NSEMX_Conf2021_005

A Brief Review of Proposed Models for Jamming Detection in Wireless Sensor Network

Grace AUDU, Michael DAVID and Abraham U. USMAN
grace.audu@st.futminna.edu.ng

ABSTRACT
Wireless sensor network (WSN) consists of a group of sensor nodes usually deployed in a hostile environment used for sensing, processing, transmitting and receiving data from the area. Sensor Nodes are characterized by limited memory, limited power and short transmission range, which exposes them to attacks like jamming. In this paper, we review different jamming attacks in WSN. We also review several proposed methods for detecting jamming. We have provided a comparative conclusion to aid researchers studying this field.

KEYWORDS: *Jamming, Jamming detection, Denial of Service Attacks, Wireless Sensor Network.*

I. INTRODUCTION

Wireless sensor network (WSN) consists of a group of sensor nodes usually deployed in a hostile environment used for sensing, processing, transmitting and receiving data where they are deployed to a base station (Osanaiye et al 2015).

WSNs have different applications. They find application were collecting data remotely is needed. These areas include military, environmental monitoring, health, controlling traffic, agriculture, and industries (Kumari et al, 2015). WSN have constrained power, storage, bandwidth and short communication distance. These constraints in addition to the open and shared wireless transmission medium makes sensor nodes prone to security attacks. Denial of Service (DoS) is one of the common attacks in WSN. These attacks occur in physical, link and network layer. At the physical layer, the most common DoS attack is jamming. Jamming occurs when a rogue node intentionally transmits a high-range signal to disrupt the normal transmission of information between legitimate nodes by reducing the signal to noise ratio. This attack affects the functionality of the network as it truncates the delivery of desired packets to the intended receiver hence impeding network capabilities (Bhushan & Sahoo ,2018). The major goal of jamming is to affect the long-term availability of sensor nodes. The jammer depletes the resources of sensor nodes by transmitting electromagnetic signals at high power towards the communication channel of the sensor nodes thereby prohibiting data from reaching its destination (Upadhyaya et al.2019).

Jamming can be perpetrated by listening passively to the communication channel in order to transmit at the same frequency as the legitimate sensor node. Jammers have high energy efficiency and are not easily detected (Pelechrinis et al., 2011)

Jamming attack may be mitigated by increasing the robustness of the legitimate signal or by implementing frequency hopping. Due to the limited resources of WSN applying those solution is difficult. WSN, hence the need for detecting jamming. In this paper we describe types of jamming attacks, metrics used for detecting jamming and review the different proposed methods to detect jamming.

WIRELESS SENSOR NETWORK ARCHITECTURE

The WSN architecture is made up of five layers (Akyildiz & Vuran, 2010). These includes:

Physical layer: is responsible for transmission, modulation and receiving techniques.

Link layer: ensures bit are transferred without errors and it controls access to the channel.
Network layer: routes the data supplied by the transport layer.
Transport layer: This layer is needed when the network is going to be access by external networks; it helps to maintain the flow of data to prevent congestion.
Application Layer: provides software for numerous applications depending on the sensing task.
Jamming attack occurs at the physical and link layer.

II. JAMMING ATTACKS IN WIRELESS SENSOR NETWORK

Constant Jammer: constant jammer transmits random bits continuously on the channel to disrupt communication on the channel. This could lead to depletion of the legitimate node's energy. The constant jammer does not follow any

Medium Access Control (MAC) layer procedure before continually transmitting series of radio signals to interrupt legitimate signal transmission in the network. This jammer continuously transmits random bits that occupy the transmission path of the network, hence disrupting legitimate data transmissions initiated by nodes (Misra et al., 2010).

Deceptive jammer: A deceptive jammer continuously injects legitimate bit sequences into the communication channel without gaps in between. The sensor nodes believe that a legitimate transmission is going on, hence they remain in the listening state. Detecting deceptive jammers is difficult since they are aware of the network protocol (Misra et al., 2010).

Random Jammer: Random jammers moves from active mode to sleep mode and vice versa to save energy. During the active state, the attacker jams the network for a specific time then it turns off its transmitter and goes to sleep mode. The attacking node begins to transmit the malicious signal again, after a while then goes back to sleep mode; the sequence continues (Misra et al., 2010).

Reactive Jammer: Reactive jammers constantly sense the channel to listen for when packets are being transmitted. Once they detect a packet transmission on the channel, they begin to transmit malicious signals to disrupt the legitimate signal. This type of jammer reduces the rate of power dissipation and are hard to detect (Misra et al., 2010).

a. PROPOSED METHODS FOR DETECTING JAMMING IN WIRELESS SENSOR NETWORK

Research on jamming detection in WSNs has been ongoing for a while. A lot of proposed methods for detecting jamming involves either the use of dedicated tools or algorithms installed on the sensor nodes. Most of these proposed methods make use of information gathered a priori about some metrics of the node when it is jammed or normal. Some of these metrics include received signal strength(RSS), packet delivery ratio(PDR), packet inter arrival time(PIAT), packet sent ratio, bad packet ratio(BPR) signal to noise ratio(SNR), consumed energy, clear channel assessment.

Osanaiye et al. (2015) proposed an approach for detecting jamming attacks that uses the cluster-based topology. The EMWA algorithm used for detecting jamming is only installed on the cluster head and base station. The base station detects jamming in the member nodes while base stations detect jamming in the cluster head. In order to minimize overhead they used only metric packet IAT to detect jamming. In order to detect changes in traffic flow during situations of both non-jamming and jamming, a trace-driven experiment using EWMA was carried out. Results obtained from their work shows that their proposed model can detect jamming attack efficiently with little or no overhead in WSN from the 20th jammed packet.

Bikalpa et al. (2019) in their work proposed a node-centric approach. To reduce overhead in nodes in this detection method, network information for detecting jamming are passively gathered by anchor nodes placed in the network. Using random forest algorithm, the information gathered a prior about the network is used differentiate when the network is jammed or not. Their work achieved 89.7% and 98.6% accuracy using RSSI from five anchor nodes for real and simulated data respectively.

In their work, Youness et al., (2020) used four metrics BDR, PDR, RSS and clear channel to identify the presence of jamming attack. They generated a large set of data in a real environment simulation and gathered measurements of these parameters when the network was jammed and when it was normal. They then used these data sets to train, validate, and test the machine learning algorithms. The simulation results showed that the proposed detects jamming attacks with an accuracy of 97.5%.

Ganeshkumar et al. (2016) proposed a framework that also uses cluster-based topology for jamming detection. They used statistical tests to compute the detection metrics normal threshold. The cluster head verifies if a packet received is from a legitimate node. The framework validates whether the node is a legitimate node by using the cluster head code. Lastly, the auditing algorithm on the CH estimates the metrics (PDR, RSSI) and makes decision about "jammed situation" or "non-jammed situation. Their proposed framework detects jamming with an accuracy of 99.88%.

A fuzzy logic–based algorithm was proposed by Vijayakumar et al. (2018) for jamming detection in cluster-based wireless sensor networks. The detection metrics is checked by the cluster head to check for jamming. An accuracy of 99.89% was gotten from their simulation. The jamming detection metrics are checked by the cluster head at the lower level and by the base station at the higher level. There by reducing the overhead cost on the member nodes.

Mistra et al., (2010) proposed the use of a fuzzy inference-based system for jamming at the base stations using three metrics. These metrics include received signal strength, total packets received during a period and the number of dropped packets during that period. The power received signal is measured at the base during the jamming attack to find the difference in value between the normal RSS.The total packets received during a specific period and the packet sent over the period is used at the base station to determine the packet drop per terminal (PDPT) and signal-

to-noise ratio (SNR). These metrics are then inputted to obtain the jamming index from the fuzzy inference system. The jamming index varies from 0 to 100. The system's true-detection rate is as high as 99.8%. In a Table 1, we present a summarize Comparison of Proposed Methods for Jamming detection in Wireless Sensor Network.

TABLE 1: Comparison of Proposed Methods for Detecting Jamming in Wireless Sensor Network

REFERENCE	MACHINE LEARNING OR NON-MACHINE LEARNING METHOD	ALGORITHM USED	Metrics	WSN STRUCTURE	ACCURACY
Osanaiye *et al* (2015)	Non-Machine Learning Method	EMWA	IAT	Cluster	100% >20 Jammed packets
Bikalpa *et al.* (2019)	Machine Learning method	Random forest	RSS	Flat	89.7% for real data and 98.6 for simulated data
Youness *et al*., (2020)	Machine Learning method	Random forest	BPR, PDR, RSS	Flat	97.5%.
Ganeshkumar *et al.,* (2016)	Non-Machine Learning Method	Auditing algorithm	PDR and RSSI	Cluster	99.88 %.
Vijayakumar *et al*.,(2018	Non-Machine Learning Method	Fuzzy logic–based jamming detection algorithm	PDR and RSSI	Cluster	99.89 %.
Misra *et al.,* 2010	Non-Machine Learning Method	Fuzzy logic	PDR, RSS	Cluster	99.89 %.

A fuzzy inference-based system to detect jamming attacks in the base stations using three metrics measured from each sensor node in the network was proposed by Mistra *et al*., (2010). These metrics are the total packets received during a specific period, the number of dropped packets during that period and the received signal strength (RSS). The base station computes the power received during the jamming attack to find any difference in value between the current RSS and the normal RSS. These values are used by the base station to compute the packet drop per terminal (PDPT) and signal-to-noise ratio (SNR) which is further used as inputs for the fuzzy inference system to obtain the jamming index The jamming index varies from 0 to 100 and is used to determine the intensity of the jamming attack, which can range between a situation of 'no jamming' to absolute jamming'. The system with its high robustness, ability to grade nodes with jamming indices, and its true-detection rate as high as 99.8%, is worthy of consideration for information warfare defense purposes. In a Table 1, we present a summarize Comparison of Proposed Methods for Detecting Jamming in Wireless Sensor Network.

III. CONCLUSION

In this paper, we presented a brief survey about jamming detection in wireless sensor networks. Different jamming attacks occurring in WSNs are described in detail. Different metrics used for detecting jamming was described. The different types of jamming are described, and detection techniques of jamming has been is pointed out. Our future work will focus on improving jamming detection.

ACKNOWLEDGEMENTS

The authors sincerely thank the reviewers for proofreading the article and providing constructive feedback.

REFERENCES

O.A. Osanaiye, S.A. Attahiru, & Gerhard P. Hancke (2018). A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Network. *Sensors*, 1691(18) 1-15

Saru Kumari, Muhammad Khurram Khan, and Mohammed Atiquzzaman. (2015). User authentication schemes for wireless sensor networks. *Ad Hoc Netw*. 27, C (April 2015), 159–194.DOI:https://doi.org/10.1016/j.adhoc.2014.11.018

B. Upadhyaya, S. Sun and B. Sikdar (2019). Machine Learning-based Jamming Detection in Wireless IoT Networks. *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS),* 1-5.

Bhushan, B. & Sahoo, G. (2018). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. *Wireless PersCommun* 98, 2037–2077. https://doi.org/10.1007/s11277-017-4962-0

Y. Arjoune, F. Salahdine, S.Islam, E. Ghribi & N. Kaabouch(2020). A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication. *The 34th International Conference on Information Networking (ICOIN 2020)* ffhal02509430f, 1-5.

Ganeshkumar, P. , Vijayakumar, K. , & Anandaraj, M. (2016). A novel jammer detection framework for cluster-based wireless sensor networks. *J Wireless Com Network, 2016 (1*). doi: 10.1186/s13638-016-0528-1

K. P. Vijayakumar,P. Ganeshkumar, M. Anandaraj, K. Selvaraj & P. Sivakumar(2018). Fuzzy logic–based jamming detection algorithm for cluster based wireless sensor network. Int Journal of Communication Systems 31(10), 1-21.

Misra, S., Singh, R. & Mohan, S.V.R (2010). Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Inference System. *Sensors* 2010, *10*, 3444-3479. https://doi.org/10.3390/s100403444

Osanaiye, O., Choo, K.K.R. & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. 2016, 67, 147–165. Journal of Network and Computer Applications 67, 147-165 https://doi.org/10.1016/j.jnca.2016.01.001

Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. (2011). Denial of service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tutor. 2011*, 13, 245–257.

Ian F. Akyildiz & Mehmet Can Vuran(2010). WSN Architecture and Protocol Stack. *Wireless Sensor Networks* 10-15

NSEMX_Conf2021_006

Design and Implementation of a Fire/Gas Safety System with SMS and Call Notification

M. A. Kolade, K.A. Abu-bilal, U.F. Abdu-Aguye, Z.Z Muhammad, and Kassim A. Y
Department of Telecommunications Engineering,
Ahmadu Bello University Zaria, Nigeria
Email: medinatapampa@yahoo.com

ABSTRACT
Swift and effective communication have a tremendous effect on the outcome of the safety and incidences. With the increase in domestic use of Liquefied gas in developing country coupled with poor infrastructures and low level of literacy, it is paramount to incorporate prompt safety measures to safeguard life and properties. The availability and wide acceptance of mobile phones in the countries make them a suitable communication means, for swift and effective remote monitoring and control. Design and implementation of a fire and gas detection system with SMS and call notification was carried out in this paper. This system is divided into three units, the control unit, sensing unit, and the alert unit. The designed system uses a micro-controller and GSM module, to translating and relate the output from the sensors. The codes used by the micro-controller were developed in Arduino IDE (Independent Development Environment) using Arduino language. The prototype of the system was developed using MQ9 and KY-026 for the gas and fire sensor respectively located at specific locations in the home. The GSM module was used to enable remote communication to the user mobile phone. It receives the information from the micro-controller and then acts as programmed. The prototyped system was subjected to load and no-load test in which the system was found to be working normally in accordance with the design specifications. When the system was subjected to reliability test, an index of 0.85 was obtained based on the failure rate of each of the component used in fabricating the system. The design system has the potential of reducing loss of lives and property to fire outbreak and gas leakages, due to its remote and surrounding alerting capabilities.

KEYWORDS: *Mobile phone, GSM module (SIM800), Arduino UNO, Gas Sensor, Fire Sensor.*

1. INTRODUCTION

Gas leakages and fire incidence are common occurrence in today's world especially in developing country where safety is least considered coupled with low level of literacy. Where fire or gas leakage is been detected early and responded to as appropriately, probability of getting out of control can be litigated. (1) designed a GSM based low-cost gas Leakage, explosion, and fire alert system with advanced security. The system is designed such that in case fire or gas leakage occurs a buzzer is turned on, an LCD outputs a message indicating the reason for the alarm and an SMS is sent to the home owner. (2) Also propose such a system, where a gas sensor is used to detect gas leakage and subsequently, turn the exhaust fan on. [4] Developed a similar system with an addition to monitor rapid temperature increase in a home. (3) Also improved on subsequent systems with a system equipped to open an exit windows to allow for diffusion of the concentrated air in case of gas leakage similar to (2), (5) in another related system, in the event of a fire, the system is equipped with a solenoid valve controlled water/carbon dioxide reservoir to douse the fire, as well as an alert system.

It is evident from the reviewed literatures that a lot of research has been done on fire and gas leakage detection systems with some going further to control the situation. Most of the implemented systems are to turn on buzzer and send SMS to the homeowner, without additional steps to ensure the sent SMS are viewed with required urgency. Hence a need for a system with an increase the probability of sent SMS been read received the required urgency which is directly related to swift response from the homeowner.

2. MATERIALS AND METHORDS

In this section, the details of the design, hardware's and software's materials used in the implementation of the system are summarized.

2.1 The Design Structure

Figure 1 shows the block diagram of the Fire/Gas Safety System. It consists of a power supply unit which supplies required power to other subsystems. The control unit consist of a programmable microcontroller - Arduino UNO, fire sensor – KY-026 and gas sensor – MQ-9 and the alert unit which consist of the GSM-module and the buzzer. The GSM module serves as the communication bridge between the microcontroller and the user's phone. SMS messages and call from the system in case of emergency are sent to the user's phone through the GSM module. The system is divided into two sections: Hardware and software.

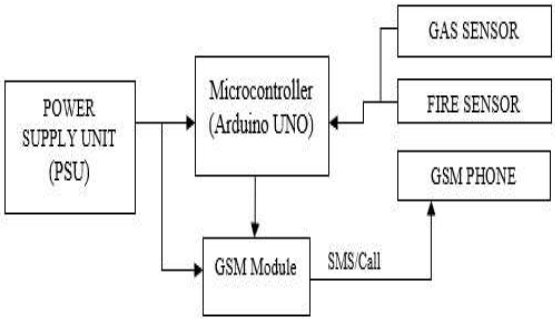


Figure 1: Block Diagram of the Fire/Gas Detection System

2.2 Hardware Design and Selection

The hardware components used are Arduino UNO, KY-026, MQ-9, GSM module SIM800, 240V/12V 3A transformer, four diodes 1N4001, filtering capacitor 2000uf and 5V 2A regulator LM78S05 and buzzer.

Detailed analysis of the various hardware units is given below.

2.2.1 Power Supply Unit

This unit is made up of several sections, the system component's power requirement is considered in this design. The control unit requires a 5V 500mA for the Arduino UNO, while SIM800 requires between 3.4V - 4.4V and 1A current for reliable operation. The fire and smoke sensors both require 3.5V - 5V and current of about 200mA. The power supply should be able to provide the combine current of 2A. Figure 2 shows the block diagram of the power supply unit.

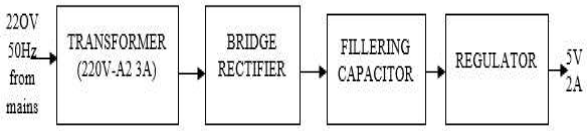


Figure 2: Block Diagram of the Power Supply Unit

The power supply unit consists of a stepdown transformer that has an output of 14V AC with output current of about 1A, a full bridge rectifier, a voltage regulator (7805) and a filter. The power requirement of the security system is 5V.

The transformer design and selection: The 220V AC from the mains is stepped down to 14V AC with the help of the transformer. The peak voltage output of the transformer is calculated using equation (1).

$$V_{peak} = \sqrt{2} \times V_{rms} \quad (1)$$

Where, $V_{rms} = 14V$

$$V_{peak} = \sqrt{2} \times 14$$

$$V_{peak} = 19.80V$$

Rectifier diode design and selection: Four 1N4001 diode connected in bridge were used for the full wave rectification of the output voltage from the transformer. IN4001 was chosen because its PIV (Peak Inverse Voltage) is 50V which is greater than V_{peak} which is approximately 20V.The value of the rectified voltage is calculated as follows.

$$V_{dc} = (2 / \pi) \times V_{peak} \quad (2)$$

But $V_{peak} = 19.80V$

$$V_{dc} = (2/\pi) \times 19.80$$

$$V_{dc} = 12.61V$$

Voltage regulation and filter design: For the section of the home security system which requires a 5V power supply, a 5V regulator (LM7805) was used. The choice is based on the IC's ability to keep its output voltage stable at 5V and it can provide up to 1A load current. LM7805 also have attached heat sink to conduct the generated heat away from it under working condition. For the filter section it is preferable to choose a filtering capacitor that holds the peak-to-peak ripples (RF) at approximately 70% - 80% of the peak voltage. The smaller the ripple factor the better the performance of the filter.

Therefore, using design specifications, the value of the capacitor can be calculated as follows:
From the relations:

$$Q = C \times V \quad (3)$$
$$Q = I \times T \quad (4)$$
$$f = \frac{1}{T} \quad (5)$$

$$I_{min} = I_{dc} = 1A$$

Here, C is filtering capacitor, Q is charge in colombs, I is current taken by the load, T is period in seconds and f is frequency in Hz. Using, equations (3) and (4) and substituting for T from equation (5), yields:

$$C = \frac{I}{Vf} \quad (6)$$

But V is the peak-to-peak voltage, and RF is the ripple factor. To calculate its value, the relation of equation (7) is used

$$V = RF \times V_{rms} \quad (7)$$

V_{rms} is given by $\sqrt{2} \times V_m$ where V_m is the system required voltage 5V, the mains frequency is 50Hz and the RF is 70%.
Therefore

$$V = 0.7 \times \sqrt{2} \times 5$$
V = 4.949 Volts
And $C = \frac{1}{4.949 \times 50}$
C = 4040µf

The standard available value used is 4400µf, where two 2200µf are connected in parallel. Figure 3 shows the circuit diagram of the power supply unit of the fire/gas detection system.

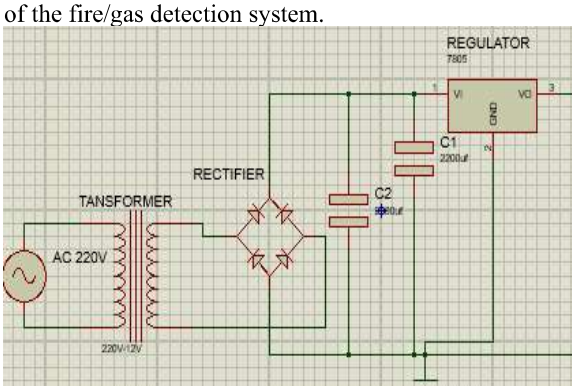


Figure 3: Circuit Diagram of Power Supply Unit

2.2.2 Control Unit: This unit is made up of three main components which are: Arduino UNO, fire sensor and smoke sensor.

Arduino UNO: is a board embedded with ATmega328 a microcontroller, ATmega328 is an integrated circuit (IC) containing all the main parts of a typical computer, which are: Processor, Memories, Peripherals, Inputs, and Outputs (6). It will provide required computing resource to achieve the aim. All communication and controls in this system pass through the microcontroller. The Arduino UNO has 14 digital input/output pins (of which 6 can be used as PWM-Pulse Width Modulation- outputs), 6 analogue inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an In-Circuit Serial Programming (ICSP) header, and a reset button. It contains everything needed to support the microcontroller. Arduino UNO board is shown in Figure 4.

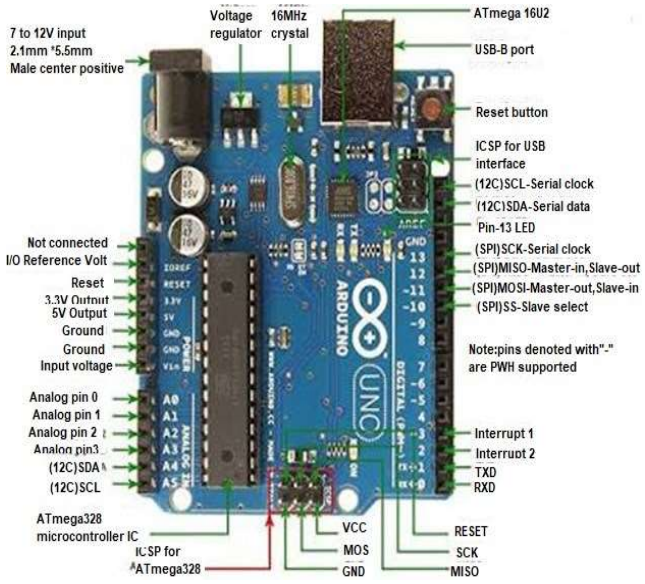


Figure 4: The Arduino UNO Board

Fire Sensor KY-026: The KY-026 consist of a 5mm infra-red receiver LED, a LM393 dual differential comparator a 3296W trimmer potentiometer, six resistors and two indicator LEDs. (7) The board features an analogue and a digital output. Its operating voltage ranging between 3.3V to 5V and Infrared Wavelength detection of about 760nm to 1100nm.The connected photo diode is sensitive to the spectral range of light, which is created by open flames. Digital Out: After detecting a flame, a signal will be outputted. The sensor has 3 main components on its circuit board. First, the

sensor unit at the front of the module, which measures the area physically and sends an analogue signal to the second unit, the amplifier. The amplifier amplifies the signal, according to the resistant value of the potentiometer, and sends the signal to the analogue output of the module. The third component is a comparator which switches the digital out and the LED if the signal falls under a specific value. You can control the sensitivity by adjusting the potentiometer. A KY-026 Fire Sensor is shown in Figure 5.

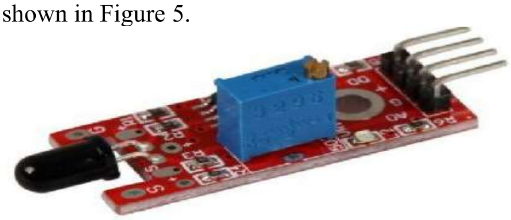
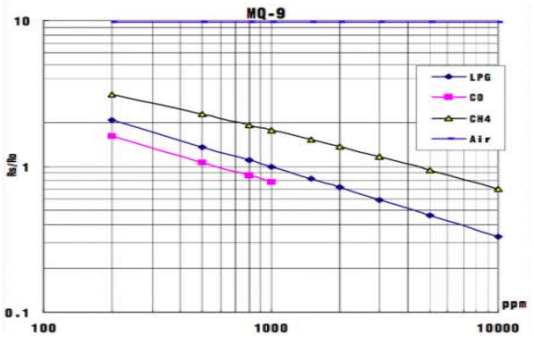


Figure 5: Fire Sensor KY-026

Gas Sensor MQ-9: (7) MQ-9 consist of a sensitive material (SnO2), which has lower conductivity in clean air, the sensors conductivity increases as concentration of carbon monoxide and hydrocarbon in the air increases. Detection is made by method of cycle high and low temperature. It has a working voltage of 5V, a with wide 2-20kΩ range of resistance and able to detect concentration of about 200ppm minimum and 10000ppm maximum. (7) A relationship between the voltage output and gas concentration level for various common gases is shown in table 1.

Table 1: Output Voltage against Gas Detected Concentration Level



2.2.3. The Alerting Unit

The alerting or output unit comprises of the GSM module and buzzer, both are to relate information from the controller, they are the link between the user and the system's control section.

GSM Module SIM800: SIM800 is a cellular communication module that can make calls, send email, SMS, and even connect to the internet. The module operates like a mobile phone, but it needs external peripherals to function properly. Figure 6 show the image of a SIM800 board.

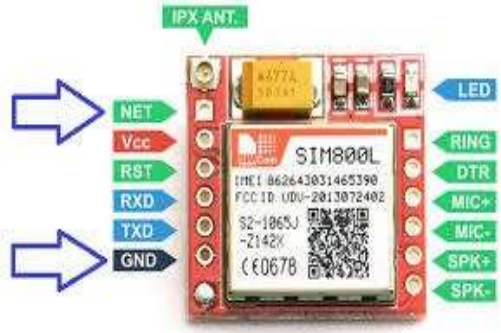


Figure 6: SIM800 Board

The module has audio channels which include a microphone input and a receiver output, a SIM card interface, and it is Quad band hence can connect to any global GSM network with any 2G SIM. The receiver pin (RXD) of the module is connected to transmitter pin (02) of Arduino while the transmitter pin (TXD) of the module is connected to the receiver pin (01) of Arduino, V_{cc} pin of the module is connected to the LM78S05 in voltage divider circuit and GND pin to the ground. Communication speed (baud rate) depends on the board to be paired with, baud rate of 115200 was chosen, this rate allows for successful communication between SIM800 and Arduino UNO.

Buzzer:

A buzzer is an electronics component usually used to add sound feature to systems, the buzzer is associated with switching ON or turning OFF at required time and adequate interval. The buzzer is powered with 5V DC and controlled through the Arduino. It has two terminals, the positive terminal is identified by (+) symbol or longer terminal lead, while the negative terminal is identified by (-) symbol or shorter terminal lead.

The hardware of the system unit comprises of LEDs-which serves as indicators, resistors, GSM module (SIM800), fire sensor, gas sensor, buzzer, and Arduino UNO. The receiver pin Pin 0 of Arduino is connected to the transmitter pin Pin Tx of SIM800 and the receiver pin Pin Rx of SIM800 is connected to transmitter pin pin1 of the Arduino, the signal pin GPIO of SIM800 is connected to pin 9 of Arduino, analog pin (A01) of the Arduino is connected to the signal pin SIC of MQ-9, while the analog pin (A02) of Arduino is connected to the analog signal pin A0 of KY-026 as showed in Figure 6. Power requirement of SIM800 is 3.3V 20mA, 3.3V for KY-026 and 5V for MQ-9. LED1 is connected to digital pin10, LED2 is connected to digital pin13. The LEDs were connected in a series connection with resistors in a simple way to stabilize the current flowing through them. Also, the buzzer is connected to pin4 of the microcontroller through an amplifying transistor, which controls the switch ON and OFF the buzzer. Figure 7 the circuit diagram of the alert units and control unit.

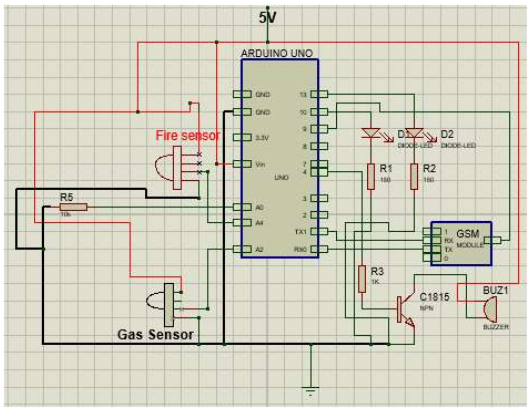


Figure 7: Circuit Diagram of GSM, Fire Sensor and Gas Sensor connected to Arduino UNO

Design and calculations:

Led design

LEDs voltage drop V_f is between 1.8V - 2.5V (a worst case is used in the design, 2.5V) and operating current I is 20mA, while V_s (supply voltage) is equal to 5V (from Arduino pin). Using these values, the value of the current limiting resistors can be obtained.

Ohms law, equation (8) was used to calculate the value of the Resistors R ($R_1$and R_2), as shown.

$$R = \frac{(V_S - V_f)}{I} \qquad (8)$$

$$R = \frac{(5-2.5)}{(20\times10^{-3})}$$

$$R = 125\Omega$$

From the obtained value of 125 ohms a standard value of **150 Ω±20%** was chosen for R_1andR_2.

Buzzer circuitry:

The home-based alert system (buzzer) requires an amplifying circuit. The amplification circuit requires a multipurpose NPN transistor (C1815) with a base resistor R_3 required to provide base current for the transistor. The value of the resistor (R_3) was calculated using equations (9):

$$R = \frac{(V_S - V_f)}{I} \qquad (9)$$

Where V is the powered voltage from the Arduino UNO 5V, V_{be} is the base-emitter voltage 0.7V and I_b is the base current (500uA)

$$R_3 = \frac{5-0.7}{0.005}$$

$$R_3 = 860\Omega$$

From the obtained value of 860 ohms a standard value of **1k Ω±20%** was chosen. The complete circuit diagram of the whole system with the power supply is shown in figure 8.

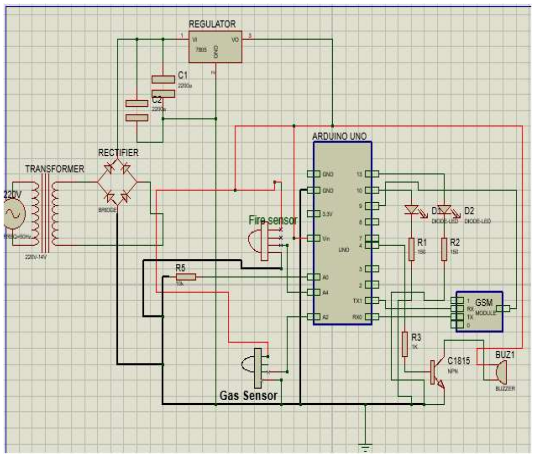


Figure 8: Circuit Diagram of the Complete System

2.3 Writing Source code for the microcontroller Arduino UNO

The source code is written to satisfy the requirement of system whose main controller is an Arduino UNO. The program was written in the Arduino IDE.

The flowchart of Figure 9 was used to develop the program.

2.3.1 Software Design Methodology

The software used in this work to control and synchronize the activities of all system parts to function as a unit is implemented using the flowchart in Figure 8. The software codes were written in Arduino integrated development environment (IDE) with Arduino programming language.

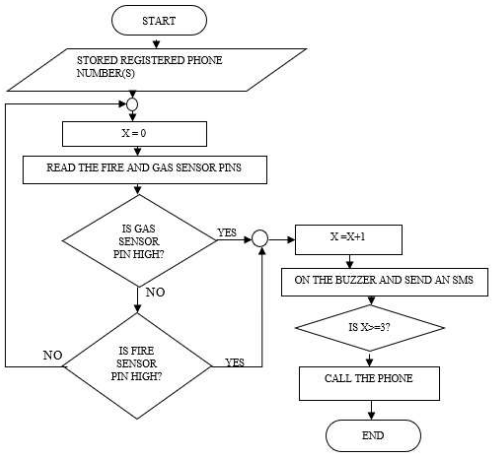


Figure 9: Flow Chart of the System Control

3. RESULTS AND DISCUSSION

3.1 Testing of the designed circuit and components

All the components used were tested to ensure workability before and after physical construction of the system's porotype to ensure that all contacts and connections were made properly. Test was conducted at unit levels. The tests conducted were categories into hardware and software test.

The hardware unit was initially designed and simulated using circuit wizard and proteus, this is to ascertain the circuit is working properly based on design specifications. After which the components are put onto breadboard for further testing and finally soldered on the Vero-board. Figure 10 shows simulation of the power supply unit.

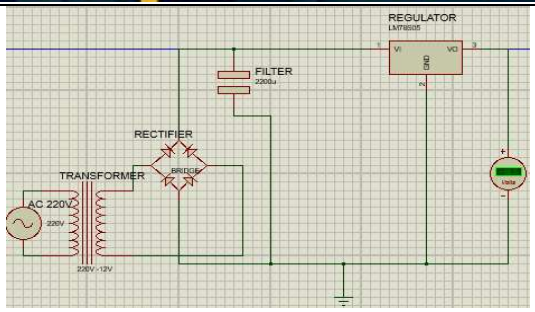


Figure 10: Screen Shot of the Power Supply during Simulation

Controller Unit

The controller unit comprises of the microcontroller board, fire detector, gas detector and the GSM module. Software was uploaded on the microcontroller and the response to stimuli from both the fire and gas detectors was monitor via the communication 3 port (COM3) of the computer. This test makes it possible to understand what is happening inside the microcontroller. The GSM module has in it a registered subscriber identification module (SIM) card. Once the GSM module is connected to power, a blinking green led (with about 2 seconds interval) on it indicates a successful connection to network. Software was also written in the microcontroller to output status of network connection. The software is presented in appendix A. Figure 11 presents the COM3 output during a stage of the test period.

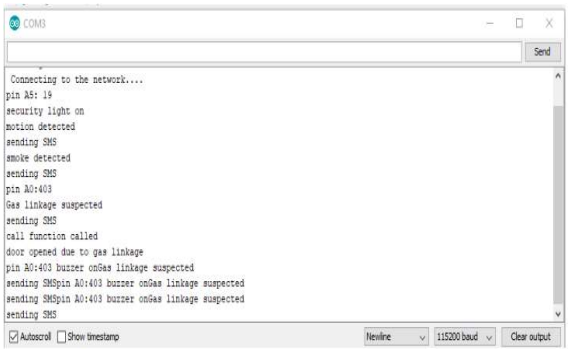


Figure 11: Software Test Result

3.3 Fire Sensor/Gas Sensor

The sensors were both tested with same situation while connected to a DC battery, a beep from both

sensors, indicate they are both in good condition, their functionality is ensured.

3.4 System Test

The full system test was to ensure proper response is given by the developed system in a case of fire outbreak or gas leakage when required by the homeowner. The system was initially designed and simulated in proteus environment, to ensure the system is working perfectly based on design specifications. The system was constructed on a breadboard; this was to ensure proper arrangement in other to ensure a potable system. Finally, the system was implemented and tested on a Vero-board.

3.4.1. Simulation Test

This simulation was carried out using Circuit Wizard, this helped in design of the circuit and testing it with software uploaded, to ascertain the circuit is working properly based on design specifications. After which the components are put onto breadboard for further testing and finally soldered on the Vero-board.

3.4.2. No - Load Test

This test was carried out when the circuit has been developed on a Vero board. A state at which the system is not faced with any control responsibility, this is the verification stage. Physical inspection was done to ensure all components and connections were in place. This was done by checking all closed tracks, jumper wires etc. for open or short circuit. Power was fed to the circuit for a minute. Fingertip was then used to sense the temperature of the components if any was overheating. Also, code inspection was carried out to ensure optimal use of memory, by employing DRY (Don't Repeat Yourself) technique. DRY technique is a principle in software development implemented to reduce software duplication. Being satisfied with this test result, load test then followed.

3.4.3. Load Test

At this stage, power consumption was monitored to ensure power specifications are met, with the voltmeter, the current consumption of the circuit was taken note of - when a response is required and when not. The response time to control was also monitored. For the software aspect, the performance of the code was scrutinized, the software was compiled and executed, parameters such as memory usage, CPU usage, response time and overall performance for the software were analyzed. Voltage test then followed. This was performed with a digital multi-meter. Voltage and current level at different points on the board was taken and compared with design specification. Figure 11 shows the test diagram used during voltage and current consumption test.

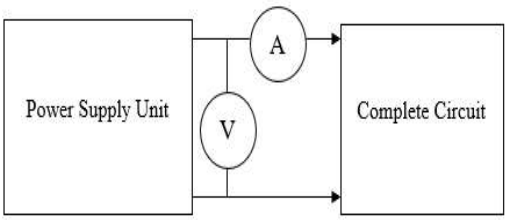


Figure 11: Test Diagram for Voltage and Current Consumption

The current consumption test of the system was carried out using two instances, when response is required and when not. This test was repeated several times and an average value computed. The voltage at the Arduino power pin was also monitored, to ensure conformance with design specifications. Results of the voltage and current test carried out are presented in Table 2 and Figure 12 shows a test instance.

Table 2: Voltage and Current Consumption Readings.

S/N	No load current (A)	Load current (A)	Voltage (V)
1	0.234	0.45	5.12
2	0.232	0.43	4.97
3	0.201	0.46	5.09
4	0.200	0.42	5.00
5	0.221	0.41	5.05
Average	0.217	0.434	5.056

Figure 12: System Current Load Test

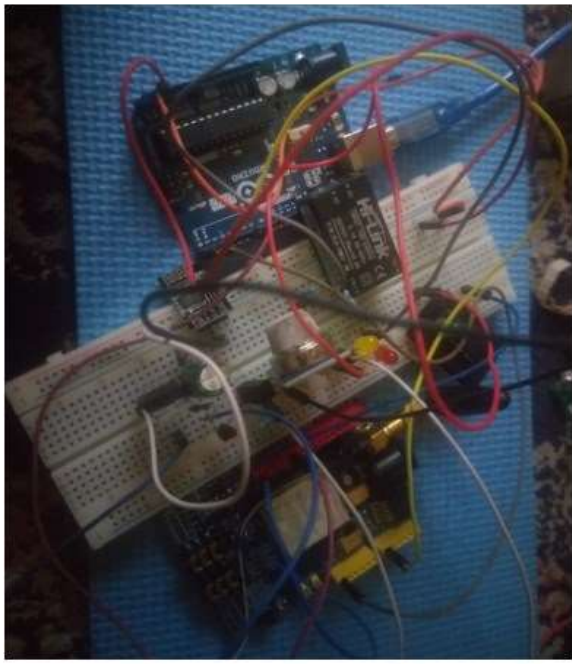


Figure 13: System on the Breadboard

Figure 14: The System Prototype

3.4.4. Reliability Test

The reliability test of the developed system was done using Part Count Failure Rate Techniques where reliability of a system is approximate as a relation of the units of parts used in the system design. Computation was done using relation with time to failure test. During this test, values of data are recorded which can be put into cumulative function, F(t). Reliability is express explicitly by equation (9) (8):

$$F(t) = 1 - R(t) \quad (9)$$

The method used in calculating the reliability of system requires information like part category, part quantities and quality factor. The system failure rate is defined in equation (10) (9). Where F_i is given as failure rate of ith part, n is number of part category, N_i is quantity of the part and π_{Q_i} is the quality factor of the ith part:

$$F = \sum_{i=1}^{n} N_i F_i \pi_{Q_i} \quad (10)$$

The failure rate of each unit was computed using equation (10) with data from reliability prediction of electronic equipment handbook table obtained from (9) and (10). The calculated failure rate of the security system is presented in Table 3. Equation (10) was used to compute the value of the reliability of the system.

From Table 3: the Calculated Failure Rate of the individual components was used to determine that of

Table 3: Calculated Failure Rate of Fire/Gas Safety System

S/N	Components	Fi/ 10^6 hours	N (category)	Ni (units)	π_{Q_i}	F10^{-5}/ 10^6 hours
1	Resistors	0.000196	1	3	0.03	1.764
2	Capacitors	0.000002	1	2	0.01	0.004
3	ICs	0.73	1	1	0.0043	313.9
4	Microcontrollers	0.015	1	1	2.4	3600
5	Semiconductors	0.0038	2	6	8.0	364.8
6	Mechanical device	0.083	1	1	0.103	854.9
7	Modules	0.028	2	3	0.26	4368
8	Inductive devices	0.0030	`1	1	0.30	90
9	Connector	0.040	1	2	0.659	5272
10	Contact/Hand soldering	0.0064	1	27	0.0013	22.464
11	Total failure rate of the system					14887.504

the system. The failure rate was then used to obtain the system reliability using equation (9) as shown below.

$$R(t) = 1 - 0.14887504$$

$$R(t) = 0.85115196$$

$$R(t) \approx 0.85$$

4. CONCLUSION

The detailed procedure for the design and implementation of a fire and gas safety system with SMS and call notification was outline in this work. The designed system was simulated using proteus, the simulated system was then fabricated using hardware components. The fabricated prototyped system worked normally as designed. The system is light in weight (that is portable) and has a reliability index of 0.85 when subjected to reliability test. The design system has the potential of reducing loss of lives and property to fire outbreak and gas leakages, due to its remote and surrounding alerting capabilities.

REFERENCES

P. Ghosh and P. K. Dhar, "GSM Based Low-cost Gas Leakage, Explosion and Fire Alert System with Advanced Security," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-5, doi: 10.1109/ECACE.2019.8679411.

M. A. F. Malbog, H. D. Grimaldo, L. L. Lacatan, R. M. Dellosa and Y. D. Austria, "LPG Leakage and Flame Detection with SMS Notification and Alarm System: Rule-Based Method," 2020 11th IEEE Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2020, pp. 323-327, doi: 10.1109/ICSGRC49013.2020.9232494.

A. Y. Nasir, Adoyi Boniface, A.M. Hassan, N. M. Tahir "Development of a Gas Leakage Detector with Temperature Control system, 2019" Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 6 Issue 12.

Rupali S. Gajare, Dr. P. M. Mahajan, "Home and Industrial Safety System for fire and gas Leakage detection, 2018", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 www.irjet.net p-ISSN: 2395-0072

Lacatan, Luisito & Dellosa, Rhowel & Malbog, Mon Arjay & Austria, Yolanda. (2020). LPG Leakage and Flame Detection with SMS Notification and Alarm System: Rule-Based Method. 10.1109/ICSGRC49013.2020.9232494

Arduino IDE available: www.arduino.org/downloads

MQ-9 data sheet assessed 06/12/2020 https://www.mouser.com/catalog/specsheets/Seed_101020045.pdf

"Proteus PCB Design & Simulation Software-Labcenter Electronics", labcenter.com, 2017. www.labcenter.com/ [Accessed: 26- jan-2020]

Walls, L., and Quigley, J. (2000). *Learning to Enhance Relaibility of Electronic Systems through Effective Modeling and Risk Assessment*. Available online: http://ieeexplore.ieee.org /document/816334

Military handbook on reliability prediction of electronic equipment (1990) (Available online: https://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf)

D. Kumar, Saurav, A. Yadav and Sharmila, "Easy to wear child guarding gadget," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777635.

Kyeongha Kwon, Seung Yun Heo, Injae Yoo, Anthony Banks, Michelle Chan, Jong Yoon Lee, Jun Bin Park, Jeonghyun Kim, John A Rogers (2019). Designed an automatic door system using a unique wireless ID by using infrared ray or Bluetooth technology. *Science Advances eaay2462*

Walls, L., and Quigley, J. (2000). *Learning to Enhance Relaibility of Electronic Systems through Effective Modeling and Risk Assessment*. Available online: http://ieeexplore.ieee.org/document/816334

Warrendale P.A. (1987). *Electronics Reliability Subcommittee*. Automotive electronics reliability handbook. Society of Automotive Engineers, Inc.page169,328-9

J. Chou (2000). *Hazardous Gas Monitors: A Practical Guide to Selection, Operation and Application*. Co-published by McGraw-Hill and SciTech Publishing