that, as far as this project could determine, has not been suggested by other researchers is what this work entitles Approach Curve Matching. This novel method is a protection mechanism where the measured approach curves from the key are compared to that measured by the car to establish validity of the access request. There are a variety of possible implementations, but they all follow the same basic logic. The key and vehicle individually record the signal strength of each other as the user approaches the vehicle. This results in two discrete data sets with signal strength, indirectly measuring distance, as a function of time which can then be compared. Assuming the data sets compared are trusted, i.e., accurate and not fabricated by an attacker, we can clearly distinguish if the key approached the vehicle or not. A significant advantage of this method over Immobility Detection is being able to protect against relay attacks while the key is in motion, such as thefts in malls, outside stores, or in restaurants. In order for an attacker to bypass such a defence, they would need to ensure that the RSSI received by the key varies similarly in time as of that received by the car - a task potentially impossible owing to the strong effect environmental factors have on RSSI.

This method can have multiple variations. The signal strength data could be one-dimensional, measuring only the distance to a single receiver in the vehicle, or multidimensional. However, measuring signal strength while entering the vehicle may not provide a distinct enough fingerprint, or enough time for measurement. In this case it is possible to employ this defense only for keyless engine start, by allowing the data collection to proceed until the user enters the car. The characteristic signal pattern of a key approaching the car, opening the door, entering the vehicle, etc., especially if multiple receivers are present in the car, would likely be complex enough to thwart any relay attack. Any attempt to oversaturate the signal by an attacker could also be detected, for example by comparing the approach curve to expected user motion. Moreover, a machine learning algorithm could be trained to identify approach curves that do not match common user patterns.

Due to exact sampling time disparity and variations in the absolute value of the signal strength, Dynamic Time Warping (DTW) may be a suitable method for curve matching. However, due to the processor intensive nature of such an algorithm the data set from the key would likely need to be transferred to the vehicle's on-board computer for analysis. This also implies that - since the authenticity of the data set must be ensured - the data set must be transmitted encrypted. While the encryption and extra transmission has an effect on the battery life, the intensive computations are on the vehicle side where more processing and battery power is available. By using no new components (only the existing wireless chip is used) the overhead power usage is not increased. The large number of extra transmissions needed to guarantee a robust dataset to base the curve matching on does draw battery power, but even older and somewhat outdated Bluetooth and RSSI chips rate their Tx currents around 10 mA resulting in a significant but not prohibiting increase in power usage. The exact power consumption must be further investigated in order to determine the viability of Approach Curve Matching conclusively.

There are however multiple other challenges with Approach Curve Matching. The algorithm relies on the symmetry of wave propagation, i.e., that the signal will theoretically be affected the same way by environmental factors between the key and vehicle in both directions, but this may not be so in practice. Furthermore, shifts in discrete sampling may have a compounding negative effect on asymmetry. Due to this method employing a relatively complex algorithm, a large amount of calibration and testing would be required before a viable commercial product could be designed. The exact sampling rate, acceptance threshold, exact comparison algorithm, etc. would also have to be determined through lengthy testing and prototyping. The implementation of such a system into existing PKE systems is not as trivial as Immobility Detection. Therefore, while this work highlights the viability and encourages further study of this method it does not investigate it in depth.

4. Implementation

The following chapter presents the implementation of the PKE system. It details and motivates chosen hardware, software architecture, software logic and, finally, presents the results obtained.

A. Hardware

The following sections describe the hardware setup for the implementation of an Immobility Detection enhanced PKE system. While the exact setup is not identical to most commercial systems, it is equivalent in all aspects that could affect the defense systems effectiveness and implement ability. Decisions regarding hardware selection were based primarily on suitability for the project, economic viability, and ease of use.

Microcomputer

The microcomputer used was the Raspberry Pi Zero W: a low-cost single-board computer with inbuilt wireless (Wi-Fi and Bluetooth) capabilities. The computational power required for the authentication protocol and Bluetooth communication is very low with essentially only the encryption being a processor heavy operation. The actual chips used commercially in key fobs and on-board computers are naturally highly optimised for cost and performance but the Raspberry Pi is suitable for a proof of concept due to its ease of use. Furthermore, it has an abundance of General-Purpose Input/Output (GPIO) pins which make it preferable for prototyping.

Bluetooth Module

The Raspberry Pi Zero W has an inbuilt Cypress CYW43438 chip for wireless communication using Wi-Fi and Bluetooth, which was used. The project did not use the low-energy capability of Bluetooth 4.1 as power consumption was not considered for the physical prototype, but the implementation would not differ significantly with BLE. RSSI was used for distance measurements.

Accelerometer

The accelerometer used was a MPU6050 sensor which includes a 3-axis gyroscope and accelerometer. Communication with the chip is done through the System Management Bus (SMBus) - a commonly used serial bus for peripherals.

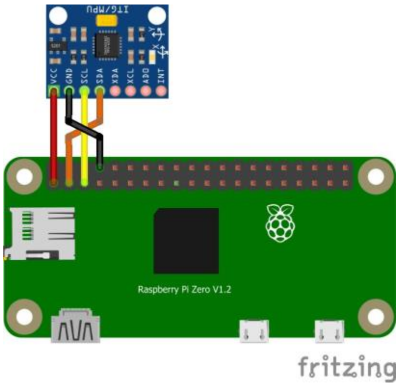

Figure 6: Connection diagram for the MPU6050 accelerometer to Raspberry Pi Zero.

Commercial products will likely employ more cost effective and resilient components such as the AIS2DW12 discussed in Chapter 3; however, the selected GY-521 is functionally identical. Since Immobility Detection does not require extremely high precision (any eventual uncertain output range during slight vibrations can be filtered with simple hysteresis) the selection of this component is not of particularly high importance. The connection diagram of the accelerometer to the Raspberry Pi can be seen in Figure 4.1. Ideally, the accelerometer would be checked only upon entering the required range from the car in order to establish if the key if in motion (since several readouts may be necessary this range could actually be slightly further than the distance needed for unlocking the vehicle). Upon entering range, the key must, per definition, be moving (unless an attacker is accessing the key); therefore, it is enough to activate the accelerometer then. However, due to a technical malfunction of the sensor during the project, where one of the three axes of acceleration measurements were lost, a workaround was implemented with the sensor active indefinitely and reporting movement upon fluctuation of the readout. Since power consumption and processing speed was not a priority of this project the alternative implementation did not have an impact on the outcome in any way.

Locking and Servo Motor

Due to project limitations, the locking mechanism was present only for demonstrational purposes. Since the lock system is completely separate from the PKE system, the complexity of the mechanism does not affect the underlying access control. The locking demonstrator uses a MG90S micro servo whose position indicates the locked/unlocked state of the vehicle. The servo control is achieved through Pulse Width Modulation (PWM) on the Raspberry Pi's GPIO pins. A duty cycle of 2% at 50Hz is used for setting the servo at 0°and 13% for rotating to 180°. A proposed CAD model can be seen in Appendix D. The models for the servo and horn were sourced online, while the rest of the mechanism was designed in Solid Edge.

B. Software

The following sections describe the software setup for the implementation of an Immobility Detection enhanced PKE system. The implementation was done in three releases. One for the base functionality consisting of the software needed for a PKE system without Immobility Detection, one with implemented Immobility Detection, and finally implementing the demonstrational locking mechanism. While certain features were omitted or greatly simplified, such as the encryption algorithm or excluding the initial button press before authentication begins often included in commercial systems, care was taken in order to ensure that the general software architecture and authentication protocol allowed for the implementation of such features. These include support for multiple keys and active RKS. The source code was written in Python and can be found in Appendices E and F.

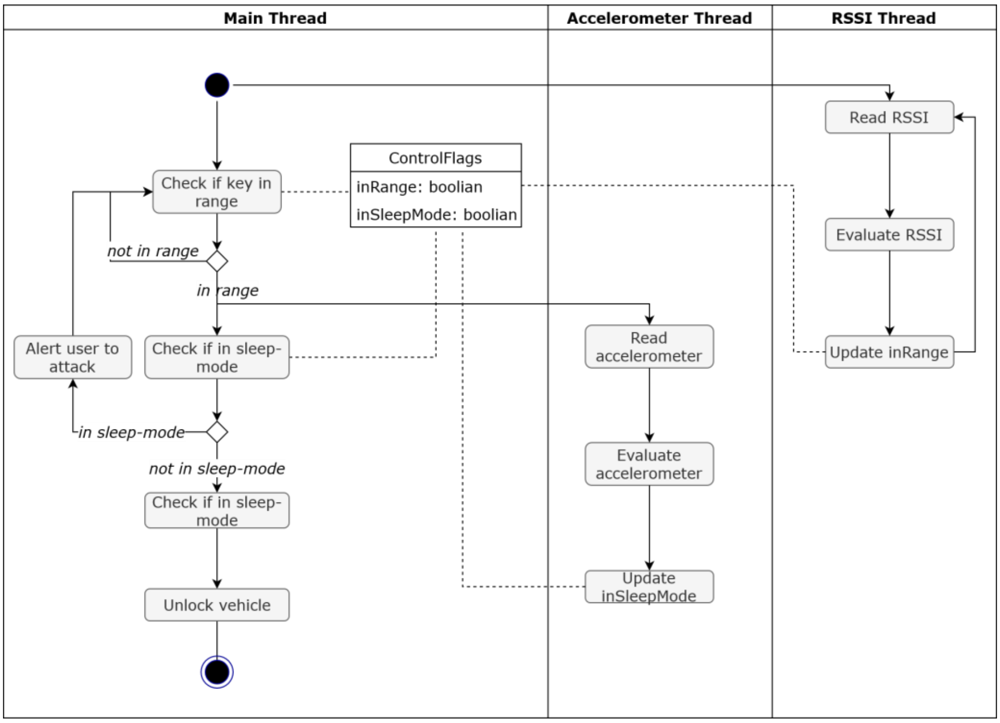

Figure 7: Activity diagram of the unlocking process for the improved PKE system with Immobility Detection.

Logic

The logic underlying the PKE system is based on existing commercial systems to a large degree. The Immobility Detection is a defence system easily implemented distinct from the base functionality which is, with the exception of some omitted features. Figure 4.2 depicts an activity diagram for unlocking the vehicle. The addition of Immobility Detection inserts an extra control after checking for proximity of the vehicle - using RSSI - where depending on the accelerometer readout either the authentication proceeds or the user is alerted to a potential attack. The alert can take any form, in this project it was sufficient to use a command-line message, but commercial systems would likely use an audible alert from the key fob.

Authentication Protocol

The authentication protocol for a successful unlocking by the intended user can be seen in the sequence diagram in Figure 4.3. The protocol can be described by the following steps:

1. The vehicle broadcasts a request for connection with its paired keys periodically, which is answered if the key is within a given range. This range may be the same or larger than the range needed for actually unlocking the vehicle, i.e., around one meter. The range is determined using RSSI, but can also be done by measuring Rx power.
2. Upon successful connection the car transmits a wake-up to the key - this step can be combined with connection but this project's implementation separates the two.
3. The key then assesses the accelerometer readouts and determines if it is in sleep mode. If so, it alerts the user and authentication may not proceed.
4. Assuming a normal use case, where the key is not in sleep mode, it confirms the wake-up.
5. The vehicle generates a cryptographic nonce and sends the challenge. While the key replies it calculates the expected response.
6. The key receives the challenge and calculates the response using its private hardware key, and transmits it back to the vehicle.
7. The vehicle compares the received response to the expected response and, assuming a match, unlocks the vehicle.

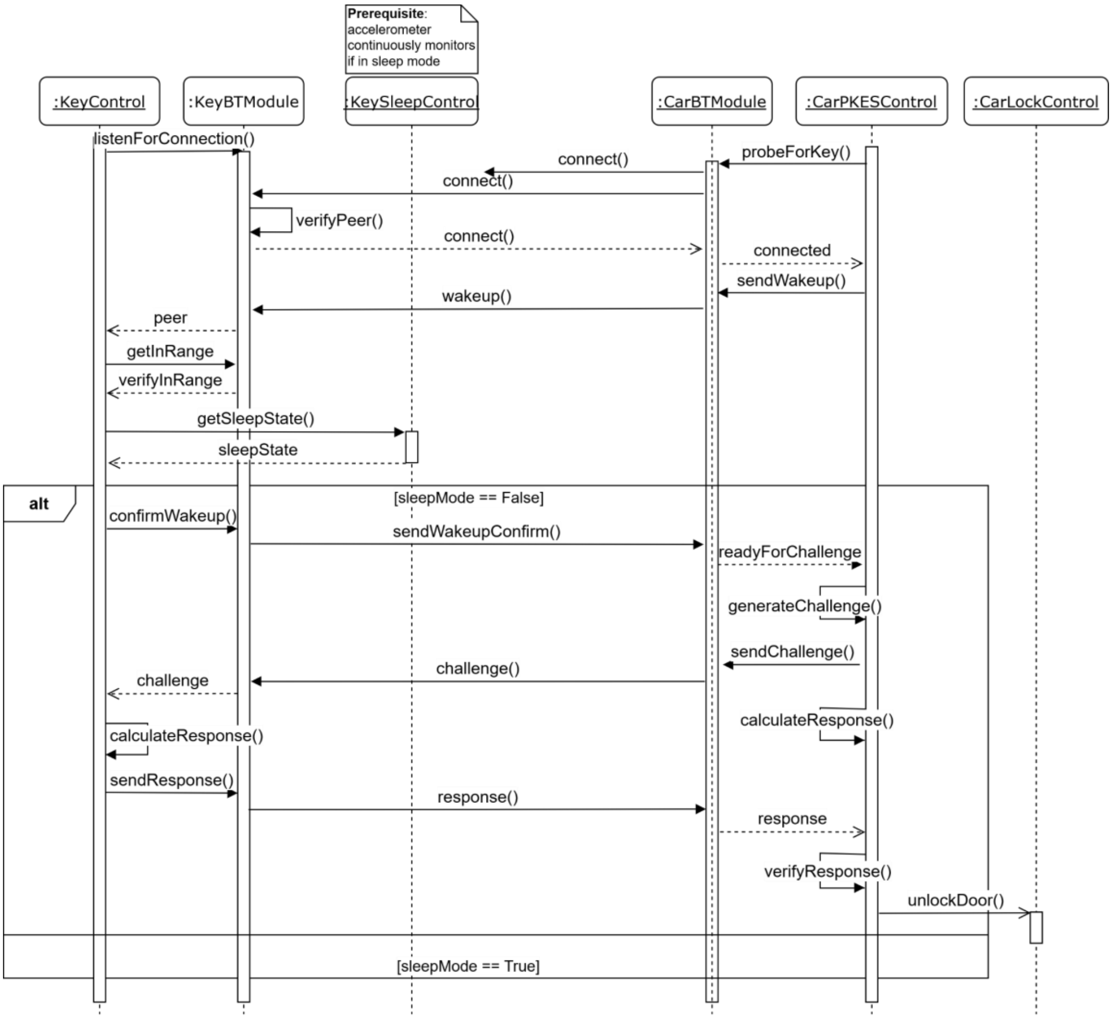

Figure 8: Sequence diagram of a successful unlocking sequence.

Software Architecture

The software for the PKE system is built-up by the software in the vehicle's onboard computer and that of the key fob. Python modules used worth mentioning are: PyBluez for interfacing with the Pi's Bluetooth resources and smbus for SMBus access through I2C for the accelerometer. The software was highly modularized - primarily for easy integration of new features - as well as for ease of development. Multi-threading was used for RSSI and accelerometer monitoring with periodic callbacks to the main Bluetooth and sleep-mode control modules to update the state of the key fob.

The key fob's software, see Appendix E, consisted of a main control module implementing the protocol logic with more specific functions delegated to other modules. The Bluetooth module implemented all necessary functions for communication such as: establishing connection, cleaning up Bluetooth sockets, and sending/receiving messages. The sleep-mode module similarly implemented all necessary functionality for monitoring the accelerometer and determining sleep-mode.

The software of the vehicle's on-board computer is much simpler. It is a two-state machine with a series of events as transition criteria from one state to the other (the authentication protocol).

Encryption

For the purposes of this project no secure encryption algorithm was implemented. As encryption does not influence the Immobility Detection system and the underlying logic it was deemed unnecessary. However, due to the protocol implementing a mock challenge-response, an unencrypted and non-random placeholder for a potential real challenge-response, the addition of such a feature would not alter the architecture of the software as a whole. Similarly, other desired features can easily be added to the system due to its modularity and regard for compatibility with omitted features.

5. Results and discussion

After developing the software and constructing the setup, as seen in Figure 4.4, the effectiveness of the implemented PKE system was assessed using a set of test cases for common use cases.

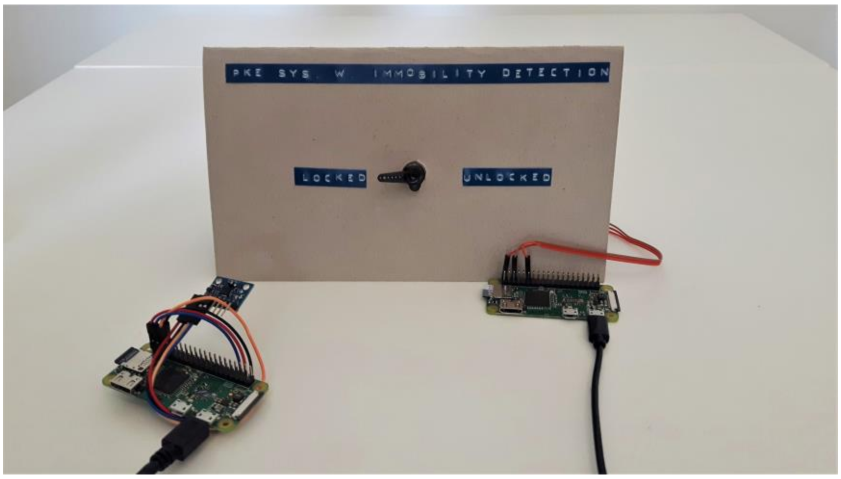

Figure 9: Prototype setup of the implemented PKE system with the key fob and accelerometer (left) and on-board computer and lock (right).

These include: the key entering communication range without getting close enough to unlock the vehicle; a complete unlocking procedure; complete locking procedure; the key entering sleep mode while in the vehicle; and a relay attack on the car while the key is in sleep-mode. All tests were performed successfully, with the system behaving as desired. It can be concluded that the PKE system worked as expected. While due to RSSI inaccuracies inherent with Bluetooth the effective range was variable, the system's response time was, from an end user perspective, immediate. The Immobility Detection system successfully protected against relay attacks while not impeding the function of the base PKE system.

However, the execution of the project also revealed insights crucial to this work. It was determined that existing PKE systems without any advanced form of protection against relay attacks can benefit from Immobility Detection. Developing such a defense system can be done to some extent separate from the existing one, allowing for smooth integration while maintaining a low level of complexity. Since the core functionality of the PKE system does not necessarily need to be altered to accommodate Immobility Detection, as opposed to for example distance bounding which requires an overhaul of the hardware as well as the protocol, the development and integration is relatively trivial. The hardware adjustment required is minimal - the currently employed processor and RFID transmitter may be kept - needing essentially only the addition of an accelerometer. Accelerometers for similar applications are already on the market, as described in Chapter 3, and are cost efficient. Furthermore, the addition of such a system was deemed to be insignificant or even positive - depending on exact implementation - on battery life, an important aspect in commercial applications.

The level of effectiveness of Bluetooth in the place of RFID based communication did not have a notable affect on this project. However, some interesting trends could be observed. The project used RSSI for measuring proximity to the vehicle, a critical feature for both security and user comfort. There were, however, major flaws detected with this. RSSI in general is not intended for absolute distance measurements. While for the purposes of this project the test environment could be limited for accurate calibration of the RSSI range, environmental factors in a commercial application would affect the readout significantly. This effect was observed to be so strong that the system designed - in its current form - could not function effectively in a varying environment. Objects in the path of the key fob, surrounding metallic objects, any covering material such as clothes, a bag, or even a person's hand all have a significant impact on the RSSI value. While Bluetooth, or rather BLE, as a technology for PKE systems may yet be ideal.

Evaluation of Immobility Detection This project has designed and developed a proof-of-concept implementation of a PKE system with Immobility Detection as a form of protection against relay attacks. It was observed that even a relatively simple Immobility Detection system is extremely effective against relay attacks on stationary key fobs and that low-cost accelerometers provide sensor data satisfactory for ensuring sleep-mode is entered when desirable. However, this system does not protect against all instances of relay attacks, as mobile keys are still vulnerable. With recent affordable and high range relay devices these thefts may become more common, posing a risk even for Immobility Detection enhanced PKE systems. Nevertheless, the clearly defined effective range of this system is an advantage in and of itself, allowing for manufacturers to clearly outline what the system achieves.

It was shown that the development of Immobility Detection is simple and can be easily integrated into existing PKE systems without requiring substantial changes to existing hardware or software. It was further found that such a system can be achieved in a cost-effective manner with existing low-cost components. If power usage optimization is desired then implementations exist where this system may increase battery life.

While some parameters, such as the timer for entering sleep mode and exact vibration thresholds, must be calibrated with regard for end use, the commercial development time of such a system is significantly shorter than many other proposed solutions and has little to no associated risks. Therefore, manufacturers could begin manufacturing newer car models with Immobility Detection in a short time-frame, while investigating other, more long-term, solutions.

Alternative Defenses Multiple proposed defenses have been described and analysed with many lacking considerations for implement ability, commercial viability, or cost, while others fall short in terms of security. It is deemed that two other methods promise potential. While distance bounding may be far from a commercial application, requiring further study not only on the protocol but also on hardware, integration into a printed circuit board, and reliability, recent advances in all of the above aspects are promising. Such a solution would be a large improvement on current access control. The second method proposed by this work - Approach Curve Matching - may also provide considerable increase in security for PKE systems. This defence system, however, requires substantial research before its feasibility can be determined.

Viability of Bluetooth LE for PKE While this work concluded that Bluetooth RSSI measurements - at least using the setup in this project - are not reliable enough for PKE applications, Bluetooth as a technology may yet be viable. The power usage of BLE is very low, having been developed for similar applications, which lends itself to access control. Albeit RSSI may not be ideal for PKE, there are novel ways of distance measurement being developed, some even specifically for the automotive industry. The added advantage of enabling access sharing using mobile phones greatly increases the attractiveness of this technology.

Additional Security Features There are a variety of added precautionary features that can contribute to an overall safer PKE system. Theft detection, such as that implemented in this project, whereby an attempted attack is not only foiled but alerted against, can increase the risk for attackers and thereby limit attempts. Moreover, access control restrictions upon failed unlock attempts can reduce the opportunity for an attacker to retry an attempted theft, use a different method, or even gather data on the protocol to be used to fine tune the attack. Since all lock systems contain parallel active keyless entry, in the case of an erroneous attempt by the intended user this additional system can still use to unlock the car. Merely the addition of an audible signal from the key fob, as is already present on the vehicle side, may provide some protection against theft. Meanwhile, generally stricter timing constraints for the authentication protocol protect against attacks with more rudimentary equipment or those over long range where potentially time intensive demodulation and modulation of the signal is often needed. Furthermore, for legal proof of theft - in an insurance claim for example - it may be advisable for the key and vehicle to store a log of recent unlocking procedures.

6. Conclusion

This paper investigated, implemented, and assessed an Immobility Detection enhanced PKE system for relay attack resistance as well as various other proposed defence mechanisms. It can be concluded that, albeit limited to the case of a stationary key, Immobility Detection is a highly effective method of protection. Additionally, the implementation of such a system, as opposed to other proposals, in existing PKE systems is found to be cost efficient, trivial in nature, and not highly time consuming. In combination with the introduction of other defensive measures, Immobility Detection can greatly increase the security of PKE systems. While this paper focuses specifically on PKE systems for vehicles, similar technology can used for other access control applications. The conclusions of this work can be used to motivate further research as well as direct action by vehicle manufacturers.

References

[1] R Rajendran, B Piali, P Chandrakala, S Majji, “Role of digital technologies to combat COVID-19 pandemic”, World Journal of Engineering, 2021.

[2] S Majji, TR Patnala, M Valleti, CS Pasumarthi, “A Study on the Comprehensive Analysis of Electro Migration for the Nano technology trends”, 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).

[3] S Kothapalli, M Samson, S Majji, TR Patnala, “Comparative Experimental Analysis of different Op-amps using 180nm CMOS Technology”, 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).

[4] Mohammed Ismail B, P Rajesh, Mansoor Alam "A Machine Learning Based Improved Logistic Regression Method for Prostate Cancer Diagnosis" International Journal of Emerging Trends in Engineering Research Volume 8. No. 9, September 2020pp.5693-5698

[5] Mohammed Ismail. B, M. Alam, M. Tahernezhadi, H. K. Vege and P. Rajesh, "A Machine Learning Classification Technique for Predicting Prostate Cancer," 2020 IEEE International Conference on Electro Information Technology (EIT) July 2020, pp. 228-232,

[6] Mohammed Ismail, Ghousia Anjum T Bhaskara Reddy "Variable Block Size Hybrid Fractal Technique for Image Compression" Proceedings IEEE 6th International Conference on Advanced Computing & Communication Systems March 2020 pp 510-515

[7] Rahul Shahne, Mohammed Ismail, CSR Prabhu "Survey on Deep Learning Techniques for Prognosis and Diagnosis of Cancer from Microarray Gene Expression Data" Journal of computational and theoretical Nanoscience16 (12), 5078-5088, Dec 2019

[8] Mohammad Ismail K Naga Lakshmi, Y. Kishore Reddy, M. Kireeti, T Swathi" Design and Implementation of Student Chat Bot using AIML and LSA" International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8 (6), 1742-1746, April 2019

[9] Mohammad Ismail, V Harsha Vardhan, V Aditya Mounika, K Surya Padmini "An Effective Heart Disease Prediction Method Using Artificial Neural Network "International Journal of Innovative Technology and Exploring Engineering' 8 (8),1529-1532, June 2019

[10] Mohammed Ismail B, Dr. T. Bhaskara Reddy, Dr. B. Eswara Reddy "Spiral Architecture Based Hybrid Fractal Image Compression" IEEE 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT)" December 2016

[11] Mohammed Ismail B, Dr. Mahaboob basha shaik, Dr. B. Eswara Reddy "Improved Fractal Image Compression Using Range Block Size" Proceedings of IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS)Nov 2015 Pages:284–289

[12] L. Huang, Q. Yang, Q. Gu, W. Zhang, H. Shan, J. Li, and Y. Zeng, Inside Radio: An Attack and Defense Guide. Springer Nature and Publishing House of Electronics Industry, Beijing, Mar 2018. doi: https://doi.org/10.1007/978981-10-8447-8

[13] S. Rizvi, J. Imler, L. Ritchey, and M. Tokar, "Securing PKES against Relay Attacks using Coordinate Tracing and Multi-Factor Authentication," in 2019 53rd Annual Conference on Information Sciences and Systems (CISS), Mar 2019. doi: https://doi.org/10.1109/CISS.2019.8692790. ISSN null pp. 1–6.

[14] A. Alrabady and S. M. Mahmud, "Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs," IEEE Transactions on Vehicular Technology, vol. 54, no. 1, pp. 41–50, Jan 2005. doi: https://doi.org/10.1109/TVT.2004.838829

[15] M. Gulsever, "A Study on Vulnerabilities in Connected Cars," B.Sc. Thesis, KTH, School of Electrical Engineering and Computer Science (EECS), Jun 2019.

[16] J. Wang, K. Lounis, and M. Zulkernine, "CSKES: A Context-Based Secure Keyless Entry System," in 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), vol. 1, Jul 2019. doi: https://doi.org/10.1109/COMPSAC.2019.00120. ISSN 0730-3157 pp. 817–822.

[17] A. Francillon, B. Danev, and S. Capkun, “Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.” IACR Cryptology ePrint Archive, vol. 2010, p. 332, Jan 2010. doi: https://doi.org/10.3929/ethz-a-006708714

[18] W. Choi, M. Seo, and D. Hoon Lee, “Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System,” Journal of Advanced Transportation, Jan 2018. doi: https://doi.org/10.1155/2018/1935974

[19] K. Leuven. (2018, Sep) Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars. [Online]. Available: https://www.esat.kuleuven.be/cosic/fast-furious-and-insecure-passivekeyless-entry-and-start-in-modern-supercars/ [Accessed: 2020-02-16].

[20] T. Gerber. (2019, Mar) SAPD: Car thieves using technology to hack key fobs, steal vehicles. [Online]. Available: https://www.ksat.com/news/2019/03/12/sapd-car-thieves-using-technology-to-hack-key-fobs-steal-vehicles/ [Accessed: 2020-03-16].

[21] The Japan Times. (2019, 01) Osaka police say thefts of vehicles using ’relay attack’ technique on rise in area. [Online]. Available: https://www.japantimes. co.jp/news/2019/01/05/national/crime-legal/osaka-prefecture-police-say-carthefts-using-relay-attack-technique-rise-area/#. XrWpskBuKP [Accessed: 2020-03-16].

[22] Y Z Y Li. (2017, 10) Car keyless entry system attack. [Online]. Available: https://conference.hitb.org/hitbsecconf2017ams/materials/ [Accessed: 202002-02].

[23] Lexus. What sized battery is used in Lexus remote keys? [Online]. Available: https:// lexus2.custhelp. com/app/answers/detail/a id/8347/ ∼/what-size-battery-is-used-in-lexus-remote-keys%3F [Accessed: 2020-02-21].

[24] J. Rodriguez. (2016, Oct) Long-range RFID emitter antennas for passive keyless entry systems. [Online]. Available: https://www.eenewsautomotive.com/news/long-range-rfid-emitterantennas-passive-keyless-entry-systems [Accessed: 2020-03-16].

[25] Sheng Zhou and J. K. Pollard, “Position measurement using Bluetooth,” IEEE Transactions on Consumer Electronics, vol. 52, no. 2, pp. 555–558, 2006. doi: https://doi.org/10.1109/TCE.2006.1649679

[26] Imec. (2018, Nov) Imec demonstrates first secure passive keyless entry solution for automotive using Bluetooth Low Energy. [Online]. Available: https://www.imec-int.com/en/articles/imec-demonstrates-first-securepassive-keyless-entry-solution-for-automotive-using-bluetooth-low-energy [Accessed: 2020-04-21].