Alarm detection with Raspberry Pi: An enhanced security model for DWU

Lyall Dale
Rodney Gunik

Abstract

The Alarm Detection Model is a proposed intelligent detection system to enhance security at Divine Word University. A customizable electronic device known as Raspberry Pi, used as a microcontroller attached with a sound sensor, and a wireless adapter used to establish a wireless network for the model's functionality. The model setup including the tools and techniques for deployment are discussed as an approach to improving the existing security infrastructure at the university.

Keywords

Alarm Detection Model, Wireless Sensor Network, Fast Fourier Transform, Divine Word University, Raspberry Pi, Python Programming language.

Introduction

Divine Word University (DWU) is experiencing annual growth with increasing staff and student numbers. A resulting challenge for the administration is the provision of effective and efficient security services for staff, students and property on campus. While the DWU Madang campus has its own security service operating under the name *DWU Rangers*, there are still areas of improvements to ensure community safety within campus perimeters.

The installation of security alarms in all campus accommodation unit alerts the Rangers to unwanted intrusions. These alarms are very basic devices that provide warning sirens and are typically mounted on interior walls of buildings. To signal an event, an alarm is activated manually providing a neighborhood alert and calling the Rangers' attention. In some cases, response may be delayed because the siren is unheard or there is difficulty in locating the source.

This paper seeks to discuss the functionality of a proposed alarm detection model that alerts the Rangers by notifications provided during the activation of an alarm to enable a swift response to an urgent situation. The paper will describe the composition of the detection system as well as the network tailored for the system to function and the possibility to scale the security system. It is now necessary to begin with the informal interviews conducted to establish the security issue.

The security issue

Some common security issues were identified from informal interviews with Rangers highlighting key areas of possible improvements. Some interview responses are now provided:

> “When the alarm rings, I hear the sound but most of the time I find it difficult to identify the location. At times, we arrive at the assumed location of the alarm but no sound so we had to ask residents in the area to identify the house” (Ranger 1, personal communication, April 10, 2018).
>
> “The ringing sound of the alarm chases off intruders and thieves before guards arrive, making it difficult to capture them” (Ranger 2, personal communication, April 12, 2018).
>
> “Unique sounds mounted at each house or dormitory can help us identify the location of the events” (Ranger 3, April 12, 2018).
>
> “Find some ways for the Rangers to keep track of each other, so that they maintain consistent surveillance on campus. Most times thefts happen when guarded spots are unoccupied” (Ranger 4, April 14, 2018).

Responding to these issues, this paper defines the detection system as an intelligent system assembled from customizable electronic device discussed further in the next section.

Overview of Raspberry Pi

Similar to personal computers, RPi has a high processing speed, graphical user interface and a backup mechanism for system files (Laurence, 2017). Mounted on the RPi’s system board is the processor, memory, storage, power supply, video output, General Purpose Input/output (GPIOs), a number of Universal Serial Bus (USB) port, reset button, audio-video port, power LED, activity LED, USB to Ethernet port, camera slot and the display slot (Figure 1).

Figure 1 A RPi 2 Model B board (The PiHut, 2019).

The RPi was developed in the UK to promote computer science and programming education in schools. Although developed for educational use, the current version exceeds its initial purpose by providing applications for a range of age groups to learn programming in languages such as Python and Scratch (Laurence, 2017). These languages are used for writing programs for the device to perform various tasks in response to sensor signals, thus enabling the RPi to interact with real-world objects (Charleston, 2017). The sensor signals are generated by sensor device as discussed in the next section.

Sensors

Sensors enable a device, a component or a system to be smart and perform intelligent tasks. According to Yurish (2010), the term smart and intelligent can mean the same thing in some languages but not in English. The first term is related to technological aspects of a sensor while the latter is the functional aspect. When the word *smart* is used with sensors, it defines a combination of a sensor, an analog interface circuit and an analog to digital converter connected in one assembly. The term *intelligent sensor* is used when a sensor has one or several other intelligent functions.

An intelligent sensor detects changes in ambient phenomena such as variations in temperature, humidity, wind, light, sounds or infrared radiation (IR). Such changes trigger the sensor to generate and transmit data to other electronic components or a computer to process (Spinsante, et. al., 2017). Although there can be sensors for each phenomenon, an intelligent sensor has the capability of detecting events in three distinct but intrinsic categories simultaneously.

A sensor can detect direct or proximal phenomena that directly trigger the sensor such as light striking a photocell sensor, sound detected by an acoustic sensor, or infra-red (IR) detected by the IR sensor. A sensor can also be triggered remotely by indirect or distal phenomena as a result of local events. An activated fire alarm might be a distal phenomenon that sends a loud sound to the sensor, or a household pet might alter heat radiation level in a room triggering an IR sensor. A sensor can also be activated by context or subtext phenomena which are events beyond proximal or distal phenomena. For example, an alarm might be activated from an electrical fault, when a switch is accidentally tripped, or when the motion of moving object (e.g. thief or insect) is detected. Such events entail some degree of uncertainty and require more information to avoid unnecessary intervention (Faludi, 2010).

The intelligent security system discussed here is based on distal phenomena such that a system consisting of a sound sensor and a RPi is deployed to observe and detect local alarm events and generate notification to a main station. Thus, the features that enable the identification of specific sounds are now discussed.

The features of sound

The sound sensor is able to detect all sounds within its locality. However, the sensor is interfaced to the RPi with a software program that has an intelligent capability of detecting sounds originating from an alarm by analyzing the sound’s intensity and frequency.

The concept of sound intensity is revealed by considering the alarms on buildings that alert using high intensity sounds to inform occupants or neighbors about events such as fire or robbery to hasten building evacuation or call for assistance. Sound intensity (measured in decibels, dB) decreases proportionally to the doubling of the distance from its source. The further away from the source, the lower the intensity reading as determined by the Inverse Square Law which states that sound intensity decreases up to 6 dB when the source distance is doubled (Thompson, 2005).

However, sound intensity traveling through air may encounter obstructions from nearby buildings or surrounding vegetation and so expected decibel values and corresponding distances (Table 1) assume line of sight propagation.

Table 1 The Inverse Square Law illustrating sound intensity relative to distance from sound source.

Weighted Decibel (dBA)	Distance (m)	Distance (km)
126	3.048	0.003048
120	6.096	0.006096
114	12.192	0.012192
108	24.384	0.024384
102	48.768	0.048768
96	97.536	0.097536
90	195.072	0.195072
84	390.144	0.390144

Whilst sound intensity by itself may be insufficient to uniquely identify a sound, the frequency has a uniqueness such that their combined use can enable the identification of the source of specific sounds. This has motivated a site inspection to identify alarm model numbers on campus and later the specifications are used to determine the decibel and frequency ratings (Table 2). The sound frequencies of these alarms were determined by analyzing the audio file for each alarm model with a spectrum analyzer.

Table 2 Common alarm model in DWU and their sound measurement ratings.

Model	Decibel (dB)	Approximate Frequency (Hz)
MS-190	114	1857 - 2838
MS-390	130	740
MS-490	112	1457

The alarm detection model

The alarm detection model (ADM) based on the RPi 2 Model B board has accessories such as a 4 GB micro Secure Digital (SD) card used to store the operating system and other files, a 5 volts micro USB power adapter, and a Wi-Fi adapter. Additional accessories required are keyboard, a mouse, a casing, a monitor and HDMI cable for viewing and typing commands during configurations.

Although RPi has a list of accessories, further equipment is required to assemble the ADM such as a high sensitivity sound sensor for sound detection, and female-to-female jumper cables for connecting the components together on a breadboard.

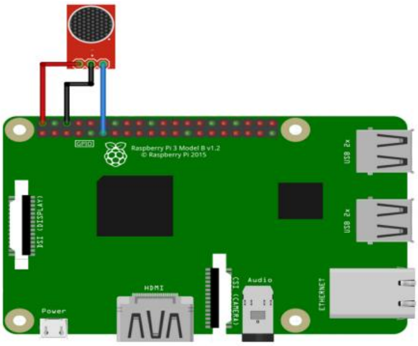

Figure 2 Schematic Diagram for the Detection Model (Courtesy of Piddler in the Root7).

A breadboard is used for temporarily installing electronic components during circuit testing. The intelligent functionality for the ADM (Figure 2) is achieved by software programs written with the purpose to detect specific sound as discussed in the following section.

The method of sound detection

Python is an interpretive high-level language used for general-purpose programming and the only scripting language pre-installed on RPi. The program that administers the functionalities of the ADM is achieved with Python's Scipy package used for scientific computation. The fast Fourier Transform (FFT) module within the Scipy package is an *inbuilt function* in Python that receives signals in the time domain then transform into the frequency domain. The reverse process is called the Inverse Fast Fourier Transform (iFFT) and both are represented by the series of sinusoidal functions.

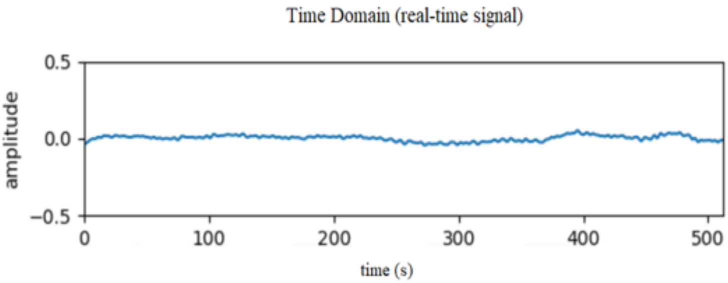

Figure 3 The graph of the audio signal in the time domain. Adapted from: https://www.swharden.com/wp/2016-07-31-real-time-audio-monitor-with-pyqt/, S. Harden, 2018. Adapted with permission.

The FFT module accepts continuous real-time sound captured at the sound sensor as amplitude variation with time (Figure 3). The signal is decomposed and presented as variation of signal intensity with frequency in the frequency domain (Figure 4). The signal is filtered based on conditions relating to the sound intensity, sound frequency and the duration of an alarm sound after the transformation. Invalid signals are considered as false alarms and are discarded.

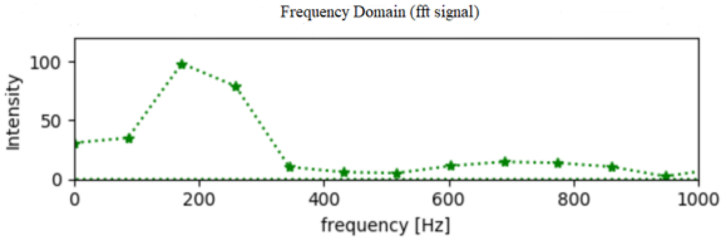

Figure 4 The graph of the same signal in the frequency domain adapted from: https://www.swharden.com/wp/2016-07-31-real-time-audio-monitor-with-pyqt/, S. Harden, 2018. Adapted with permission.

The signals are filtered and processed on real-time feeds with a discrete sample space and a sample rating is determined by the frequency ranges of the alarm model such that unwanted frequencies are disregarded. The program considers frequency range (0.7 – 3 kHz), sound intensity level (84 dB or higher) and sound duration (>120 seconds) to be validated as true to generate notification to alert the Rangers.

The main station provides the analysis and processing of the sensor data. As the validated data are received from the ADM, source locations are identified from the ADM's network address. Therefore, the real-time sensor data from each zone of deployment requires a network for transmission to the main station via wireless networks as will be discussed in the next section.

The wireless sensor network

A wireless sensor network (WSN) is a collection of standalone microcontrollers or radio adapters with typically one or more sensors (e.g. temperature, light level) that are interconnected through wireless transmission. Microcontrollers may have limited processing capability for some sensor projects, therefore, the wireless connection allows communication with a main station to achieve load balancing and resource conservation. The standalone microcontrollers are also known as nodes of the network and connections are established by a wireless adapter at each node. The sensor node is composed of a microcontroller such as RPi, a communication medium, and the sensor (Figure 5) and is considered the first layer of the network. The data received at the sensor node is transmitted to the second layer node which processes and presents the data and is called the data node, consisting of a microcontroller and a communication medium. The aggregator node is the third layer node and it is responsible for recording data for short term or forwarding to a database server to store for later use. In addition, the aggregator node acts as a gateway that connects multiple data node so that data can be stored and accessed in one location.

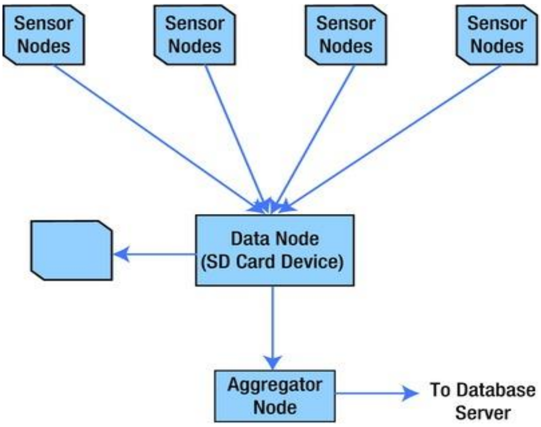

Figure 5 The hierarchical design of a wireless sensor network. Reprinted from Beginning *Sensor Network with Arduino and Raspberry Pi* (p. 9) C. Bell, 2013, New York, NY: Apress. Reprinted with permission.

The sensor nodes rely on power to function but most often this is not available when nodes are deployed in remote locations. The nodes are, therefore, mostly dependent on battery power to function and to achieve the necessary monitoring whilst using the least amount of energy (Guy 2006). To conserve energy, sensors are deployed with configurations for low-performance processing and minimal memory requirements (Maheswari, 2018). The deployment techniques such as cluster nodes or low energy consumption wireless protocols can be adopted.

The DWU Madang campus spans about 35 hectares and a WSN is established to function throughout the campus with wireless connectivity achieved by Wi-Fi or Xbee adapters. The Wi-Fi adapter situates the sensor node to rely on a networking device such as a wireless access point or a router for data transmission. The Xbee adapter, on the contrary, establishes connections without the need for a networking device.

The choice of a Wi-Fi or an Xbee adapter in the WSN depends on factors such as radio channels, coexistence mechanism, network size, security of the transmitted data and the transmission time (Lee, et. al., 2007). According to Lee, Su and Shen, the radio channels of Wi-Fi and Xbee use a direct sequence spread spectrum (DSSS) technique in the unlicensed 2.4 gigahertz (GHz) industrial, scientific and medical (ISM) band. They further state that Xbee uses 16 channels and a bandwidth of 2 megahertz (MHz) for data transmission while Wi-Fi uses 14 channels and a bandwidth of 22 MHz. The coexistence of Wi-Fi and Xbee uses dynamic frequency selection which is likely to encounter interference with the use of both adapters within a particular setting. The maximum number of device that determines the network size is 65000 for Xbee adapter and 2007 for Wi-Fi in a structured network. Both Wi-Fi and Xbee have the encryption and authentication mechanism for secure transmission of data between the nodes where Xbee adapter adopts the AES block cipher with counter mode and the cipher block chaining message authentication code while Wi-Fi uses the RC4 stream cipher for encryption and the cyclic redundancy check (CRC) for checksum integrity. The transmission time for Wi-Fi and Xbee on the contrary depends on data rates, the message size and the distance between the nodes (Lee, et. al., 2007).

The WSN is mainly an *ad hoc* network that requires no infrastructure to deploy projects such as the ADM and it is portable to setup anywhere. However, sensor projects are deployed on existing infrastructure which is further discussed in the following section.

The wireless infrastructure network

The ADM can also be deployed on DWU’s existing network infrastructure that provides a channel to allow the transmission of sensor data between the nodes. The sensor nodes are deployed in proximity of an access point within each deployment zone (Figure 7) and protocols make the sensor data transmission possible.

Protocols define the rules to communicate and transmit sensor data over a network. RPi has built-in communication protocols such as the Universal Asynchronous Receiver Transmitter (UART), Inter-Integrated Circuit (I^2C) and Serial Peripheral Interface (SPI). The UART defines the rules for entering commands on a terminal program whereas the I^2C protocol determines transmission of data from the sensors to the microcontroller. The SPI defines the rules for data transmission between nodes on a sensor network (Abdallah, 2015). These protocols enable RPi to communicate in an *ad hoc* WSN using wireless adapters, however, consideration of a different approach is necessary to transmit sensor data over an infrastructure network with TCP/IP as the transport protocols.

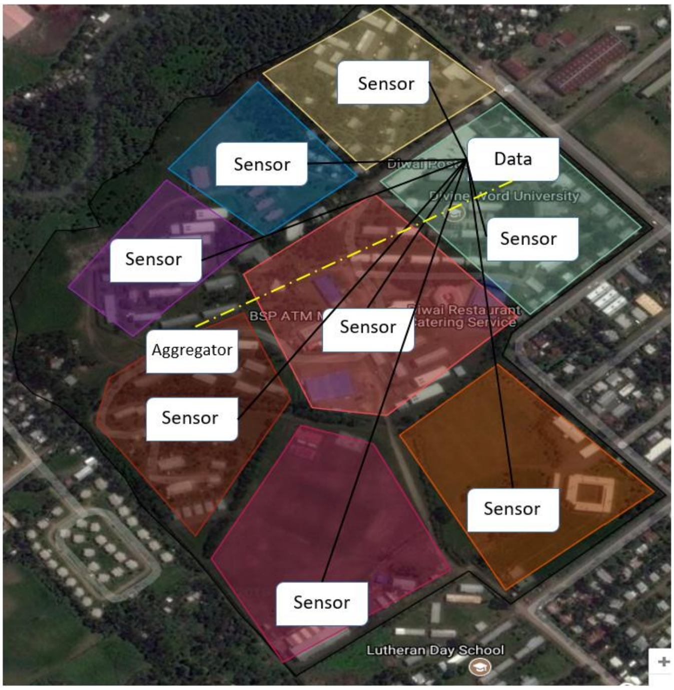

Figure 7 A logical representation of wireless connection across the campus for each sensor node.

A socket enables the communication between microcontroller nodes on an infrastructure network. A network socket is an internal endpoint within or between two nodes on a network for data communication. A socket application is a software program that specifies the Internet Protocol (IP) address, port number and the status of a node as a client or a server. In relation to the ADM, the sensor nodes are client sockets while the data nodes are the data processing server sockets and the aggregator node is a server sockets for data storage. Thus, utilizing socket communication in an infrastructure network enables the ADM nodes to be able to communicate and transmit sensor data over the network.

While sound sensors detect alarms, the possibilities of interfacing more sensors to the RPi at the sensor node is available if there are more GPIO pins. The RPi version discussed here has 40 GPIO pins which indicated the possibility of more sensors that furthers the discussion for the security model.

Further Enhancements

The ADM addresses the common issues by decreasing the guard response time, however, the sensor node expansion is possible by interfacing additional sensors for video, image, motion detection and infrared detection.

Security surveillance is a significant issue and the need for video monitoring has driven technology further. Video surveillance has improved technologies for CCTV cameras, IP cameras monitoring with LCD and integrated video surveillance systems. These new surveillance technologies can be mounted and accessed via a wireless connection using smartphones, tablets, or PCs anywhere in the world. However, RPi achieves the same capability for video surveillance with a camera module mountable on the microcontroller. The camera is further customized with software programs for capturing live video stream and storing for later use. The RPi camera module has a sleep mechanism to conserve energy such that a motion detector wakes the camera when motion is detected. In the state of awakening, the camera resumes live video streaming for some time before it transitions to sleep.

Images are also used for security measures by permitting RPi cameras to capture images from scenes. The captured images are for facial recognition when an image is required to identify persons at an incident scene. Images are also obtained from paused video during live streaming. Thus, video surveillance and image processing both rely on the RPi camera.

A motion detector observes alteration in the level of infrared radiation in an environment. The passive infrared (PIR) sensors are activated by heat signatures on objects that emit infrared radiation in the sensor’s proximity (Rothad, 2017). The PIR sensor detects motion of objects, humans or animals with its wide view and longer coverage range. The useful applications are seen in automatic activation of lighting or alarm system (Rathod, 2017). The PIR sensor is further used in restricted areas to alert unauthorized access at a given time. Hence, the alert provide notification of the intrusion so that guards move in to secure the area.

More improved sensors are being developed and are inexpensive to upgrade RPi to a more intelligent security system model.

Conclusion

This paper has sought the discussion on using the RPi minicomputer as a microcontroller to build an alarm detection model as an intelligent security system for DWU. The discussion began using personal interviews conducted with DWU Rangers where some issues raised have suggested the need for such security system as the ADM. The overview of RPi, the sensors and the features of sound which comprised the ADM were discussed. The techniques and tools for observation and identification of alarm were the sound intensity, sound frequency, sound duration, the sound sensor and FFT module from Python. The deployment of the ADM on both the wireless sensor network and a wireless infrastructure network provide a means for discussing the functionalities of the ADM on a network. The paper finally discussed improvements to the security model for achieving higher levels of intelligence for the security system.

References

Abdallah, M. (2015). Raspberry Pi - Lecture 3 Embedded Communication Protocols. Slideshare. Retrieved 6th December 2018, from:

https://www.slideshare.net/mohabdallah/raspberry-pi-lecture-3-embedded-communication-protocols.

Bell, C. (2013). *Beginning Sensor Network with Arduino and Raspberry Pi*. New York, NY: Apress.

Charlestom, T. (2017). *Raspberry Pi 3: Enchanted Guide for Starters*. Kindle Direct Publishing.

Faludi, R. (2010). *Building Wireless Sensor Networks*. Sebastopol, CA: O'Reilly Media Inc.

Guy, C. (2006). *Wireless sensor networks*. Sixth International Symposium on Instrumentation and Control Technology, SPIE.

Harden, W.S. (2016). *Python Real-Time Audio Frequency Monitor*. Retrieved 29th November 2018, from:

https://www.swharden.com/wp/2016-07-31-real-time-audio-monitor-with-pyqt/.

Laurence, P. (2017). Raspberry Pi 3: *The Ultimate Guide on How To Design and Build Your Own Projects with Raspberry Pi 3*. Kindle Direct Publishing.

Lee, J., Su, Y. & Shen, C. (2007). A Comparative Study of Wireless Protocols: Bluetooth, UWB, Zigbee, and Wi-Fi. Annual Conference of IEEE Industrial Electronics Society, Taiwan.

Maheswari, A. U. (2018). *A Survey on Recent Techniques for Energy Efficient Routing in WSN*. International Journal of Sensors and Sensor Networks. Vol. 6, No. 1, 2018, pp. 8-15. doi:10.11648/j.ijssn.20180601.12.

Piddler in the Root. (2017). *Sound Sensor*. Retrieved 1st December 2018, from:

http://www.piddlerintheroot.com/sound-sensor/.

Rothad, H. (2017). *PIR Motion Sensor with Raspberry Pi*. Retrieved 3rd December 2018, from:

https://www.hackster.io/hardikrathod/pir-motion-sensor-with-raspberry-pi-415c04.

Spinsante. S., Ricciuti, M., Cippitelli, E. & Gambi, E. (2017). *Fall Detection with Kinect in Top View: Preliminary Features Analysis and Characterization*. Springer Nature, Switzerland AG.

Thompson, D.M. (2005). *Understanding Audio: Getting the Most Out of your Project or Professional Recording Studio*. Boston, MA: Berklee Press.

Acknowledgements

I would like to acknowledge Prof. Peter K. Anderson, Head of Department for the Information Systems Department and the Mathematics and Computing Science Department for his endless leadership, encouragement, reviewing and editing of this paper. I also acknowledge Mr. Picky Airi, senior tutor from the same department for his ideas initially contributed to the paper. However, responsibility for any errors of fact or opinion, or infelicities of expression must remain with the main author.

Authors

Rodney Gunik (main author) is a senior tutor in the Department of Mathematics and Computing Science at Divine Word University. He holds a Bachelor Degree in Mathematics and Computing Science, a Cisco Certified Academy Instructor and a Post Graduate Certificate in Higher Education Teaching & Learning. He specializes in Applied Mathematics, Computer Science and CCNA and he has research interests including software development, mathematics and computer science.

Lyall Dale is a senior tutor in the Department of Mathematics and Computing Science at Divine Word University. He holds a Bachelor Degree in Mathematics and Computing Science and a Cisco Certified Academy Instructor. His research interest includes mathematics and cyber security.