Journal of Software Engineering and Applications, 2022, 15, 116-129
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Intrusion Detection System with Remote Signalling for Vehicles Using an Arduino Controller and Radio-Frequency Technology

Senghor Abraham Gihonia[1], Rostin Makengo Mabela[1], René Gilles Bokolo[1], Eddy Kimba[1], Matondo Katshitshi[1], Matshitshi Kalombo[2], Michel Tshodi[1], Nathanael Kasoro Mulenda[1]

[1]Department of Mathematics and Computer Sciences, University of Kinshasa, Kinshasa, Democratic Republic of the Congo
[2]Faculty of Electronic Engineering, University of South Africa, Pretoria, South Africa
Email: senghorgihonia80@gmail.com

How to cite this paper: Gihonia, S.A., Mabela, R.M., Bokolo, R.G., Kimba, E., Katshitshi, M., Kalombo, M., Tshodi, M. and Mulenda, N.K. (2022) Intrusion Detection System with Remote Signalling for Vehicles Using an Arduino Controller and Radio-Frequency Technology. *Journal of Software Engineering and Applications*, **15**, 116-129.
https://doi.org/10.4236/jsea.2022.154006

Received: February 7, 2022
Accepted: April 16, 2022
Published: April 19, 2022

Abstract

Malicious activities or policy violations have been a concern for the past years. For example, many people have been victims of robbery on vehicles. A conceptual diagram of an Intrusion Detection System (IDS) [1] [2] for vehicles with remote signaling using an Arduino controller and radio-frequency technology is proposed in this paper. To address malicious activities on vehicles, two aspects are considered here, namely: notifier and detector. Firstly, an object-oriented C module that puts on and off a controller (installed inside the vehicle) and an anti-theft electronic editing that powered using an alternator and supported by a back-up battery are implemented. Secondly, a magnetic intrusion sensor, controlled by a proximity detector using radio-frequency technology, has been installed on each vehicle door. To enable IDS, a user needs to activate the monitoring system when leaving their vehicle. This is done using a remote system. In case the user does not activate the monitoring system while leaving the vehicle, a 5-meter-proximity detector will automatically lock the system and set off the monitoring system whenever the user is outside the detection zone. The detection zone is a 5-meter radius area centered at the controller. Here, monitoring consists of geolocating any intruders within the detection zone. This means, if any of the vehicle doors is opened while the system is still locked, the controller will activate the vehicle alarm for a few seconds, thereafter send an SMS notification to the owner. The system automatically unlocks as soon as the proximity detector is within the detection zone. The contribution of this paper, as compared to other similar work, is to reinforce the electronic implementation of IDS.

Keywords

Intrusion Detection, Magnetic Intrusion Sensor, Arduino Controller, Radio-Frequency Technology, GSM Module

1. Introduction and Literature Review

Malicious activities have raised the bar over the past years. Many people have been victims of robbery on vehicles. An Intrusion Detection System (IDS) is a set of devices or applications or both that monitors a system or equipment for suspicious activity and alerts when such activity occurred. This is done by either detecting signs of harmful patterns or monitoring user behavior to detect malicious intent around the object of interest. Vehicles are the objects of interest considered in this work.

Many people are victims of loss of vehicles or loss of items kept in vehicles which happened after breaking car doors at parking. Vehicle safety (VF) is an essential challenge to be addressed. Though VF has greatly improved over the past years, there are still rooms to strengthen VF. VF includes Anti-Lock Braking Systems, Driver Monitoring Systems, Lane Departure Warning Systems, and Anti-theft Systems (ATS) [3]. ATS are considered in this work [4]. ATS are preferred over other types of VF for two reasons. Firstly, they are easy to implement and considered as active VF systems. Also, they provide fair results and are more robust to types of vehicles.

ATS protect goods such as vehicles and personal belongings such as phones and jewelry. ATS include devices such as locks, keys, and tags. They have been proposed in literature and industries. Their first implementation was motivated by vandalism. It happened that the defensive strategies put in place to overcome this scourge have proven to be ineffective [5]. The first ATS devices to be built were mechanical with diverse embedded locks systems. These devices have evolved over the years (e.g. steering wheel locks, tire locks, hood locks, gearshift locks, ignition column/steering wheel locks) and are still being used.

In recent years, the use of ATS has been increased, which has evolved into Electronic Car Intrusion Systems. They can be divided into three main categories: engine immobilizers, vehicle tracking systems, and vehicle alarms. The need to provide applicable security solutions to all objects offered in the marketplace is crucial [6]. This requires achieving efficient data collection across multiple systems and performing data analysis that is independent of the object being monitored. It offers an intrusion detection solution based on data discrepancies around monitored objects.

To handle this issue, techniques based on efficient tracking techniques and various machine learning have been proposed in the literature. Such approaches allow automated detection of system bugs independently from the type of object being monitored. The last step is to trigger a descriptive alert indicating that an

intrusion is detected. This is achieved by displaying an alert message with code "60" on the analysis system. Technically, such an alert message would normally be transmitted to a monitoring system. Although not implemented yet, the alert engine could correlate events associated with the intrusion in order to take actions such as preventing intrusions from occurring. For example, in the case of the Mirai botnet, once an alert is triggered, the scanning system could restart the infected device, *i.e.* removing the injected malware. It could also recognize the Mirai infection patterns and alert users to change device passwords.

Furthermore, in [7], the authors propose an ingenious and simplistic vehicle ATS characterized by efficient access and immobilization mechanisms. Immobilizers indicate that vehicles can't move when intruded. Regarding access mechanisms, there is a hidden button which grants permission to switch on the monitored vehicle once triggered. It is a microcontroller-based system programmed and properly placed using a state diagram-based study. In [8], the authors point out that in recent years, vehicle theft has become a major issue. Vehicles lost need to be located. Their project aimed to detect lost vehicles. Arduino is the main component used to interface DC motor and GPS for tracking of vehicles and provides locations of stolen devices using GSM services. Stolen vehicles are identified using ESP 8266 Wi-Fi module. There are diverse reasons that limit the protection of vehicles using alarm systems. For example, the sound of a siren can't be heard beyond some distance. Also, crowds can affect sound systems negatively. Authors propose a technique presenting a mechanism to minimize loss of vehicles by ensuring system safety which is done by sending an alert message as soon as a wrong move is noticed around the vehicle without the owner's knowledge. The system also provides location updates periodically to the registered user via the Internet of Things.

In [9], the authors reiterate the fact that in large cities, one of the most concerning issues is to ensure the safety of vehicles, as the number of stolen vehicles has been growing in recent years. To improve situations, they offer a vehicle ATS which is based on a smart mobile device, similar to smart mobile phones, capable of remotely commanding the vehicle, including geolocalisation of the vehicle in the case of loss. To avoid downtime, a unique identification number is assigned to both the artifact and mobile devices. The system also implements an automated battery recharging module. When a vehicle is stolen, the artifact makes phone calls with its unique number assigned to the vehicle. Also, the control unit sends electrical tripping orders to very sensitive areas of the vehicle, thereby immobilizing the vehicle and preventing it from starting. The owner can notify the position of the vehicle in coordination with the call center. The system was designed using ATMEGA microcontrollers. The output of this capstone project is only applicable if the vehicle is already stolen and does not offer any workaround, because the main goal is not to find a stolen vehicle but to prevent a vehicle from being stolen.

A decision-making process might need to be incorporated into ATS to improve the process. In [10], the authors point out that vehicular ad hoc networks

(VANETs) are so difficult to secure due to the limitations of wireless technologies and their well-known security holes. An ATS is built by creating a protocol based on intrusion malicious actions detection performed on the system by analyzing incoming and outgoing packets to identify malicious signatures. However, without a decision-making mechanism, such actions are proven to be ineffective. It is therefore required to design a decision-making system, coupled with an intrusion detector, which constitutes a protocol for security information in VANET. The authors based their solution on two IDS approaches. In the first approach, IDS are installed on vehicles. In the second approach, they are installed on road units (RSU). In both approaches, vehicles are grouped together according to their speed. The corroboration of an attack is based on a probabilistic model that calculates the ratio between vehicles or RSU that responded to the signature of the attack. Thus, when an attack occurs, the protocol allows corroboration and alerts neighboring clusters.

Unlike the aforementioned authors, the approach to be proposed in this paper aims to provide a new paradigm of IDS. It is based on radio-frequency technology for alerting mechanisms (*i.e.* a real-time notification system). This system is based on GSM technology, which allows the owner of the vehicle to be controlled from any location when the system is locked. However, coverage of vehicles does not go beyond the network coverage area. GSM technologies are also used in other work. For example, [11] proposes a system using a GSM module and a GPS technology to track vehicles. It considers the facial recognition of the owner using an OpenCV-based application. The image of the owner is stored in a database which the application retrieves whenever the owner tries to start their vehicle. The downsides of such a system include the rate of false positive and false negative, and the high cost of hardware.

[12] proposes a system for detecting and tracking stolen vehicles by designing a device using vehicle tracking hardware composed of GPS and GSM modules. This system facilitates coordination and has a live camera to capture the intruder's face. Each time the vehicle engine starts, an OTP (one-time password) will be sent to the owner's mobile phone for verification. If the OTP is not verified or an incorrect OTP is entered, the buzzer starts and an alert will be sent to the owner. Although has interesting features, this system is only able to alert when the vehicle is already stolen. Also, it takes significant time to alert the owner. Finally, the materials being used to implement such a system are costly.

Our proposed module uses two security modes:

- Alarm system;
- Message notification.

The advantage of our proposed IDS is summarized as follows:

1) In terms of equipment, the system is independent of the vehicle's energy source; the controller is installed in the vehicle supplied by its own battery (alternator). The controller has also a back-up battery.

2) Magnetic intrusion sensors (reed switch) are installed in each vehicle door and connected to the controller. Magnetic sensors are installed on each vehicle

door to trigger alarms once a door is wrongly opened, unlike what other designers offer.

3) The user will have in their possession a proximity detector using radio-frequency technology (in form of a tag) which can be attached to a key.

To enable IDS, a user needs to activate the monitoring system when leaving their vehicle. This is done using a radio-frequency-based remote. In case the user does not activate the monitoring system while leaving their vehicle, a 5-meter-proximity detector will automatically lock the system and launch the monitoring system whenever the user is outside the control space. The control space is a 5-meter radius area centered at the controller. This means, if any of the vehicle doors is opened while the system is still locked, the controller will activate the vehicle alarm for a few seconds, thereafter send an SMS notification to the owner. The system automatically unlocks as soon as the proximity detector is within the control space.

The methodology used in this work is introduced next.

2. Proposed Anti-Theft System

A real-time system is an approach used in this paper. A real-time system is a system where the response should be guaranteed within a specified timing constraint or the system execution time should meet some deadline. For example flight control systems, real-time monitors, etc. It contains five stages, namely: analysis, conception, knowledge base formalization (KB), implementation, and test.

2.1. Research Diagram

A module diagram of the proposed system is shown in Figure 1. It designates any type of vehicle, motorized or not, intended to transport passengers using different transport possibilities including road and air. It contains a programmable circuit capable of executing a program and having integrated interface circuits with the outside world and has a Global System for Mobile Communications

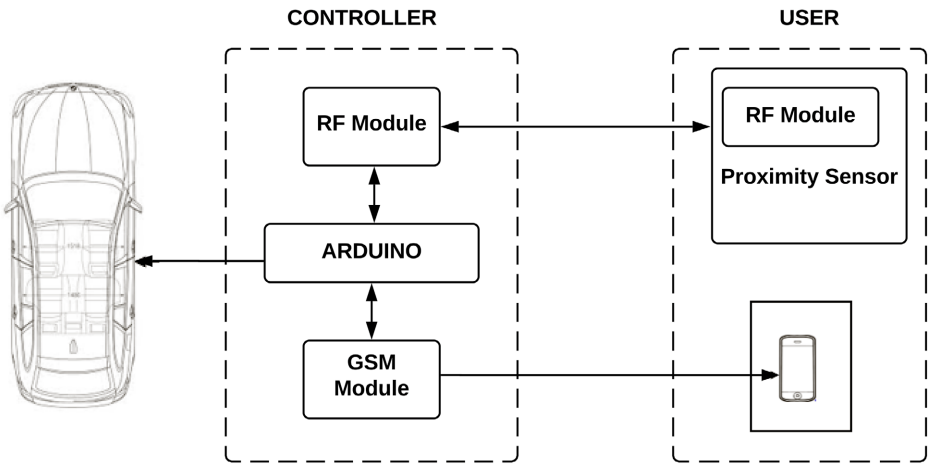


Figure 1. Module diagram.

(GSM) (Groupe Special Mobile) which is a second-generation (2G) digital standard for mobile telephony. It also contains a communication device originally designed to transmit human voices and be able to communicate remotely.

2.2. Radio Frequency (RF) Technology

Radio frequency (RF) technology is used in the proposed system. RF technology has existed for the past century. It is a type of dielectric-based heating causing molecular rotation in materials. It is an electromagnetic wave whose frequency is less than 300 GHz, *i.e.* a wavelength in the vacuum is greater than 1 meter (frequencies below 300 MHz) for so-called "radiofrequency" radio waves, and a wavelength in vacuum is greater than 1 millimeter (frequencies between 300 MHz and 300 GHz) for so-called "microwave" radio waves. RF technology uses radio waves, commonly known as radio waves.

Adapted to the transport of signals from voice and images, radio waves allow radiocommunications (walkie-talkie, cordless telephone, remote control, mobile telephony, etc.), broadcasting and radars. Their biological and environmental effects, at certain frequencies and intensities, have been studied intensively. For example, numerous studies on radio waves have been discussed in the context of the development of wireless communications (e.g. 5G).

2.3. GSM Module

The system also uses a GSM module which is required for communication between system and user. GSM/GPRS module in Seed Studio is an Arduino compatible interface board. SIM900A is a type of GSM module. SIM900A is selected for communication. It can operate in the 900 - 1800 MHz dual-band and is designed only to be used outside of Europe and the United States. It has a standardized performance, industrial grade interface standard plus a built-in TCP/IP protocol that makes it presentable and suitable for electronic projects [9]. Since it consumes little power in its operation, it is therefore said to be easy to communicate with any microcontroller with low power consumption. It can be interfaced using many interfaces some of which are I2C, SPI interface, PWM, antenna pad and two serial interfaces. It allows anyone to send and receive a SMS, to perform voice communication using the mobile network. The module is based on the SIM900 circuit and it is a product of SIMCOM. It is controlled through AT commands from an Arduino board.

The module is delivered with a remote patch antenna. A connector on the back of the board is provided to receive a SIM card as well as a Lithium CR1220 battery. Communication between the module and an Arduino board is asynchronous; using an asynchronous serial link: UART or a software serial link. The module requires a SIM card from an active network to operate and a plan to be able to send messages.

2.4. Arduino UNO Controller

Arduino UNO controller is the intelligent part of the system where various

components such as inspection, detection and alert algorithms reside. Since Arduino is the main board, the microcontroller which is ATmega328 is used as the main controller to manage the circuit accordingly. ATmega328 is a well-known open-source microcontroller-based kit for creating digital devices and interactive tools that can interact with LEDs, LCD displays, switches, buttons, motors, speakers" and many others. The Arduino system offers a set of analog and digital pins that can be built into many other boards and circuits that have absolutely different functions in one design. The Arduino board provides a USB serial communication interface to load codes from the computer. To develop coding, Arduino has prepared its own software called Integrated Development Environment (IDE) which fully supports C and C++ programming languages.

The receiver will be connected to an Arduino UNO controller which will monitor the status of the doors; check whether the system is armed or not, and decide to send the SMS. This is accomplished by sending the instructions to the GSM module. The Arduino controller will communicate with the GSM module and with the CC1101 transmitter through a serial communication interface.

2.5. Arduino NANO Controller

A transmitter will be controlled by an Arduino Nano. It is similar to the board used for the Arduino UNO but smaller. This is ideal when we would like the remote control not to be bulky.

2.6. Magnetic Sensor

A magnetic sensor is a device that can detect if one of the vehicle doors is open. For this project, magnetic switches will be used. Integrated Hall effect magnetic sensors are used in the automotive and computer industries for their deeper penetration properties into other applications but it is mainly hampered by the problems of switching noise and offset and drift associated with the packing stress [11]. A magnetic switch has two ends which form a magnetic field. If the ends are separated and the field disappears, the switch contact opens. As part of our application, one end will be placed on the door and the other on the vehicle frame. Thus, while the door is closed, the contact is closed and while the door is open, the contact is open.

2.7. Stabilized Power Supply

A stabilized power supply is given in **Figure 2**. The features are as follows:

- Receiver: Power supply (12 V/2A from the alternator), 9 V as the backup battery
- Transmitter: Power supply (5 V/500mA)

3. Experimentation and Discussion

We implemented our method using Arduino. Our simulation was run on actual vehicles. Our code can be found at https://github.com/Gsenghor/detection_intrusion. An example of architecture

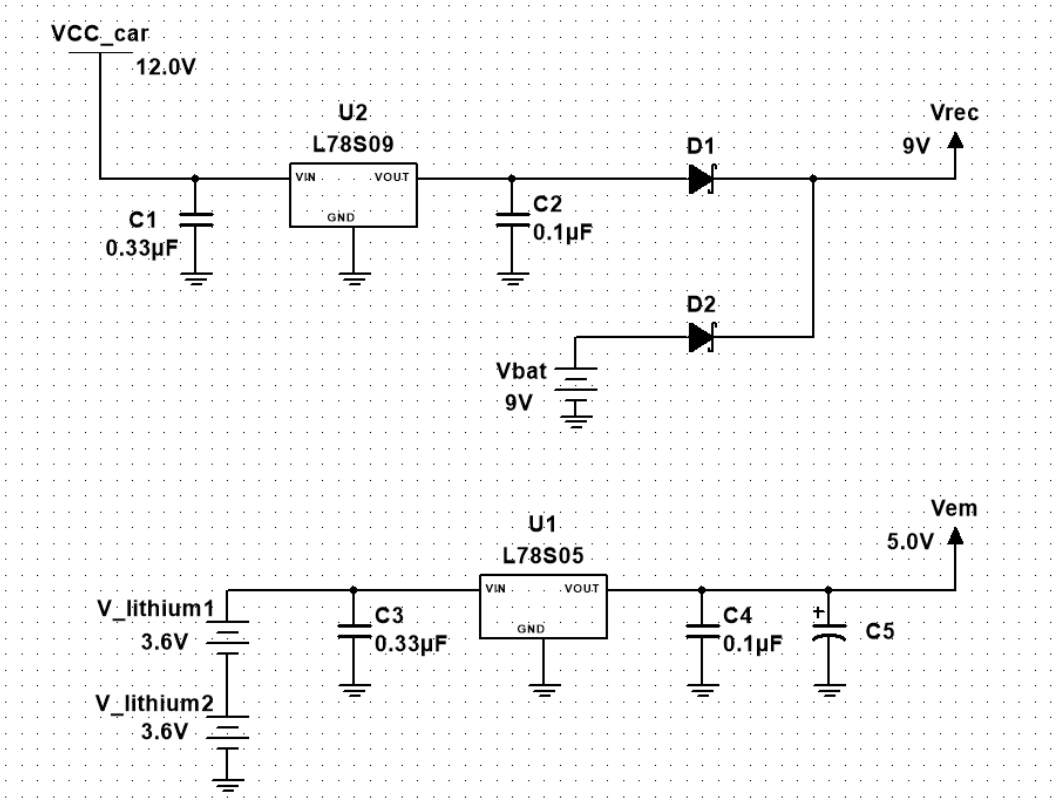


Figure 2. Stabilized powering.

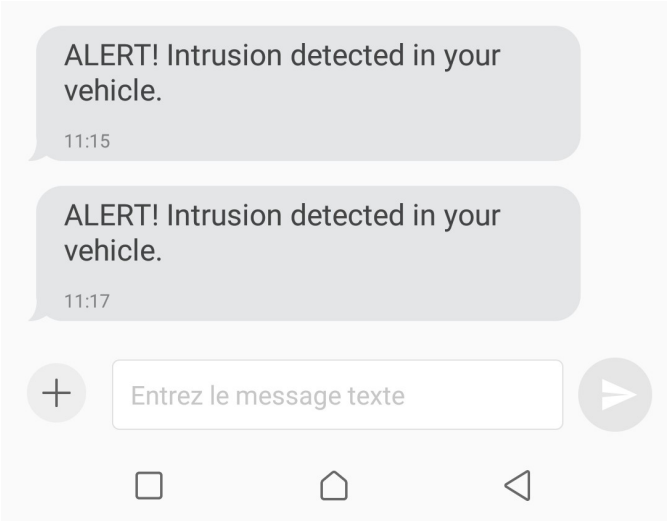


Figure 3. An SMS received as notifications in case of intrusions.

used to run our system is shown in **Figure 4**.

3.1. Algorithms Used and Electronic Editing

3.1.1. Issuer Algorithm

The Issuer algorithm is shown in **Figure 5(c)**. The issuer sends a signal to the RF and the RF can verify the nature of the signal, whether it is to lock or unlock the system. If the signal is to unlock, the controller checks if the module is locked. If

Figure 4. An example of architectures used to run our implementation. There are a passing car, a pedestrian and a car with in-built IDS to detect and report intruders. There is a BTS that connects our IDS to user's phone for notifications.

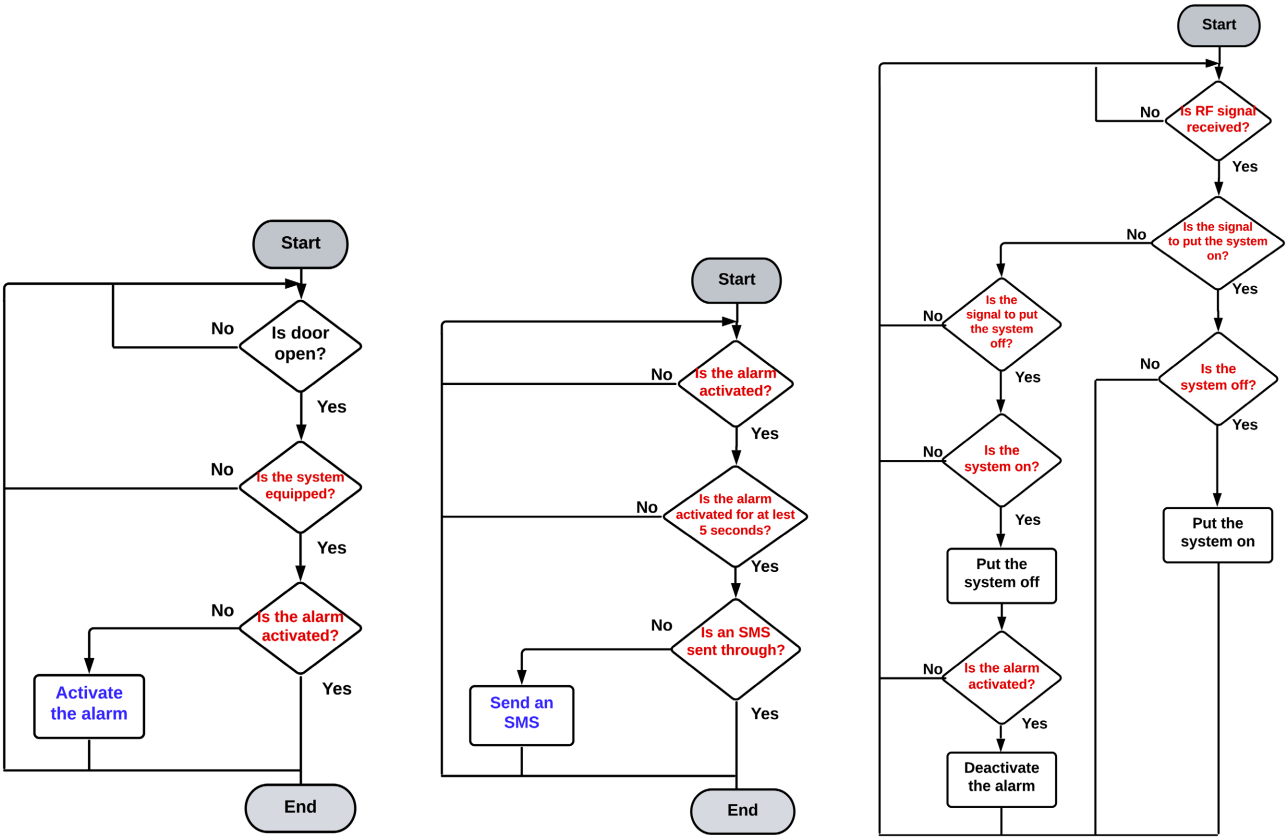


Figure 5. SMS alert algorithm. This illustrates the algorithm used to notify the own of a vehicle being intruded. (a) Alarm algorithm. (b) SMS alert algorithm. (c) Issuer algorithm.

so, the module unlocks and the alarm deactivates simultaneously.

3.1.2. Alarm Algorithm

When one of the doors is open, the system is locked. A final step is to check the alarm when it is activated. When the module is locked and a door is open, the retention alarm loops. The alarm approach used in this paper is shown in Figure 5(a).

The code source for the experimental investigation run in this paper can be found at https://github.com/Gsenghor/detection_intrusion. An example of an SMS notification sent to the vehicle's owner and an example of architectures used to run our experiments are shown in Figure 3 and Figure 4 respectively.

3.1.3. SMS Algorithm

This is how the SMS notifier works as shown in Figure 5(b). The GSM module waits for an impulse to send the message to the vehicle owner when a door opens and the alarm sounds. This is assumed to be a true positive, not a false alert. If it is a positive alert, the 2 GSM modules will then send an SMS after 5 seconds. The architecture of the intrusion detector is shown in Figure 7 (Figure 7(a) for module and Figure 7(b) for control).

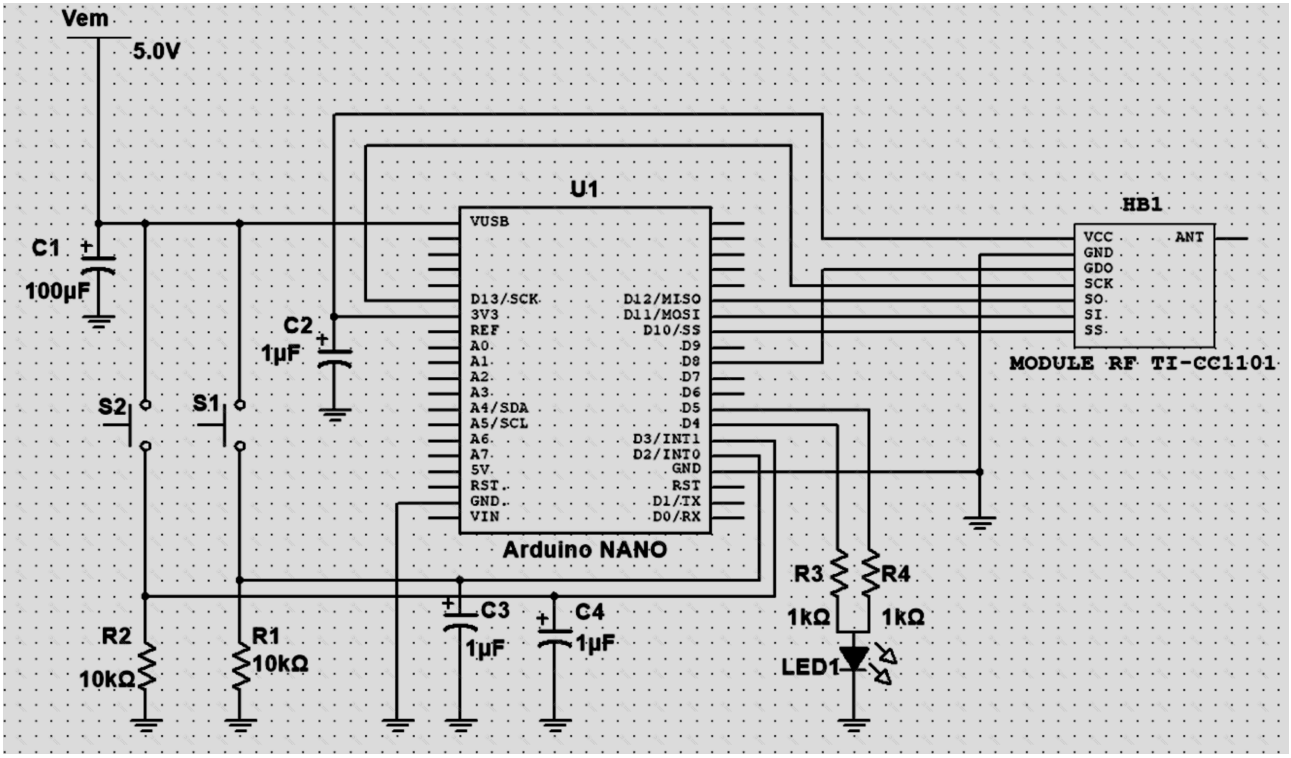
3.2. Electronic Diagram

3.2.1. Transmitter

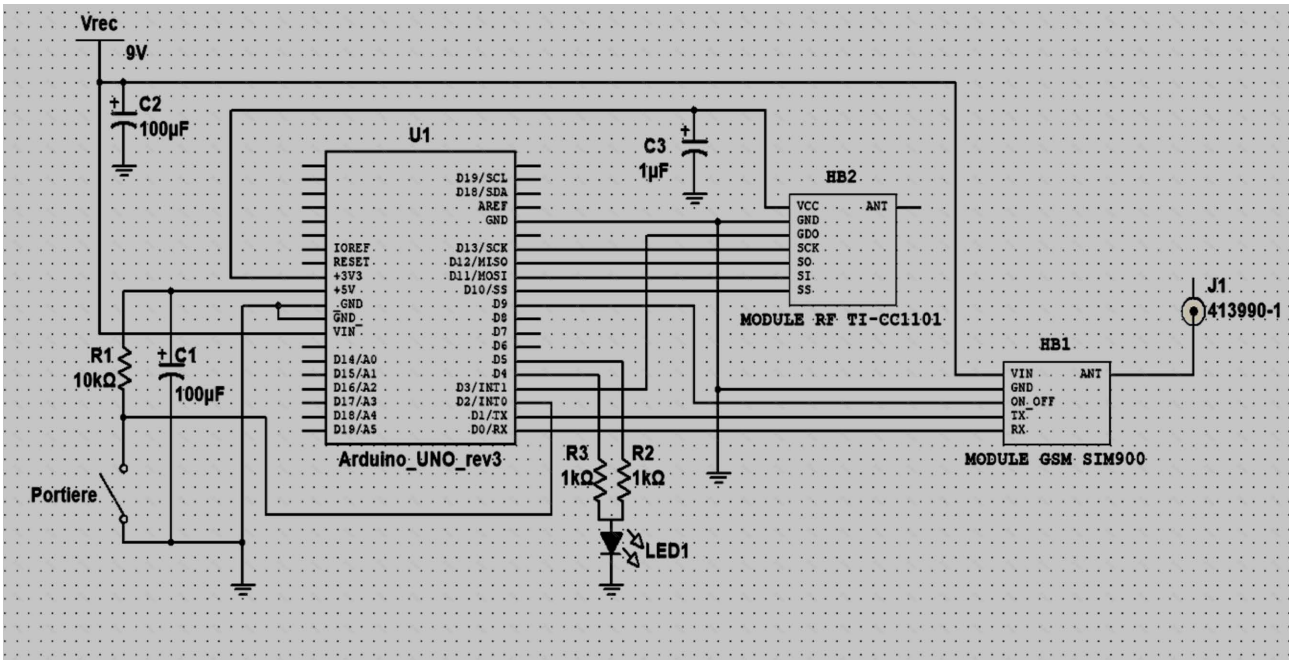
A radioelectric wave transmitter is electronic telecommunications equipment, which through a radioelectric antenna, radiates electromagnetic waves into space. The signal transmitted by these radio waves can be a broadcasting program (radio, television), a remote control, a conversation (radiotelephony), a computer data link, or a radar remote sensing pulse. The architecture of the transmitter is shown in Figure 6(a).

3.2.2. Receiver

Mounting a radio receiver (also called: radio set, transistor, tuner, car radio, etc.)

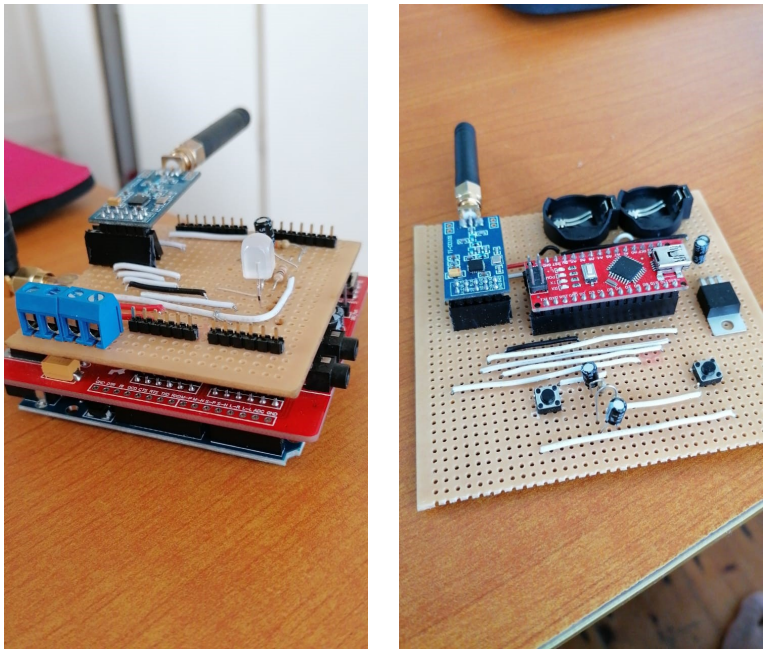


(a)



(b)

Figure 6. Receiver and transmitter diagrams. (a) Transmitter Diagram. (b) Receiver Diagram.



(a) (b)

Figure 7. Intrusion Detector. (a) Intrusion detector module. (b) RF remote control.

is an electronic device intended to capture, select and decode the radio waves emitted by radio transmitters. The architecture of the receiver is shown in Figure 6(b).

3.3. Discussion

Our experiment is similar to some prior similar work. Some aspects are consi-

dered to make things better in terms of functionality. For example, the authors in [6] use an approach which might be ambiguous. Although having used advanced methods for anomaly detection, the work has considered several aspects which can lead to a false alarm. In fact, alerts are transmitted only to checkpoints rather than informing the owner who might have caused the alarm.

To address this, a system capable of transmitting alert information to the owner is considered first. After alerting the owner, the alert center (or control) is then alerted with a delay of 2 minutes in case of inaction. The approach used in [7] requires an authorization to start a vehicle by pressing a button hidden under the vehicle, rather than a remote control. Such a mechanism seems to be very insecure since intruders can easily emulate the behavior. This is why a remote control system is offered in our proposition for the user to relate incidents that occurred. This solution is a little expensive and less intuitive to intruders. In addition, the module positioning guarantees a decrease in vulnerabilities of the system. It is securely hidden, highly hard to be seen by potential intruders and it has its own internal battery to ensure its autonomy.

In [8], the range of the vehicle's control system, the audibility of the siren which proves to be attenuated in overcrowded or noisy areas and especially the identification of the device which originated the siren are the main challenges of anti-theft systems. In this work, these challenges are handled from the fact that deterrent alarms can only be considered to have a fair protective value for gear only if additional alerts are added to them. In addition, a device stolen in a noisy environment is not intended to stay there, however, by leaving the noisy environment with a siren which will be heard continuously, the suspicions of theft will be raised continuously as well, which constitutes a deterrent for the attacker.

As for the range, the use of GSM, the coverage which is estimated at at least 90% in urban areas, is proving to be a major asset, downgrading the alibi for the scope of the control system, which, moreover, remains decisive. The technology used and the alert triggering times proposed in [9] seem to be very naive. In fact, using calls rather than texting for notifications seems annoying, although it may wake up attention more efficiently. Also, multiple notifications to different people are not taken into account with this technology. For the notification delay, the authors opted for a 15-minutes respite before notifying users, which is enough for an expert to locate and deactivate the micro-controller board. This is why the detection and notification algorithm is considered to be unsuitable. This requires the development of a better version to satisfy the clauses of this system.

4. Conclusions and Future Work

In this paper, we have designed and built an ATS offering high-performance detection and notification system in case of loss of vehicles. While existing ATS are mostly based on a pre-theft warning system in a short distance and with no notifications, our contribution consisted of adding a notification layer to ATS and reinforcing detection mechanisms and autonomy. Our proposed method is

based on the intrusion detection principle which has the ability to anticipate intrusions. Issues related to the distance between the vehicle and the owner implemented using SMS notification.

Our experiments ran our approach on various configurations. When an intrusion is detected, an SMS is sent to the owner of the car. Assuming it is not a false alarm, the owner will then notify the police service by sharing the location of their car while trying to render where the car was parked. If it was a false alarm, the owner has the ability to disable the notification system from ringing. Compared to previous work, the notification system of our IDS tends to be faster and materials used to construct our ATS are quite cheap.

There are a number of avenues of interesting work to further develop our understanding of ATS. First, it would be good to establish ATS on vehicles theoretically. Further, it may be possible to obtain an intelligent version of ATS using machine learning and computer vision to reduce false alarms. Finally, it would be interesting to reinforce notification systems and optimize battery energy consumption.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Smaha, S.E., *et al.* (1988) Haystack: An Intrusion Detection System. *Fourth Aerospace Computer Security Applications Conference*, Orlando, 12-16 September 1988, 37-44. https://doi.org/10.1109/ACSAC.1988.113412

[2] Liao, H.-J., Lin, C.-H.R., Lin, Y.-C. and Tung, K.-Y. (2013) Intrusion Detection System: A comprehensive Review. *Journal of Network and Computer Applications*, **36**, 16-24. https://doi.org/10.1016/j.jnca.2012.09.004

[3] Hu, J.-M., Li, J. and Li, G.-H. (2012) Automobile Anti-Theft System Based on GSM and GPS Module. 2012 *Fifth International Conference on Intelligent Networks and Intelligent Systems*, Tianjin, 1-3 November 2012, 199-201. https://doi.org/10.1109/ICINIS.2012.86

[4] Gustafsson, F. (2009) Automotive Safety Systems. *IEEE Signal Processing Magazine*, **26**, 32-47. https://doi.org/10.1109/MSP.2009.932618

[5] Abuzalata, M., Momani, M., Fayyad, S.M. and Abu-Ein, S. (2012) A Practical Design of Anti-Theft Car Protection System Based on Microcontroller. *American Journal of Applied Sciences*, **9**, 709-716. https://doi.org/10.3844/ajassp.2012.709.716

[6] Gassais, R. (2018) Intrusion Detection on Connected Objects by Behavioral Analysis. Polytechnic School Montréal, **91**, 46-50.

[7] Acakpovi, A., Kester, Q.-A. and Koumadi, K.M. (2013) Semi-Automatic Car Anti-Theft Design Using ATMega168 Microcontroller. *International Journal of Computer Applications*, **63**, 41-46. https://doi.org/10.5120/10586-5765

[8] Poushya, M., Rupasri, K., Supritha, N., Hema, K. and Tejaswini, R. (2018) IoT Based Vehicle Theft Detection. *IRE Journals*, **1**, 52-55.

[9] Rahnamei, A., Khoshnevis, F., Vajdi, M. and Farhadi, P. (2012) A Design for CAR Anti-Theft System using Cell Phone. *International Journal of Advanced Scientific*

Research and Technology, **1**, 1-5.

[10] Coussement, R., Bensaber, B.A. and Biskri, I. (2013) Decision Support Protocol for Intrusion Detection in VANETs. *Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, Barcelona, 3-8 November, 2013, 31-38. https://doi.org/10.1145/2512921.2512928

[11] Wolf, M. and Daly, P.W. (2009) Security Engineering for Vehicular IT Systems. Springer, Berlin. https://doi.org/10.1007/978-3-8348-9581-3

[12] Priya, J.G., Revathi, T., Subasri, G. and Shivani, A. (2021) Detection and Intimation of Vehicle Theft in Parking Slots. *Revista Geintec-Gestao Inovacao e Tecnologias*, **11**, 2057-2067. https://doi.org/10.47059/revistageintec.v11i2.1825