Design and Development of Intruder Detection Security Device

Principal Investigators: Engr. Dr. Icheke Linus Ejike

[Director of Engineering, National Engineering Design Development Institute, Nnewi]

Initiator/Team Lead: **Engr. Chukwu Nelson Nnaemeka**

[Assist Chief Engineer, National Engineering Design Development Institute, Nnewi]

Contact: 1-3 Emma Biu Street, Okpuno-egbu
Date: October 2025

1. Executive Summary

Our Intruder Detection Security Device is a cutting-edge solution designed to provide advanced security features for homes, offices, and industrial settings. This device utilizes state-of-the-art technology to detect and alert users of potential intruders, ensuring a safe and secure environment.

The security system is designed to detect intrusion, such as unauthorized entry, into a building or other areas such as a home, offices or schools. Security systems used in residential, commercial, industrial, and military properties protect against burglary (theft) or property damage, as well as personal protection against intruders. Security systems in neighborhoods show a connection with diminished robbery. Prisons also use security systems for the control of inmates.

Our team seeks funding to design and develop a low-cost, intelligent intruder detection security device aimed at enhancing safety and property protection in homes, offices, and public facilities. This project responds to the growing security challenges faced across the country due to frequent cases of burglary, vandalism, and unauthorized access to restricted areas.

The proposed device will integrate motion sensors, infrared technology, and microcontroller-based alert systems to detect intrusions and immediately trigger alarms or notifications via mobile devices and also vision via your mobile devices. Unlike existing commercial systems, this solution will be locally developed, cost-effective, and adaptable to varying security needs and environments.

2. Background and Problem Statement

2.1 INTRUSION DETECTION SYSTEM (IDS)

For the intent of this work, an Intrusion Detection System is defined as a system that is ‘designed to detect and signal the presence, entry or attempted entry of an intrusion into an alarmed or classified area’. It is a set of interconnected devices that is aimed to protect an

object, usually a facility, against intruders and to notify the owner or a monitoring station/center of any violation of the protected zones.

2.2 PROBLEM STATEMENT

This work is necessitated as a result of security breaches that often happen in our environment and household when we are not around or at night when we are asleep.

3. Project Objectives

The objectives are;

1. To design a device that is armed and disarmed from any location by the authorized Phone number or numbers and sends text messages to the authorized numbers in breach of security.

2. To design a device that responds in real time with an alarm and vision at the break-in of an intruder into a classified area.

3. To construct a security device that has inbuilt power supply system besides public utility.

4. To evaluate economic feasibility and promote commercialization in collaboration with NASENI in the area of security.

SCOPE OF THE WORK

To build a security device that is armed and disarmed from any location through the authorized phone number. The device also sounds an alarm in the process and sends a notification message to the authorized phone number and area view via mobile devices.

4. Technical Innovation & Design Description

1. You can control it from anywhere in Nigeria
2. No false alarm of any kind
3. It works on real time
4. It detects windows or doors not properly closed
5. It gives you the geographic map of the classified area
6. It has alarm system with different tones of warning.
7. It has the capacity to show area view via your mobile device.

System Components

- Subscriber Identification Module (Sim)
- Global System for Mobile Communication (GSM)
- Global Positioning System (GPS)
- AT Mega 328 Micro-controller
- Battery Module

4.1 Design Considerations

The intruder detection security device is made up of four operational modules. These include:

1. The Central Control module (the central control system)
2. The Operational /Input Module which involves receive/feedback instructions to the device. This is of three categories:
   - Initialization of authorized handsets
   - Arming/ activation of the device
   - disarming /deactivation of the device
   - The Power Module
3. Output Module: transmitted (output) response of the security device

4.2 Central Control Module

4.2.1 AT Mega 328 Micro-controller: is a single chip controller that has 8-bit architecture. It controls the input/output working of the device. It controls the data transport therein and the working principles of other systems such as the Sim card, the GPRS, GPS, etc. and operates within the range of 1.8V-5.5V. The device achieves throughput approaching 1 MIPS per MHz.

The device and its pin configuration are shown in fig.3.1 . C/C++ and assembly language is used to program the microcontroller. The flowchart of our system and its programming implementation is shown in fig. 3.11. Some of the significant characteristics of ATmega-16 are given below:

- 8 bit Microcontroller, RISC Architecture, 32 × 8 General Purpose Working Registers
- EEPROM = 512B, Internal SRAM = 1 KB, In-System Flash program memory = 16 KB
- 32 Programmable I/O Lines, Peripheral Features

4.2.2 Subscriber Identity Module (SIM): Receives the GSM/GPRS signal from the network provider (MTN) and in turn communicates to the administrator handset a Short Message Service (SMS).

4.2.3 General Packet Radio Service (GPRS): This has an antenna incorporated in it to enable the device switch to the network and communicate to the data transport.

4.2.3 Global Positioning System (GPS): gives the geographical position of the area being secured through the use of GPS satellites as part of the message sent to the authorized handset.

We have used GPS receiver module SIRF3 chip from Sparkfun. The device shown in fig.3.5. This GPS module, when powered on, waits for the signal from at least 3 of the orbiting satellites in the space. Upon reception of signals successfully, it uses trilateration process to compute its coordinates. Some of the significant characteristics of SIRF3 chip are given below:

- 20 Channel Receiver with Built-in antenna, Sensitivity = -159dBm,

  Accuracy = 5m, Baud Rate = 4800
- Power = 44mA, DC operation = 4.5-6.5, NMEA 0183 and SiRF binary

  protocols ($GPRMC)
- Hot Start = 1 seconds, Warm Start = 38 seconds, Cold Start = 42 seconds

4.3. **Operational/Input Module**

4.3.1 Initialization of authorized handsets

For the administrator or any other authorized personnel to communicate with and be recognized by the device, a procedure has to be followed. This procedure is called initialization.

Below is the process of initializing the authorized administrator handset and other handsets:

- Initialize the device by sending “Begin+ Password”
- The device will reply “Begin Ok|”
- To create authorization for the authorized personnel (admin), the device phone number is called up to ten times with the authorized personnel phone number, the administrator number is automatically registered as the authorized administrator number.

Note: the system can accept five to ten administrators.

4.2.2 Arming /Activating the Device

The device is armed through the activation code written and sent to it from the authorized administrator handset. The SIM card in the device receives the information and communicates to the micro-controller which in turn sends signals to the respective sensors connected in parallel and mounted at the doors and windows of the secured building as the case may be. These sensors are therefore activated. This is followed by an alarm sound.

When these happens, the micro-controller sends a feed-back message to the administrator handset through the SIM card that the "device is activated". If by any chance a sensor is not closed (vis a vis door/window), the device will fail to arm.

Below is the activation code for the arming of the device from the administrator.

- Send "arm xxxxxx" from the administrator handset to the device
- The device will reply "device armed"

4.2.3 Disarming/Deactivating the Device

The device is disarmed through the deactivation code written and sent to it from the authorized administrator handset. The sim card in the device receives the information and communicates to the micro-controller which in turn sends signals to the respective sensors connected in parallel and mounted at the doors and windows of the secured building as the case may be. These sensors are therefore deactivated.

When these happen, the micro-controller sends a feed-back message to the admin handset through the sim card that the device is deactivated. This is also followed by an alarm sound.

Below is the deactivation code for the disarming of the device from the administrator.

- Send "disarm xxxxxx" from the admin handset to the device
- The device will reply "device disarmed"

5. Design Calculations

5.2 Power Module

5.2.1 Battery

The power source to the device is of two types

- The alternating current (AC) power supply
- The direct current (DC) from 12V rechargeable battery

The 240V AC supply is converted to 14V DC by the power converter pack. This is used to charge the 12V DC battery

The power rating of the device is 350mAhr which is the consumption rate. From the above rating, the number of hours the battery can sustain the system in the absence of an AC supply is thus calculated.

$1hr = 350mAhr$ (1)

$1hr = 350*10^{-3}Ahr = 0.35Ahr$ (2)

$1hr = 0.35A$ (3)

But the battery current = 20A (4)

Therefore, 20A = 20*1/0.35 = 57.142hrs (5)

But 24hrs =1day (6)

57.142hrs = 57.142*1/24 =2days 10hrs (7)

The battery can sustain the system in the absence of an AC supply for 2days 10hrs.

DESIGN ANALYSIS

This design consumes minimal power for its workability.

Power . P=I×V.

Where I= Current

V= Voltage

Therefore P=800mAh, which is = 800×10^{-3}Ahr

=0.8A

Voltage= 12V

So P=0.8×12 =9.6W

Power=9.6W.

The module configuration gives:

Network	GSM/GPRS
SIM Card	MTN
Band	850/900/1800/1900Mhz
GSM/GPRS Module	SIM900B
GPS Module	SIRF3 chip
GPS Sensitivity	-159dBm
GPS Accuracy	5m
GPS Start time	
Cold status	45s
Warm status	35s

Hot status	1s
Storage Temp.	-40°C to +85°C
Operation Temp.	-20°C to +65°C
Humidity	5%--95% non-condensing.

6. Societal and Economic Benefits.

6.1 Societal Benefits

- **Enhanced Security and Safety**

The device helps protect homes, offices, schools, and public spaces from unauthorized entry, reducing cases of burglary and vandalism.

- **Improved Public Confidence**

With reliable intrusion detection systems, people feel safer in their homes and workplaces, promoting a sense of peace and community stability.

- **Crime Deterrence**

Visible or well-known security systems discourage potential intruders or criminals from attempting unlawful acts.

- **Emergency Response Support**

Many intruder detection systems can be integrated with emergency services, enabling quicker police or security intervention in case of a breach.

- **Protection of Lives and Property**

By alerting owners or security personnel early, these devices help prevent loss of life or damage to valuable assets.

- **Technological Awareness and Adoption**

Promotes a culture of embracing smart and digital security solutions, especially in developing societies where security technology is still emerging.

Economic Benefits

- **Reduction in Economic Losses from Theft**

Preventing intrusion directly saves individuals, businesses, and institutions from the financial burden of theft, property damage, or loss of critical assets.

- **Lower Insurance Premiums**

Many insurance companies offer reduced premiums for properties equipped with modern security systems, saving owners money over time.

- **Job Creation and Entrepreneurship**

The design, installation, maintenance, and monitoring of intruder detection devices create skilled and semi-skilled job opportunities in the tech and security sectors.

- **Boost to Local Manufacturing and Innovation**

Developing and producing such devices locally encourages innovation, supports local industries, and reduces dependence on imported security technologies.

- **Increased Productivity**

With greater security assurance, employees and business owners can focus more on productive activities rather than worrying about security threats.

- **Support for Economic Growth:**

A secure environment encourages investment, tourism, and business expansion, which are essential drivers of economic development.

7. Budget Breakdown (Indicative, ₦)

S/N	Item	Cost (₦)
1	Power component Section	2,320,000
2	Protection and Isolation Devices	535,000
3	Power Supply and Wiring	95,000
4	Indication and Measurement	137,000
5	Detection and Control Parts	10,535,320
6	Testing & Evaluation	5,200,000
7	Personnel & Training (10)	35,027,680
	Total	53,850,000
	Contingencies 10%	5,385,000.
	Grand Total	**59,235,000.00**

Grand Total. Fifty-Nine Million, Two Hundred and Thirty-Five Thousand Naira only.

REFERENCES

[1]. Rui Azevedo Antunes, (2020). Intruder Alarm Systems: The State of the Art, International Conference on Electrical Engineering, *Journal of physics*. 3(1) 112-231

[2].Tarek S. Sobh, (2016). Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces*, 28(6), 670–694.

[3].Tchakounté, F. Hayata, F., (2017). Mobile Security and Privacy, Intrusion Detection Systems. *Security Journal*, 5(2), 78-99.

[4].Anamika Chauhan, Rajyavardhan Singh and Pratyush Jain, (2020). A Literature Review: Intrusion Detection Systems in Internet of Things. *Journal of Physics: Conference Series*, 2(1) 1518-2040

[5] Ankit Kumar Jain, (2016). Application of Intrusion Detection System in Automatic Evidence Collection using Digital Forensics, *Security Journal*, 6(1), 115–132.

[6].Clifton L. Smith, David J. Brooks, (2013). In Security Science, *Security Journal*, 25(1), 98–116.

[7].Mohamed Allsubaie, (2011). Intruder Alarm System, *Security Journal*, 2(2), 4-37

[8].Graften, David E., (2014). Introduction to Intrusion and Alarm Systems, *Journal of Physics*, 4(5), 32-87

[9]. U.S. Homeland Security, (2004). Intrusion Detection Sensors, Retrieved from System Assessment and Validation for emergency Responds (SAVER) website: https://www.rkb.us/saver

[10].Home Security Guru. 2012. Introduction to Home Security Systems: Alarms and Sensors. Available:http://www.homesecurityguru.com/introduction-to-home-security-systems-alarms-and-sensors.

[11].Arafat, H. (2001). A new model for monitoring intrusion based on Petri Nets. Information Management and Computer Security 9(4):175-182.

[12].Chan, P. and Wei, V., (2002). Preemptive distributed intrusion detection using mobile agents. Paper presented at IEEE International Workshop on Enabling Technologies, June, Carnegie Mellon University, Petersburge, P.A

[13].Obbo Aggrey Mbarara, (2009). An Intrusion Detection System for Academic Institutions Article CITATION 1 READS 5,639 1 author: https://www.researchgate.net/publication/255670538. University of Science & Technology

Research Team and Expertise

1. **Engr. Dr. Icheke Linus Ejike** - Principal Investigator, is a seasoned Electrical Electronics Engineer with over Twenty-Fives work experience with many publications to his credit. Presently a Director and Head of Manufacturing Services at the National Engineering Design Development Institute (NEDDI), Nnewi.
2. **Engr. Chukwu Nelson Nnaemeka .** Co-Principal Investigator. He is an Electrical Electronic Engineer that has good experience in Electronics and has many publications and works to his credit.
3. **Mr. Jacob Koburu.** Head, Research and Development at the National Engineering Design Development Institute (NEDDI), Nnewi.
4. **Mr. Stanley Noah Tams.** Co-Researcher Seasoned Data analyst for Optimization of Systems and minimization of false positives. Data Engineer, Proficient in cloud devops and cloud storage .
5. Mr. Mafiana Edward. Co-Researcher, Assistant Chief Scientific Officer at the National Engineering Design development Institute, Nnewi