**Chapter ΙΙ**

**REVIEW OF LITERATURE AND STUDIES**

This chapter deals with review of related literature and studies, which are closely related to this research work. This chapter shows the other related literature and studies about this research based from theother researches and articles from the websites. This research also discusses the research paradigm and the definition of terms. All of this provides a basis to have a better stand for the research.

**Burglar Alarm System**

Burglar (or intrusion), alarms are electronic alarms designed to alert the user to a specific danger. Sensors are connected to a control unit via low-voltage wiring or a narrowband RF signal which is used to interact with a response device. The most common security sensors are used to indicate the opening of a door or window or detect motion via passive infrared (PIR). New construction systems are predominately hardwired for economy. Retrofit installations often use wireless systems for a faster, more economical installation. Some systems serve a single purpose of burglar or fire protection. Combination systems provide both fire and intrusion protection. Systems range from small, self-contained noisemakers, to complicated, multi-zoned systems with color-coded computer monitor outputs. Many of these concepts also apply to portable alarms for protecting cars, trucks or other vehicles and their contents (i.e., "car alarms"). Burglar alarms (or perimeter security systems, perimeter detection systems, Perimeter protection, intrusion detection systems and many more terms for the same thing) are divided to two main fields: home burglar alarms and industrial burglar and perimeter intrusion detection.

**Principle of Burglar Alarm**

All alarms systems consist of three main component areas such as Detection Devices, to detect if an intrusion has occurred. Warning devices, bells, sirens and remote monitoring. Control Panel, to control the various states of the system and a Power Supplies, including backup batteries.

**Detection Devices**

Detection devices do exactly as the name implies, these are the senses of the system and detect intrusion by a number of different means. One of the most common detection devices is the contact switch which detects the opening of windows, doors, etc. Numerous different types of contacts are available for different applications such as roller shutters requiring large heavy duty types or domestic doors requiring neat flush fitting types. From a burglars point of view, it is some times more convenient to smash their way through a door or window than to open it and some even less desirable methods have been employed for gaining access to a premises. Other types of detection are used where this is a risk. Devices such as lead foil tape can be used for glass sections or closed circuit wiring for semi-solid structures such as doors, walls, etc. These last two types are relatively old forms of detection and although they facilitate a very inexpensive installation they have the disadvantage in that they must be replaced after an attack has occurred. A more modern device for detecting forced entry is the vibration sensor (or inertia sensor). Primarily it has the advantage, in that it can be easily installed and, coupled with the relevant analyzer it can differentiate between different types of vibrations. This makes it very suitable for different structures e.g.; solid walls, glass, wood, etc. In some cases, it is not always cost effective to cover every entry point so units such as motion detectors can be used and in fact these detectors are used quite extensively in modern domestic and commercial systems. A motion detector, as the name implies, detects the motion of an intruder within a certain area. The maximum range of these detectors is about 35 meters.

**Warning Devices**

These are devices to alert the owner of the house or facility that alarmhas been installed in. Some of the devices use include Bells, Sirens and Remote Monitoring.

**Control Panel**

This is the heart and local brain of the system. It receives the first notification that an alarm condition has occurred and then decides what action has to be taken. With simpler panels this usually means activating the warning devices. With microprocessor type panels this action could be considerably more complex such as interrogating the detection device to verify the condition, recording events in the memory or ignoring the device until it activates again. Control panels display conditions by means of lights or LED’s flight emitting diodes on the front of the panel e.g., clear, fault, mains on, etc. For more sophisticated panels this is sometimes effected by means of an alphanumeric display. A series of words and numbers will be produced on a screen such as, zone one open, tamper zone three, etc. A key switch or keypad is provided to switch the system on or off. Again with more complex panels the keypad can be used to perform functions like interrogating the memory, inhibiting a zone, testing the warning devices and programming the system to react in the required manner to different situations.

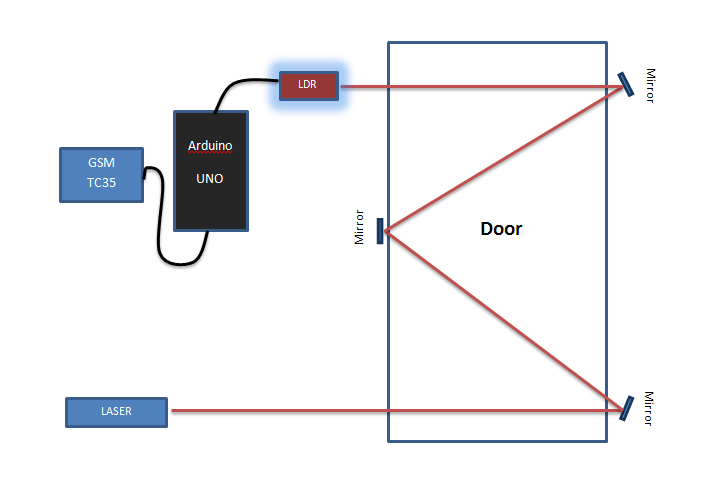
**Power Supplies**

Power for the alarm system is derived from the 220V AC mains supply. It is converted to 12V DC by the power supply unit and it is this voltage that is used for the System should a mains failure occur then standby batteries, housed inside/the control panel, will take over and power the system. When mains return these batteries will automatically recharge. (<https://www.academia.edu/3824247/LITERATURE_REVIEW_OF_A_BURGLAR_ALARM_SYSTEM>)

**Design of SMS Based Intruder Alarm**

The first step in designing the block diagram of the equipment that used was to consider the aspects of the equipment and its location where the installation was occur. Before the installation, all of the equipment was needed to test to prove that the equipment was in a good condition.

From an operational standpoint, equipment that operates independently from other equipment was a good candidate for the main distributor. In either case the I/O subsystem can distribute to varying degrees, based on the physical layout of the equipment in other system.



**P.S**

**P.S**

**Figure 1.***SMS Based Intruder Alarm Layout Design*

In Fig.1 it shows the design of the SMS Based Intruder Alarm. When designing the system, the LASER beam throw a monochromatic light that proceed to the mirror (optional) and the mirror throw the light directly proportion through to the photoresistor where the photoresistorgive signal if the light cut off. The Arduino UNO send signal thru to the GSM TC35 and the GSM will send a message to the proponents.

**Related Studies**

To protect the household from these possible incidents of intrusion, several studies were made to develop home security systems for the occupants’ convenience and safety especially during the day.

Yanbo Zhao and Zhaohui Ye of the Dept. of Automation of Tsinghua University in Beijing developed a low cost GSM/GPRS based wireless home security system. The system is a wireless home network which contains a GSM/GPRS gateway and three kinds of wireless security sensor nodes that are door security nodes, infrared security nodes and fire alarm nodes. The nodes are easy installing. The system can response rapidly to alarm incidents and has a friendly user interface including a LCD (liquid crystal display) and a capacitive sensor keyboard. The wireless communication protocol between the gateway and the nodes is also suitable for other home appliances.

This study used wireless technology to interconnect the components of the system. It is low cost and easy to use. The system becomes ineffective when there is no one to alarm or notify about an incident. The author decided not to integrate wireless technology in connecting the design components, but in communicating with the security administrator himself.

Dechuan Chen and Meifang Wang from Hangzhou Dianzi University in China introduced an experimental home security monitoring and alarming system based on Zigbee technology, which is capable of monitoring door and window magnetic contact, smoke, gas leak, water flooding, providing simple controls such as turning off the valves, and sending the alarms to the residential area security network etc. The system used a control key fob for activating and deactivating the alarm easily, supports Web interface so that user can access the system remotely to control, search or review the history record, and offers a LCD panel for simple configuration. The experimental system had been designed and its wireless communication test result showed that the Zigbee wireless network can improve the home security with low power and easy to implement solution.

Similar to the aforementioned study, students from the College of Information Science & Engineering, North-eastern University in Shenyang researched an intelligent home security surveillance system based on ZigBee. In their study, they implemented real-time surveillance of the home security; the intelligent remote monitoring system was developed for home security based on ZigBee technology and GSM / GPRS network. The system can send abnormal images and warning messages through MMS and SMS; receive remote instruction, and remote monitor household appliances. Meanwhile, the introduction of a variety of sensors guaranteed that the intelligent remote monitoring system can be responsible for home security. The results of their experiment showed that the system can attain remote surveillance of intelligent home safety with high availability and reliability.

Their studies primarily focused on home security monitoring, real-time surveillance and monitoring of household appliances. However, these systems could be very expensive since they are highly intelligent. The former uses Web interface to allow the user to control the system remotely. This may be complicated for typical household occupants and may require several computing resources. The latter can actually process images taken from its surveillance cameras and decide whether these images are normal or not. It may also consume a lot of power for it uses several cameras and a variety of sensors. Also, this system has to utilize several computing resources, and a considerable amount of storage for its images.

Considering Axelsson’s demands of an intrusion detection system, this may seem to be impractical for a home security system. Ishiguro, K. and Runhe Huang of Hosei University in Japan describes in the “Implementation of a Wireless Communication Technologies-based Home Security System” a light weighted home security system that exploits the common use of wireless communication technology like mobile phone, Bluetooth communication, wireless sensors, etc. The paper discussed that the system scale must be small and the cost must be low, which is more suitable for the smaller scope of a home and a general civilian family.

Thus, the latter’s use of GSM technology and the former’s capability of monitoring door and window contact were used as bases for the development of the author’s conceptual model of a simpler, low-cost home intrusion detection system which is capable of reporting incidents to its security administrator using SMS messaging.

**Research Paradigm**

The study shows proper procedures of SMS Based Intruder Alarm System. The diagram is how the proponent illustrates the procedures required for the installation of the intruder alarm system.

* Assembling
* Installation
* Testing

SMS Based Intruder Alarm System in Electronics Laboratory

* Design Development
* Materials Procurement

INPUT

OUTPUT

PROCESS

**Figure 2.** *SMS Based Intruder Alarm System Paradigm*

As shown in figure 2, input represents the presentation and design of the materials to be used. While the process is the assembling, installation, and testing the device use inSMS Based Intruder Alarm System, and then output represents complete development of SMS Based Intruder Alarm System in Electronics Laboratory.