Simulation of presence as a strategy for protecting vacant residential environments

ISRAEL MARQUES, PAULO GARCIA
Electrical Engineering Department
Mackenzie Presbyterian University
01302-907 Rua da Consolação 940, São Paulo-SP
BRAZIL
israel.avansi@gmail.com

Abstract: - Projecting automation and control systems has been an increasingly important occupation for engineers since the beginning of the 20th Century. In our current era, the undeniable relevancy of automation in areas such as productivity, education and recreation acts as constant stimuli for draftsmen to keep conceiving new applications for computerized systems. Among these many uses, automation components acquire special significance when devoted to home security, since they should deal not simply with work rate boosts or enhancing entertainment options, but the protection of life and property. This article proposes an arrangement of electronic hardware to perform a simulation of the property's owner presence in empty environments as a strategy to reduce the possibilities of home theft, once it is known that delinquents should feel strongly dissuaded to proceed with trespassing the area if they conclude that the said property is being inhabited.

Key-Words: - Home Automation System Securitym, Simulation, Microcontroller, Arduino Raspberry Xbee

1 Introduction

1.1 Origins of automation

Oxford Dictionaries defines automation as "The use or introduction of automatic equipment in a manufacturing or other process or facility" [1]. Hence, the main advantage brought by the employment of automated systems lies in the fact that the machines which compose them possess the capability of verifying their own performance and correct processes' missteps without human intervention, in the large majority of cases. Given such scenario, pre-programmed and self-correcting machines can complete their tasks at a much faster rate when compared with manual or non-automated labor.

Earlier occurrences of automated devices include the invention of floating valves to regulate liquid flow in oil-lamps, wine dispensers and water tanks in primal Greek and Arabic communities, as well as the fabrication of the Ktesibios water-clock in ancient Alexandria [2]. Greek temples from the Hellenistic period employed self-animated mechanical devices denominated as "automata" shaped like humans and animals as part of their liturgical activities [2]. By the 17th Century, Cornelis Drebbel conceived a closed loop control system to operate a furnace, thus creating an archaic thermostat [2].

The first instance of an automatized process in an industrial environment retraces to the late 1920s when Toyota Industries founder, Sakichi Toyoda developed a weaving machine capable of identifying mechanical malfunctions and cease its operation until the problem was solved, thus giving birth to toyotism and inaugurating the era of the "third Industrial Revolution" [3]. Since then, the world witnessed an expansion in the use of automated systems that are no longer restrict to factories' production lines but span through multiple commercial, governmental, academic, agricultural, medical and domestic applications [4-9].

Home automation systems in particular have experienced growth in both quantity of utilizations and relevancy in past years. Out of the many functions that a home automation system can perform, the control of electrical appliances, multimedia features, communication systems, amenities and security circuits [10].

More recent automation projects can even learn how to arrange themselves in order to best cater to the needs of the environment they are inserted based on the changes of behavior and habits of their owners, without the obligation of recurrent manual reconfigurations [11].

1.2 Automation as a security tool

It is an unfavorable fact that densely-populated human societies will invariably be confronted with acts of delinquency perpetrated by criminals, in higher or lower degrees. However, the use of automated systems as allies of security can help attenuate the lethality and losses brought by criminal acts. Recent security innovations present in the domestic security automation industry include, among many others, smart locks that can be opened via smartphone, wireless video monitoring cameras that can be remotely accessed by the user, sensors kits that are able to notify the owner of invasions or domestic accidents, communication systems that notify constabulary authorities of invasions and criminal acts and even special sensors and devices that cater to specific pet necessities, all these allied with digital displays that give the proprietor complete control over home appliances and security devices in operation. [12,13].

It is noteworthy to mention that advanced home security systems are often expensive and complex. This paper presents an alternative strategy for implementing a system that uses simple home appliances devices whose operation is coordinated by a Programmable Logic Controller (PLC) that will activate appliances at arbitrary times in order to simulate the presence of the owner in an empty residential environment.

1.3 Simulation of presence

Professionals from insurance and home protection markets warn and agree that the probability of home invasion occurrences increases a significant lot in vacation periods when families travel and temporarily leave their residences unoccupied, stimulating intruders to carry criminal acts such as invasion and theft. In a Brazilian context, Diuri explains that the number of home theft incidents increases about 30% at the beginning of the year, mostly from December to January, when school vacation time arrives and families start their touristic voyages [14]. In the same context, Davini addresses the fact that lawbreakers are often looking for situations where they can minimize their risks to conduct illegal acts with minimum effort, thus vacant residences present an easy and temptating target [15].

With the knowledge that the invasion of an occupied property is generally declined by delinquents, it is patent that simulating the presence of individuals in an empty residential environment holds the potential to decrease the probabilities of the same occurs. Silva, Campos and Lima Filho argue there is a new trend among automation developers that involves mastering the control of electro-electronic appliances in pre-programmed dates during temporal lengths can be used as a tool to increase the security of a precinct, and such systems would have the function of simulating the presence of people in the said precinct to strengthen the security of an environment [16]. The following section will describe the authors' proposed presence simulation system as well as its implementation and the details on how the components interact with each other.

2 Proposed System

2.1 System components

The automated system was envisioned as a set of electro-electronic appliances wirelessly connected through Xbee modules to a Raspberry Pi 2 single-board computer. The said appliances include one incandescent light bulb, one audio speaker connected to an Arduino Uno R3 board to play .mp3 audio files and a motion sensor to alert the user of possible trespasses. A schematic diagram of the components is shown in Figure 1. A comprehensive list of all components employed in the construction of the system follows. After the list, a brief description of the main electronic hardware utilized in the project is provided:

- 1 Raspberry Pi 2 board;
- 4 Xbee modules;
- 1 Arduino Uno R3 board;
- 1 Arduino Mini board;
- 1 Adafruit Music Maker Arduino MP3 shield;
- 1 2GB microSD card;
- 4 Xbee modules;
- 1 Protoboard;
- 1 audio speaker;
- 1 audio amplifier;
- 1 relay switch;
- 1 incandescent light bulb;
- 1 motion sensor;
- 2 9V batteries;
- 1 Android smartphone;
- 2 medium-sized hard plastic cases;

2.1.1 Raspberry Pi 2 board

The central processing board of this security system, the Raspberry Pi 2 board is a compact-sized computer with a ARM Cortex-A7, that allows the configuration and manipulation of electronic devices through its 27 GPIO pins by use of Python programming language. Possessing a computational power comparable to that of a desktop machine, it

has its own operational system, the Raspian. Raspian is, by its turn, a variant of Debian (a language that shares traits similar to Unix) optimized for the board.

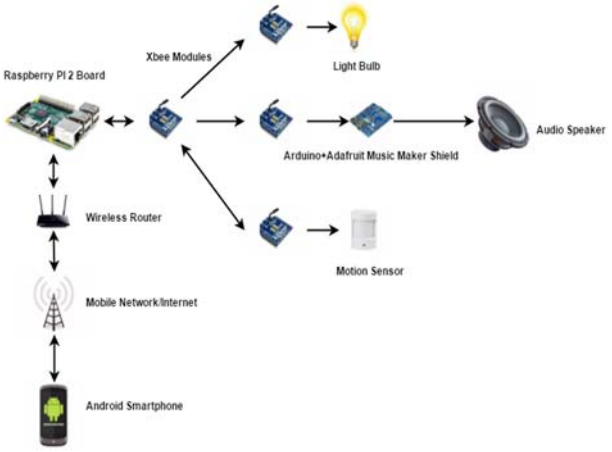

Fig. 1. Schematic diagram of the proposed system and its main components. Black arrows indicate the direction of the information traffic.

Raspberry is a popular platform for the development of many sorts of applications where low power consumption is a demand, such as cloud computing, automation and control, wireless equipment, and even devices used in space [17]. Therefore, it meets the requirements of high processing power necessary to the conclusion of this project.

2.1.2 Arduino UNO R3 board

The component used in this project to execute audio files is the Arduino UNO R3 board. Arduino is an development microcontroller board conceived by Massimo Banzi and his colleagues at the Interactive Design Institute in the Italian city of Ivrea, and its use is enthusiastically assimilated among professionals and amateurs programmers for its easy-to-use language and the fact that it is an open-source platform [18]. Because it doesn't possess as much processing speed as the Raspberry Pi 2 board, the Arduino UNO R3 is less expensive and has found its way into a wide range of applications thanks to an extensive global community of developers that contribute daily with new projects that explore Arduino's potentialities [18]

Thanks to its popularity, many complementary hardware components have been envisioned and manufactured to maximize the board's functionalities. Among them lies the Adafruit Music Maker, a shield needed for the progression of this project that owns a VS1053 codec, allowing for the implementation of functions to control the audio files (play/pause, next/previous buttons) while also being capable of reproducing different types of audio files extensions, such as .mp3, .aac, .ogg, .wma, .midi, .way, et cetera [19].

2.1.3 Xbee Wireless modules

Xbee modules were chosen to complete the task of achieving the *de facto* wireless communication between the boards. The modules carry this name because they make use of the ZigBee wireless communications protocol, which has gathered the attention of many researchers for its peculiar characteristics [20]. As opposed to WiFi, that operates under high data transmission rates and Bluetooth, that deals with the connectivity of mobile devices [21], the Zigbee network was designed having in mind applications where low power consumption is desirable and slower bit rates are allowed, such as home automation, security and medical monitoring and environmental sensoring [22].

Each Xbee device must be programmed to function as master or slave via the X-CTU software provided with the modules. On this particular project, the modules are structured following the mesh topology. Their operation consists basically in transmitting to each other the states (HIGH or LOW) of their digital inputs and outputs through RFID signals, so the hardware connected to them is able to decide what is the correct course of action [23]. Relevant functioning details of the Xbee modules include its communications protocol: IEEE 802.15.4, transmitting power: 0 dBm, receptor sensitivity: -92 dBm, indoor range: 30 m, outdoor range: 90 m, transmission current: 45 mA, reception current: 50 mA, voltage source: 2.4 – 3.4 V, and frequency of operation: 2.4 GHz. [24].

As bearers of the aforementioned features, Xbee modules are aligned with the exigencies of the proposed project as conceptualized by the authors of this article.

2.2 Implementation & Details

2.2.1 User Interface

The Android smartphone functions as the interface between the user and the Raspberry Pi 2 board. Through an app developed in MIT AppInventor website, all operations of the system can be controlled by pressing the buttons with the icons that represent the functions they will activate. When the buttons are pressed, the smartphone communicates with the Raspberry Pi 2 board, which in turn will then activate the components via Xbee wireless communication. The functions present in the app are: turning the light bulb on/off, activating

the music player (with play/stop/pause and forward/backward buttons), activating the motion sensor (it will notify the user when it detects an intruder) and starting "simulation mode", where the user inputs an initial and final time during which the presence simulation will take place (the light bulb will be on and the Arduino R3 board will start a playlist of songs that will be heard through the speaker). A capture of the interface's initial screen can be seen in Figure 2.

Fig. 2. Capture of the app's initial screen. From top to bottom, left to right: the title: "Security System", the light bulb activation button, the music player icon, the alarm activation button, which reads: "Alarm System Deactivated", an IP camera button for future system expansions, the icon for programming the initial and final moments of the simulation of presence and a last tile with information that reads: "Beginning", "End", "Time", "Activate Vibration".

2.2.3 Music Player

The music player of the proposed system was envisioned as an Arduino UNO R3 board that is connected to a speaker and plays .mp3 files through an Adafruit Music Maker Arduino shield. The music files are stored in a 2GB microSD card. The Arduino board is connected to a Xbee module that will receive signals coming from the Raspberry Pi 2 board. When the user presses the buttons of the music player icon as well as its functions (play, pause, forward, *et cetera*) on the app, the Raspberry Pi 2 board will send signals to the receiving Xbee module connected to the Arduino board which is programmed to execute the music player functions according to the signals received.

The signals arrive in the receiving Xbee module as 3-bit packets that will be interpreted by the Arduino board, each combination of bits corresponding to one different operation mode. These include: the previously mentioned "simulation mode", where the Arduino board will command the Adafruit Music Maker shield to execute all of the .mp3 files in a row, the "music player mode", where the Arduino board will be set to read the bit packets as codes for the buttons being pressed (play, stop, pause, forward and backward buttons) and the "Intimidation Mode", where the music player starts executing a fearsome audio file in order to demoralize the trespasser in case an invasion actually takes place. "Intimidation Mode" shall be further explained in the next subsection.

Due to the low values of current coming out from the TRS audio jack present in the Adafruit Music Maker Arduino shield, it is unwise to connect it directly to the speaker, once the signal amplitude would be too low to produce audible sounds. Therefore, an audio amplifier was included between the Adafruit shield and the speaker to boost the audio signals.

2.2.4 Motion Sensor

Likewise connected to the Raspberry Pi 2 board via Xbee module, one motion sensor was added to the system so it can detect the presence of incoming invaders. If the motion sensor icon is pressed by the operator on the app start screen, it will activate the sensor and its function: should the simulation fail to reach its purpose and the criminal individual decide to persist with the intrusion, the motion will send a signal to the Raspberry board once it detects movement. Raspberry will, in turn, send a message to the user's smartphone through an internet connection notifying him/her that an invasion is taking place. It will also force the system to go into "Intimidation mode", in which all activities of presence simulation or music reproduction are interrupted so a loud and frightful audio file can be executed. This is a last resort to alert neighbours that the property is being invaded as well as to make the lawbreaker realize that his presence has been noticed.

2.2.5 Further System Technicalities

The programming software utilized in the coding of the Raspberry Pi 2 board was Python IDLE 2.0, with Python as the programming language. The software used for compilating the Arduino codes was Arduino IDE, which uses a variant of C/C++ for its functions. The Android smartphone application was developed through an open-source code from MIT AppInventor website [25].

An Arduino Mini board was added between the motion sensor and its respective Xbee module to avoid complications regarding frame multiprocessing given that "Intimidation Mode" requires constant communication between the sensor and the Raspberry board.

A hard-plastic case and 9 V batteries were used to encapsulate the motion sensor and provide it with electricity. The Arduino UNO R3 board, which acted as the music player, was also encased and was powered by the common electric grid.

The Xbee modules follow a mesh network topology and have a sensitivity of -102 dBm, therefore the components attached to the Xbee can be spaced apart up to 90 meters (considering no obstacles) from the Raspberry Pi 2 board, which acts as the system's PLC. There is, naturally, a delay time between the pressing of the icons on the smartphone app and the execution of the said function, which amounts to approximately 1 or 2 seconds, depending on the selected icon.

3 Conclusion

The contribution that advances in automation, fueled by the pursuit of new ways to increase productivity, brought to all spheres of mankind's lifestyle is undeniable. This paper, focus on one of automation's many fields that experiences ongoing expansion: residential security.

Living with the hard reality of property breaching makes the development of this niche of automation a crucial issue for maintaining the well-being of law-abiding citizens, given the fact that it's not a mere matter of improving the efficiency of production chains or providing a more ostentatious way of living, but protecting their very lives and belongings.

As unfortunate as the reality of property breaching might be, there are many devices and systems that are capable to mitigate the number of criminal invasions. This is a niche that has acquired significant relevance and manufacturers' attention, particularly in developing countries that often face challenges like burglary and property vandalism [26]. Thus, creative ways of dealing with the aforementioned issues emerge as an answer to attend necessities of home protection and monitoring.

The system presented on this paper was designed, tested and assembled in Mackenzie Presbyterian University's facilities by the authors as a Course Conclusion Work and functioned exactly as described. The modular nature of the proposed system allows it to be expanded by adding more components (those include but are not limited to temperature sensors, gas sensors, glass break detectors, IP cameras, *et cetera*) to be controlled by the Raspberry Pi 2 board via Xbee connection in order to improve monitoring, if the consumer so desires. For future developments, functionality such as contacting the city's police department once criminal activity is detected is greatly recommended. Obviously, there are virtually infinite possibilities of complementary additions to the system, which will depend on the creativity and necessities of the designers. In fact, the system was designed so that the typical computer scientist could easily program the Raspberry Pi 2 and Arduino UNO R3 board according with what the context demands.

In sum, this paper has presented the construction an automated system that explores psychological warfare against criminal intruders and holds the potential to reduce home trespassing in empty environments by making use of presence simulation, deceiving lawbreakers in a non-confrontational, nonviolent fashion.

References:

[1] automation - definition of automation in English, *Ox. Dict.*, 2017. https://en.oxforddictionaries.com/definition/automation

[2] E. Hayden, M. Assante, T. Conway, An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity, *A S. Anal. White*, 2014, pp.8-9. https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf.

[3] G. B. da Luz, D. L. Kuiawinski, Mecanização, Autonomação e Automação – Uma Revisão Conceitual e Crítica, *Simp. de Eng. de Prod.*, 2006, pp. 1-2. http://www.simpep.feb.unesp.br/anais/anais_13/artigos/1210.pdf.

[4] C. S. Filho, A Automação nos anos 2000: Uma Análise das Novas Fronteiras da Automação, *Congr. e Expo. Int. de Auto.*, 2000, pp.1-7.

[5] A. Accorsi, Automação bancária e seus impactos: o caso brasileiro, *Rev. de Admin*. Vol. 27, 1992, pp.39-46.

[6] C. Magalhães, J. L. C. Dos Santos, J. I. Salém, Modelos e cenários para a Amazônia: o papel da ciência: Automação de coleções biológicas e informações sobre a biodiversidade da Amazônia, *Par. Estr.* Vol. 12, 2001, pp. 294-312.

[7] J. V. L. Botega, R. A. Braga Jr., M. A. Lopes, G. F. Rabelo, Diagnóstico da Automação na Produção Leiteira, *Ciên. e Agrotec.*, Vol. 32, 2008, pp. 635-639. http://www.scielo.br/pdf/cagro/v32n2/45.pdf,

[8] R. M. Braz, V. L. Andreozzi, P. L. Kale, Detecção precoce de epidemias de malária no Brasil: uma proposta de automação, *Epidemiol. Serv. Saúde*, 2006, Vol.15.

[9] C. L. A. Dias, N. D. Pizzolato, Domótica: Aplicabilidade e Sistemas de Automação Residencial, *Vért.* Vol.6, 2004, pp.10-32. http://essentiaeditora.iff.edu.br/index.php/vertices/article/viewFile/1809-2667.20040015/86

[10] J. R. Muratori, P. H. D. Bó, Automação residencial: histórico, definições e conceitos. *O Setor Elé.*, Vol. 62, pp.70-77, 2011. http://www.osetoreletrico.com.br/web/documentos/fasciculos/Ed62_fasc_automacao_capI.pdf

[11] J. A. Sgarbi, F. Tonindanel, Domótica Inteligente: Automação Residencial baseada em Comportamento. *Cent. Univ.o da Fei – Unifei*, 2006. http://fei.edu.br/~flaviot/pub_arquivos/WTDIA06.pdf

[12] C. McCormack, The 50 Best Smart Home Security Systems, 2016. https://www.safety.com/blog/50-best-smart-home-security-products/

[13] Honeywell: Security for Your Home and Family, Home Security, 2017. http://homesecurity.honeywell.com/home_security.html#pets

[14] L. Diuri, Férias sem preocupações, *Allianz*, 2016. https://www.allianz.com.br/-/azb-na-ferias-sem-preocupacoes

[15] L. R. Davini, A importância de sistemas de segurança residencial e ação policial, *Interview granted to the authors of this paper*, 2015.

[16] T. D. Da Silva, A. L. P. S. Campos, F. S. De Lima Filho, Sistemas de Simulação de Presença Residencial, *Hol.*, 2010, pp.130-140. http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/download/308/313

[17] F. Kaup, P. Gottschling, D. Hausheer, PowerPi: Measuring and modeling the power consumption of the Raspberry Pi. *39th Ann. Ieee Conf. On Local Comp. Net.*, 2014, pp.236-243.

[18] A. A. Galadima, Arduino as a learning tool. *11th Intl. Conf. On Electr., Comp. And Compttn*, 2014, pp.1-4.

[19] S. H. Kim, J. S. Kang, H. S. Park, D. Kim, Y. Kim, UPnP-ZigBee internetworking architecture mirroring a multi-hop ZigBee network topology. *IEEE Trans. On Cons. Electr.*, Vol. 55, No. 3, 2009, pp.1286-1294.

[20] M. A. Sarijari, M. S. Abdullah, A. Lo, R. A. Rashid, Experimental studies of the ZigBee frequency agility mechanism in home area networks. *39th Ann. Ieee Conf. On Local Comp. Net. Work.*, 2014, pp.711-717.

[21] M. F. M. Fuzi, A. F. Ibrahim, M. H. Ismail, N. S. A. Halim, HOME FADS: A dedicated fire alert detection system using ZigBee wireless network. *2014 Ieee 5th Contrl. And Sys. Grad. Res. Coll.*, 2014, pp.53-58.

[22] V. Georgitzikis, O. Akribopoulos, I. Chatzigiannakis, Controlling Physical Objects via the Internet using the Arduino Platform over 802.15.4 Networks. Ieee Lat. Am. Trans., Vol. 10, No. 3, 2012, pp.1686-1689.

[23] Digi International Incorporated, *Xbee Datasheet*, 2009. URL: https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee-Datasheet.pdf

[24] Vlsi Solution, *VS1053b - Ogg Vorbis/MP3/AAC/WMA/FLAC/ MIDI Audio Codec Circuit Datasheet*, 2012. URL: https://cdn-shop.adafruit.com/datasheets/vs1053.pdf

[25] MIT App Inventor, *Explore MIT App Inventor*, 2016. http://appinventor.mit.edu/explore/

[26] A. Farias, Os quinze bairros campeões de roubos e furtos a residências, *V. S. Paulo*, 2016. http://vejasp.abril.com.br/cidades/confira-os-15-bairros-com-mais-roubos-e-furtos-a-residencias/