# **PROJECT REPORT**

**ON**

## **“MODERN IRRIGATION SYSTEM”**

Submitted in partial fulfilment for the award of Degree of Bachelor of Technology

in

Electronics & Communication Engineering



2018-19

**Submitted To: Submitted By:**

Mr Rajesh Bathija Pragya Nahar (15EJCEC143)

and Sanket Sharma(15EJCEC188)

Ms. Shruti Kalra Ritikesh(15EJCEC172)

**Guided By:** Madhur Gautam (15EJCEC105)

Mr. Bhoopesh Kumawat

**DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING, JAIPUR EGINEERING COLLEGE AND RESEARCH CENTRE SITAPURA, JAIPUR (Raj.)-302022**

**Acknowledgement**

**“It is not possible to prepare a project report without the assistance & encouragement of other people. This one is certainly no exception.”**

On the very outset of this report, we would like to extend our sincere & heartfelt obligation towards all the personages who have helped us in this endeavor. Without their active guidance, help, cooperation & encouragement, we could not have made headway in the project. First and foremost, we would like to express our sincere gratitude to our guide, **Mr. Bhoopesh Kumawat,** we were privileged to experience a sustained enthusiastic and involved interest from her side. This fuelled our enthusiasm even further and encouraged us to boldly step into what was a totally dark and unexplored expanse before us. She always fuelled our thoughts to think broad and out of the box. We would also like to thank HOD (ECE), **Ms. Shruti Kalra** who, instead of his busy schedule, always guided us in right direction. I would like to thank the entire staff member for motivation guidance and support. We are indebted to a number of friends and well-wishers who have extended their co-operation and help in the preparation of the project. Last but not the least, it goes without saying that we are deeply indebted to our parents for their support and their patient guidance.

**CONTENTS**

1. ABSTRACT

2. INTRODUCTION

3. LITERATURE SURVEY

4. TYPES OF RANDOM NUMBER

5. ARCHITECTURE

6. FPGA DESIGN AND PROGRAMMING

7. APPLICATIONS

8. REFERENCES

**Abstract**

The smart water irrigation system developed by our team is an adaptive plants and crops irrigation system. The purposes of our smart water irrigation system are to provide a water delivering schedule to the crops to ensure all the crops have enough water for their healthy growth, to reduce the amount of water wasted in irrigation, and to minimize the economic cost for the users. Our system takes in real time data of the water content of the plant as input argument, combines it with other parameters such as water cost schedule and precipitation on the crop field, runs the designed linear optimization system periodically and outputs the most efficient amount of water the plants need, which is translated by a specific actuation time of the water pumps. The linear optimization system, which is essentially the brain of our system, is able to make decisions for the users when to distribute water into the crops fields and how much water should be delivered. Given the number of factors to take into account and the different crop requirements to take into account for each type of plant, this problem because much too complex to solve through simple management methods and has to be supported by automated systems such as the one provided by our group. In the droughty California nowadays, utilizing our smart water irrigation system not only supports the environmental sustainability of the regional area, but also significantly lowers the expense of water usage for the farmers.

**INTRODUCTION**

The **Internet of things** (**IOT**) is the network of devices such as vehicles, and home appliances that contain electronics, software, sensors, actuators, and connectivity which allows these things to connect, interact and exchange data.

The IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally *dumb* or non-internet-enabled physical devices and everyday objects. Embedded with technology, these devices can communicate and interact over the Internet, and they can be remotely monitored and controlled.

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data. Thanks to cheap processors and wireless networks, it's possible to turn anything, from [a pill](https://www.zdnet.com/article/how-sensors-enabled-eli-lilly-to-improve-the-patient-experience/)to [an aeroplane](https://www.zdnet.com/article/ten-examples-of-iot-and-big-data-working-well-together/) to a self-driving car into part of the IoT. This adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without a human being involved, effectively merging the digital and physical worlds.

Pretty much any physical object can be transformed into an IoT device if it can be connected to the internet and controlled that way.

[A lightbulb](https://www.zdnet.com/article/building-my-own-internet-of-things-ambient-experience-one-step-at-a-time/) that can be switched on using a smartphone app is an IoT device, as is a motion sensor or a [smart thermostat](https://www.zdnet.com/article/johnson-controls-cortana-powered-thermostat-is-up-for-preorder-in-march/) in your office or a connected streetlight. An IoT device could be as fluffy as [a child's toy](https://www.zdnet.com/article/fbi-to-parents-beware-your-kids-smart-toy-could-be-a-security-risk/) or as serious as [a driverless truck](https://www.zdnet.com/article/driverless-trucks-are-coming-but-for-now-adoption-is-in-the-slow-lane/), or as complicated as a jet engine that's now filled with thousands of sensors collecting and transmitting data back to make sure it is operating efficiently. At an even bigger scale, [smart cities projects are filling entire regions with sensors](https://www.zdnet.com/article/las-vegas-announces-smart-city-plans-with-cisco/) to help us understand and control the environment.

The term IoT is mainly used for devices that wouldn't usually be generally expected to have an internet connection, and that can communicate with the network independently of human action. For this reason, a PC isn't generally considered an IoT device and neither is a smartphone -- even though the latter is crammed with sensors. A [smartwatch](https://www.zdnet.com/article/could-your-apple-watch-save-your-life-how-smartwatch-sensors-are-helping-tackle-a-dangerous-heart/" \t "_blank) or a [fitness band](https://www.zdnet.com/product/fitbit-ionic/) or other wearable device might be counted as an IoT device.

**What is the history of the Internet of Things?**

The idea of adding sensor and intelligence to basic objects was discussed throughout the 1980s and 1990s (and there are arguably some [much earlier ancestors](https://innovateuk.blog.gov.uk/2017/07/03/the-history-of-internet-of-things-iot/)), but apart from some early projects -- including an internet-connected vending machine -- progress was slow simply because the technology wasn't ready.

Processors that were cheap and power-frugal enough to be all but disposable were required before it became cost-effective to connect up billions of devices. The [adoption of RFID tags](https://www.zdnet.com/article/rfid-heralds-the-internet-of-things/) -- low-power chips that can communicate wirelessly -- solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking. The [adoption of IPv6](https://www.zdnet.com/article/finally-ipv6s-killer-app-the-internet-of-things/)-- which, among other things, should provide enough IP addresses for every device the world (or indeed this galaxy) is ever likely to need -- was also a necessary step for the IoT to scale. [Kevin Ashton](https://en.wikipedia.org/wiki/Kevin_Ashton) coined the phrase 'Internet of Things' in 1999, although it took at least another decade for the technology to catch up with the vision.

"The IoT integrates the interconnectedness of human culture -- our 'things' -- with the interconnectedness of our digital information system -- 'the internet.' That's the IoT," Ashton [told ZDNet](https://www.zdnet.com/article/if-you-want-to-succeed-you-must-fail-first-says-the-man-who-dreamt-up-the-internet-of-things/).

Adding RFID tags to [expensive pieces of equipment](https://www.zdnet.com/article/uk-hospitals-embrace-rfid/) to help track their location was one of the first IoT applications. But since then, the cost of adding sensors and an internet connection to objects has continued to fall, and experts predict that this basic functionality could one day cost as little as 10 cents, making it possible to connect nearly everything to the internet.

The IoT was initially most interesting to business and manufacturing, where its application is sometimes known as machine-to-machine (M2M), but the emphasis is now on filling our homes and offices with smart devices, transforming it into something that's relevant to almost everyone. Early suggestions for internet-connected devices included 'blogjects' (objects that blog and record data about themselves to the internet), ubiquitous computing (or 'ubicomp'), invisible computing, and pervasive computing. However, it was Internet of Things and IoT that stuck.

**How big is the Internet of Things?**

Big and getting bigger -- there are already more connected things than people in the world. [Analyst Gartner calculates](https://www.gartner.com/newsroom/id/3598917) that around 8.4 billion IoT devices were in use in 2017, up 31 percent from 2016, and this will likely reach 20.4 billion by 2020. Total spending on IoT endpoints and services will reach almost $2tn in 2017, with two-thirds of those devices found in China, North America and Western Europe, said Gartner.

Out of that 8.4 billion devices, more than half will be consumer products like smart TVs and smart speakers. The most-used enterprise IoT devices will be smart electric meters and commercial security cameras, according to Gartner.

**What are the benefits of the Internet of Things for business?**

The benefits of the IoT for business depend on the particular implementation, but the key is that enterprises should have access to more data about their own products and their own internal systems, and a greater ability to make changes as a result.

Manufacturers are adding sensors to the components of their products so that they can transmit back data about how they are performing. This can help companies spot when a component is likely to fail and to swap it out before it causes damage. Companies can also use the data generated by these sensors to make their systems and their supply chains more efficient, because they will have much more accurate data about what's really going on.

"With the introduction of comprehensive, real-time data collection and analysis, production systems can become dramatically more responsive," [say consultants McKinsey](https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things).

Enterprise use of the IoT can be divided into two segments: industry-specific offerings like sensors in a generating plant or real-time location devices for healthcare; and IoT devices that can be used in all industries, like smart air conditioning or security systems.

While industry-specific products will make the early running, by 2020 Gartner predicts that cross-industry devices will reach 4.4 billion units, while vertical-specific devices will amount to 3.2 billion units. Consumers purchase more devices, but businesses spend more: the analyst group said that while consumer spending on IoT devices was around $725bn last year, businesses spending on IoT hit $964bn. By 2020, business and consumer spending on IoT hardware will hit nearly $3tn.

**What is the Industrial Internet of Things?**

The Industrial Internet of Things (IIoT) or the fourth industrial revolution or Industry 4.0 are all names given to the use of IoT technology in a business setting. The concept is the same as for the consumer IoT; to use a combination of sensors, wireless networks, big data and analytics to measure and optimise industrial processes.

If introduced across an entire supply chain rather than just individual companies the impact could be even greater with just-in-time delivery of materials and the management of production from start to finish. Increasing workforce productivity or cost savings two potential aims, but the IIoT can also create new revenue streams for businesses; rather than just selling a standalone product for example like an engine, manufacturers can sell predictive maintenance of the engine too.

**What are the benefits of the Internet of Things for consumers?**

The IoT promises to make our environment -- our homes and offices and vehicles -- smarter, more measurable, and chattier. Smart speakers like [Amazon's Echo](https://www.zdnet.com/article/amazon-echo-the-four-hard-problems-amazon-had-to-solve-to-make-it-work/) and [Google Home](https://www.zdnet.com/product/google-home/) make it easier to play music, set timers, or get information. [Home security systems](https://www.zdnet.com/product/amazon-cloud-cam/) make it easier to monitor what's going on inside and outside, or to see and talk to visitors. Meanwhile, smart thermostats can help us heat our homes before we arrive back, and smart lightbulbs can make it look like we're home even when we're out.

Looking beyond the home, sensors can help us to understand how noisy or polluted our environment might be. Autonomous vehicles and smart cities could change how we build and manage our public spaces.

**What about Internet of Things security?**

Security is one the biggest issues with the IoT. These sensors are collecting in many cases extremely sensitive data -- [what you say and do in your own home](https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/), for example. Keeping that secure is vital to consumer trust, but so far the IoT's security track record has been extremely poor. Too many IoT devices give little thought to basics of security, like encrypting data in transit and at rest.

Flaws in software -- even old and well-used code -- are discovered on a regular basis, but many IoT devices lack the capability to be patched, which means they are permanently at risk. Hackers are now actively targeting IoT devices such as routers and webcams because their inherent lack of security makes them easy to compromise and [roll up into giant botnets](https://www.zdnet.com/article/satori-malware-code-given-away-for-christmas/).

Flaws have left smart home devices like refrigerators, ovens, and dishwashers open to hackers. Researchers found [100,000 webcams that could be hacked with ease](https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/), while some internet-connected smartwatches for children have been found to contain security vulnerabilities that allow hackers to track the [wearer's location, eavesdrop on conversations](https://www.zdnet.com/article/security-flaws-in-childrens-smartwatches-make-them-vulnerable-to-hackers/), or even communicate with the user.

When the cost of making smart objects becomes negligible, these problems will only become more widespread and intractable.

All of this applies in business as well, but the stakes are even higher. Connecting industrial machinery to IoT networks increases the potential risk of hackers discovering and attacking these devices. Industrial espionage or a destructive attack on critical infrastructure are both potential risks. That means businesses will need to make sure that these networks are isolated and protected with data encryption with security of sensors, gateways and other components a necessity. The current state of IoT technology makes that harder to ensure, however, as does a lack of consistent IoT security planning across organisations.

The IoT bridges the gap between the digital world and the physical world, which means that hacking into devices can have dangerous real-world consequences. Hacking into the sensors controlling the temperature in a power station could trick the operators into making a catastrophic decision; taking control of a driverless car could also end in disaster.

**LITERATURE SURVEY**

Irrigation is most important for high yield of the farm. Today, by using WSN technology it is possible to monitor and control the environmental conditions as soil moisture, temperature, wind speed, wind pressure, salinity, turbidity, humidity etc for irrigation.

[1] M.Nesa Sudha et al., 2011 proposed a TDMA based MAC protocol used for collect data such as soil moisture and temperature for optimum irrigation to save energy. MAC protocol plays an important role to reduce energy consumption. Two methods used for energy efficiency as Direct Communication method and aggregation method. Direct Communication method provides collision free transmission of data, because all the sensor nodes send data directly to the base station without the need of header node. This method is better where the base station is near but it is not optimum where the base station is far because sensor nodes consume more energy during transmission of data and if there is much data to the sensor node, sensor nodes quickly damaged. The data aggregation method is better to use rather than direct communication method. The sensor node senses the data and send to the head node. The head node collects data from the entire sensor node, performs aggregation using various aggregation techniques, and then sends data to the base station. Thus by using aggregation method overall energy consumption reduce of the network. The simulation result show that aggregation method provide better performance rather than direct communication method. It provides 10% increase in residual energy and 13% increase in throughput. Sensor nodes consume more energy while transmitting data.

[2] Man Zhang et al., 2012 analysis the temporal and spatial variability of soil moisture for the realization of variable irrigation and for improve yield in the farm. Temporal variability adopts the changes of soil moisture at the place where the sensor nodes installed and analyze soil moisture variation at different times according to season. Spatial variability analyses calculate all parameter of soil moisture as average, maximum, minimum in whole area. The temporal variability curve has drawn according to measure data. It showed that the corn was in severe water stress state during the completely monitoring period.

[3] Joaquin Gutierrez et al., 2013 proposed an irrigation system that uses photovoltaic solar panel to power system because electric power supply would be expensive. For water saving purpose, an algorithm developed with threshold value of temperature and soil moisture programmed into a micro controller gateway. The system has a full duplex communication links based on internet cellular interface using GPRS based on mobile data for graphically display and stored in a database server. The automation irrigation system consists of two components were WSU and WIU. Wireless Sensor Units (WSU) components were used for minimize power consumption because microcontroller is well suited by its lower power current in sleep mode. Wireless Information Unit (WIU) transmits soil moisture and temperature data to a web server using GPRS module. The WIU identify recorded and analyzed received temperature and soil moisture data collected by WSU. WIU functionality is bases on microcontroller that programmed to perform different task as to download the date and time information from web server and compare the temperature and soil moisture value with maximum soil moisture and minimum temperature value so that irrigated pumps activated.

[4] Sherine M.Abd El-kader et al., 2013 proposed APTEEN (Periodic Threshold oldsensitive Energy-Efficient sensor Network) protocol. APTEEN is a Hierarchical based routing protocol in which nodes have grouped into clusters. Each cluster has a head node and head node is responsible for broadcast data to the base station. APTEEN broadcast parameters attribute, which is a set of physical parameters, in which the user is interested to obtain info, Thresholds value as Hard Threshold and Soft Threshold, Schedule as TDMA schedule uses to assign slots to save energy, which provide collision free transmission. It controls the energy consumption by changing threshold values and count time. The performance of proposed protocol is better than LEACH on average 79% and by LEACH-C on average 112%.

[5] Anuj Nayak et al., 2014 describe that sensor nodes batteries are charged by using harnessing wind energy. A routing algorithm named DEHAR is proposed to extend overall batteries power. The proposed method is efficient where the amount of sensor nodes very low because of latency experienced due to synchronous sleep scheduling. A small band belt used to harness wind energy to sensor nodes. Wind belt is aero elastic flutter, which is capable for harnessing wind energy. Harnessing wind energy is a renewable energy source. However, the main problem using harnessing wind energy is the unreliability as the power of the wind is not permanent.

[6] Yunseop Kim et al. represents real time monitoring and control of variable rate irrigation controller. The sensor nodes measure environmental parameter and transmit data to base station where base station process data through a user-friendly decision making program and all data commands send to irrigation control station. The Irrigation control station sends machine location using GPS to the base station.

[7] B. Balaji Bhan et al., 2014 proposed a system to develop WSN based soil moisture controllers that determine the water requirement by comparing soil moisture with predefined threshold value. An intelligent remote system consists of wireless sensor nodes and computer system in which data is transmitted to a server system from where the data accessed by individuals for decision making for automated control of irrigation for the yield productivity. Field validation tests routinely performed on different soils to measure the soil moisture, water amount in soil for efficient irrigation system. If the stored data does not match with the soilmeasured data, an interrupt sent to the pressure unit and stop irrigation automatically.

[8] Sbrine Khriji et al., 2014 describe different type of sensor nodes for real monitoring and control of irrigation system. Each node consists of TelosB mote and actuator. TelosB mote is an ultra low power wireless module for monitoring applications. Soil nodes used to measure the soil moisture weather nodes used to measure environmental parameter and actuator used for controlling the opening of valves for irrigation. The system has cost efficient and reduce the power consumptionThe experimental result shows that the plants are well irrigate and if there is any change in threshold value the system alert to farmer about the problem to take the appropriate decision.

[9] T.C. Meyer et al., 2015 represents the design of smart sprinkler system using mesh capable WSN for monitoring and control of field irrigation system. This system provides accuracy by controlling the soil moisture level between the thresholds. Sensor nodes send data to base station every time the timer variable overflows. Base station has an actuator interface to control solenoid valve using GUI. GUI provides system feedback to user and allows changing the parameter and initially setup the system. Air temperature, soil temperature and humidity greatly influence the tomato crop. Certain disease occurs in tomato crop due to high humidity and warm temperature such as gray mould and leaf mould.

[10] Ravi Kishore Kodali et al.,2015 represents the overall history of spices as black pepper, cardamom and clove in different states where these spices are cultivated and exporters of spices and the problem faced by farming community related to pest and irrigation. Therefore, WSN used to measure different soil and environmental parameter and the presence of pests among crops and provides measures value to the user to take appropriate decision to improve crop yield. MEMSIC eko nodes used for real time monitoring of parameters and control of irrigation system.

[11] Nelson Sales et al., 2015 proposed cloud based WSAN communication system, monitoring and control of a set of sensors and actuators to measure water plant needs. Cloud computing provide high storage capacity and high processing capability. The proposed architecture divided into three components such as a WSAN component, a cloud platform components and a user application component. WSAN contain three types of nodes are a sink node, a sensor node and an actuator node. Cloud computing provide attractive solution to large amount of data. In addition, the web application provides user interfaces that allow the user to visualize the location of the network nodes to access historical data.

[12] Shaik Ameer et al., 2015 describe the use of solar power for an automatic irrigation system to supply required water to the pump set. Solar module used to convert sunlight to electricity. The electricity produced from sunlight can be stored in batteries. Humidity sensors used to sense the wet and dry conditions of the soil. After sense the data, the sensor node sends signal to microcontroller and microcontroller give signals to relay which is an electrically controlled switch for on and off to turn on the motor if the soil is dry and off the motor in wet conditions.

[13] Joaquin Gutierrez et al., 2015 represents that the sensors use Smartphone to capture and process images of soils. Images can be capture to estimate the water content of the soil. The router node is used to forward collected values to the gateway that provide automatically pump the water to the crop in a field. An Android app used for connectivity such as Wi-Fi. Android app wakes up the Smartphone by using given parameters. In-built camera takes an RGB picture of the soil through an anti-reflective glass window to take estimation of wet and dry area. The mobile app enables the Wi-Fi connection of Smartphone to transmit the estimation value to the gateway via a router node for control an irrigation water pump.

[14] You-zhu et al., 2016 proposed support vector machine to forecast water consumption and genetic algorithm is used to select parameter of SVM. GA-SVM is more robust and accurate because of its strong global search capability. Experimental result shows that GA-SVM can achieve greater forecasting accuracy then ANN (Artificial Neural Network) in forecasting the water consumption used in agriculture.

[15] Jaume Cosadesur et al., 2016 proposed an algorithm using feedback mechanism that gives response about the effect of applying the schedule it generate for the crop water needs. The goal of this algorithm is to schedule irrigation according to requirements of each grove and to the variability during the season caused by weather conditions and other factors. The algorithm performs seven different tasks as firstly it measures the amount of water given each day to the farm depending on weather conditions and crop growth. It implements the installation of the water management system to manage the amount of water delivered to the crops in the farm, execute the irrigation schedule, and measure the effects of the schedule on the crop and the data collected by the sensors processed to extract meaningful information for decisionmaking. The algorithm detect an event will trigger the execution of specific procedures for that type of event and at last implement the feedback mechanism for close the loop of the algorithm. The result shows that the simple water balance gives fast response rather than feedback mechanism for weather conditions.

[16] P. Alagupandi et al. proposed a simple and cost effective smart irrigation system. The system is modeled in outdoor environment using Tiny OS based IRIS motes to measure the moisture level of the paddy field. Moisture sensors measure the soil moisture level. The system set a threshold value and if the voltage exceeds that threshold then it represents the driest soil. Proposed system has better visualization and monitoring GUI. The motor automatically switch on by pressing the button task of visualization panel. AIS work with the help of MOTEWORKS visualization tool.

[17] Anurag D et al., design a WSN to remotely monitor the agriculture parameter and automated control the irrigation and fertigation for a precision agriculture. Static routing algorithm develops to prevent the wastage of address space and using tree-based structure maintains efficient routing. When the threshold value increases, the system can be generate an automated alert message on the console about which appropriate action performed. The valves automatically open according to the value to start irrigation and fertigation according to the need.

[18] Hema N. et al., propose a technique to predict real-time local weather parameter of interpolation using Automated Weather Station. Using sparse WSN with soil moisture sensor, this paper provide error correction and accuracy about 99.59% for real time interpolated data. This system provide past, present predict and future predict using nearby ASW data and control the irrigation in conditions like rainfall. For irrigation control, soil moisture and AWS data used and for error correction, interpolated data is comparing with soil moisture data.

[19] Bhushan G. Jagyasi et al., proposed agro- adversary system which provide an event based querying modeling which helps to query the history of events and their linkage in spatialtemporal dimensions. mKRISHI mobile phone application can be used by farmers to raise a query using text, voice, picture and video. All the information stored in the form of events in EventBase. In mKRISHI architecture various events defined such as sensor based events, an event occur when any parameter observed by a sensor is abnormally high or low, any query made by farmer is an event and responses of experts o the query is an another event. Many actions like irrigation performed by the farmer also an event and many other events occur. The event-based approach provides past experience to improve decision-making. This approach provides the history of agriculture experience to agricultural experts, to improve responses of the farmer’s query. For the mKRISHI agro-advisor system the model provides an experience sharing platform between different experts.

**SENSORS**

Sensor Is an input device which provides an output (signal) with respect to a specific physical quantity (input). Another unique definition of a Sensor is as follows: It is a device that converts signals from one energy domain to electrical domain

TYPES OF SENSORS USED:

1. DHT11

DHT11 Temperature & Humidity Sensor features a temperature & humidity sensor complex with a calibrated digital signal output. By using the exclusive digital-signal-acquisition technique and temperature & humidity sensing technology, it ensures high reliability and excellent long-term stability. This sensor includes a resistive-type humidity measurement component and an NTC temperature measurement component, and connects to a highperformance 8-bit microcontroller, offering excellent quality, fast response, anti-interference ability and cost-effectiveness. DHT11 Temperature & Humidity Sensor features a temperature & humidity sensor complex with a calibrated digital signal output. By using the exclusive digital-signal-acquisition technique and temperature & humidity sensing technology, it ensures high reliability and excellent long-term stability. This sensor includes a resistive-type humidity measurement component and an NTC temperature measurement component, and connects to a highperformance 8-bit microcontroller, offering excellent quality, fast response, anti-interference ability and cost-effectiveness. Power and Pin DHT11’s power supply is 3-5.5V DC. When power is supplied to the sensor, do not send any instruction to the sensor in within one second in order to pass the unstable status. One capacitor valued 100nF can be added between VDD and GND for power filtering. Communication Process: Serial Interface (Single-Wire Two-Way) Single-bus data format is used for communication and synchronization between MCU and DHT11 sensor. One communication process is about 4ms. Data consists of decimal and integral parts. A complete data transmission is 40bit, and the sensor sends higher data bit first. Data format: 8bit integral RH data + 8bit decimal RH data + 8bit integral T data + 8bit decimal T data + 8bit check sum. If the data transmission is right, the check-sum should be the last 8bit of "8bit integral RH data + 8bit decimal RH data + 8bit integral T data + 8bit decimal T data".

DHT Responses to MCU (Figure 3, above) Once DHT detects the start signal, it will send out a low-voltage-level response signal, which lasts 80us. Then the programme of DHT sets Data Single-bus voltage level from low to high and keeps it for 80us for DHT’s preparation for sending data. When DATA Single-Bus is at the low voltage level, this means that DHT is sending the response signal. Once DHT sent out the response signal, it pulls up voltage and keeps it for 80us and prepares for data transmission. When DHT is sending data to MCU, every bit of data begins with the 50us low-voltage-level and the length of the following high-voltage-level signal determines whether data bit is "0" or "1" (see Figures 4 and 5 below). Figure 4 Data "0" Indication Page | 8 Figure 5 Data "1" Indication If the response signal from DHT is always at high-voltage-level, it suggests that DHT is not responding properly and please check the connection. When the last bit data is transmitted, DHT11 pulls down the voltage level and keeps it for 50us. Then the Single-Bus voltage will be pulled up by the resistor to set it back to the free status.

Attentions of application

(1) Operating conditions Applying the DHT11 sensor beyond its working range stated in this datasheet can result in 3%RH signal shift/discrepancy. The DHT11 sensor can recover to the calibrated status gradually when it gets back to the normal operating condition and works within its range. Please refer to (3) of Conditions Minimum Typical Maximum Power Supply DC 3V 5V 5.5V Current Supply Measuring 0.5mA 2.5mA Average 0.2mA 1mA Standby 100uA 150uA Sampling period Second 1 Page | 9 this sec on to accelerate its recovery. Please be aware that opera ng the DHT11 sensor in the non-normal working condi ons will accelerate sensor’s aging process.

(2) Attention to chemical materials Vapor from chemical materials may interfere with DHT’s sensi ve-elements and debase its sensi vity. A high degree of chemical contamina on can permanently damage the sensor.

(3) Restoration process when (1) & (2) happen Step one: Keep the DHT sensor at the condi on of Temperature 50~60Celsius, humidity 70%RH for 5 hours.

(4) Temperature ect Rela ve humidity largely depends on temperature. Although temperature compensa on technology is used to ensure accurate measurement of RH, it is s strongly advised to keep the humidity and temperature sensors working under the same temperature. DHT11 should be mounted at the place as far as possible from parts that may generate heat.

(5) Ligh t ect Long me exposure to strong sunlight and ultraviolet may debase DHT’s performance.

(6) Connection wires The quality of connec on wires will affect the quality and distance of communica on and high quality shielding-wire is recommended.

(7) Other attentions \* Welding temperature should be bellow 260Celsius and contact should take less than 10 seconds. \* Avoid using the sensor under dew condi on. \* Do not use this product in safety or emergency stop devices or any other occasion that failure of DHT11 may cause personal injury. \* Storage: Keep the sensor at temperature 10-40℃, humidity <60%RH.

1. IR

Infrared technology addresses a wide variety of wireless applications. The main areas are sensing and remote controls. In the electromagnetic spectrum, the infrared portion is divided into three regions: near infrared region, mid infrared region and far infrared region.

The wavelengths of these regions and their applications are shown below.

* Near infrared region — 700 nm to 1400 nm — IR sensors, fiber optic
* Mid infrared region — 1400 nm to 3000 nm — Heat sensing
* Far infrared region — 3000 nm to 1 mm — Thermal imaging

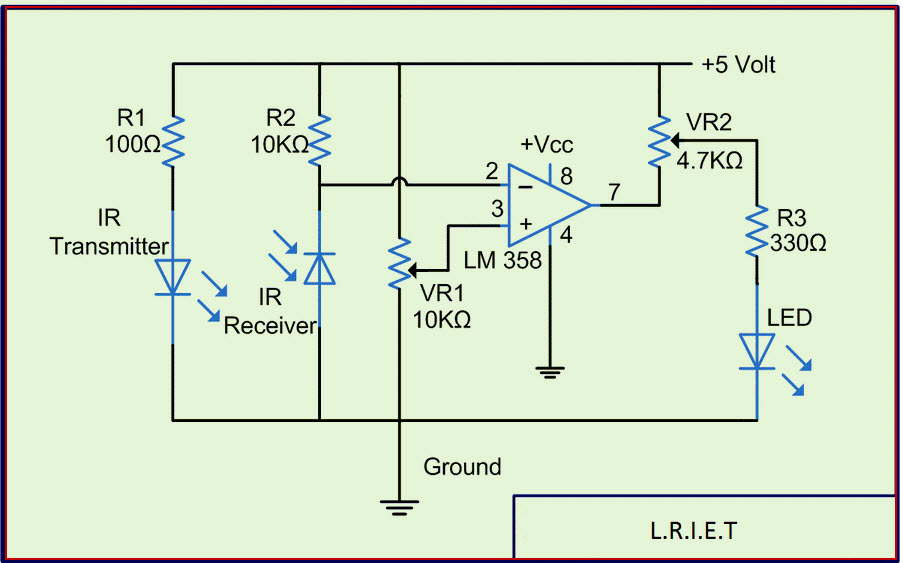
The frequency range of infrared is higher than microwave and lesser than visible light.

The basic concept of an Infrared Sensor which is used as Obstacle detector is to transmit an infrared signal, this infrared signal bounces from the surface of an object and the signal is received at the infrared receiver.

Active infrared sensors consist of two elements: infrared source and infrared detector. Infrared sources include an LED or infrared laser diode. Infrared detectors include photodiodes or phototransistors. The energy emitted by the infrared source is reflected by an object and falls on the infrared detector.

## *I*R Sensor Circuit Diagram and Working Principle

An infrared  sensor circuit is one of the basic and popular sensor module in an [electronic device](https://www.elprocus.com/basic-components-used-electronics-electrical/). This sensor is analogous to human’s visionary senses, which can be used to detect obstacles and it is one of the common applications in real time.This circuit comprises of the following components



In this project, the transmitter section includes an IR sensor, which transmits continuous IR rays to be received by an IR receiver module. An IR output terminal of the receiver varies depending upon its receiving of IR rays. Since this variation cannot be analyzed as such, therefore this output can be fed to a comparator circuit. Here an [operational amplifier](https://www.elprocus.com/op-amp-ics-pin-configuration-features-working/) (op-amp) of LM 339 is used as comparator circuit.

When the IR receiver does not receive a signal, the potential at the inverting input goes higher than that non-inverting input of the comparator IC (LM339). Thus the output of the comparator goes low, but the LED does not glow. When the IR receiver module receives signal to the potential at the inverting input goes low. Thus the output of the comparator (LM 339) goes high and the LED starts glowing. Resistor R1 (100 ), R2 (10k ) and R3 (330) are used to ensure that minimum 10 mA current passes through the IR LED Devices like Photodiode and normal LEDs respectively. Resistor VR2 (preset=5k ) is used to adjust the output terminals. Resistor VR1 (preset=10k ) is used to set the sensitivity of the circuit Diagram.

### Different Types of IR Sensors and Their Applications

The speed sensor is used for synchronizing the speed of multiple motors. The [temperature sensor](https://www.elprocus.com/temperature-sensors-applications/) is used for industrial temperature control. [PIR sensor](https://www.elprocus.com/pir-sensor-basics-applications/) is used for automatic door opening system and  [Ultrasonic sensor](https://www.elprocus.com/motion-detector-circuit-with-working-description-and-its-applications/" \t "_blank) are used for distance measurement.

### IR Sensor Applications

IR sensors are used in various [Sensor based projects](https://www.elprocus.com/sensor-based-electronics-projects/) and also in various electronic devices which measures the temperature that are discussed in the below.

#### Radiation Thermometers

IR sensors are used in radiation thermometers to measure the temperature depend upon the temperature and the material of the object and these thermometers have some of the following features

* Measurement without direct contact with the object
* Faster response
* Easy pattern measurements

#### Flame Monitors

These types of devices are used for detecting the light emitted from the flames and to monitor how the flames are burning. The Light emitted from flames extend from UV to IR region types. PbS, PbSe, Two-color detector, pyro electric detector are some of the commonly employed detector used in flame monitors.

#### Moisture Analyzers

Moisture analyzers use wavelengths which are absorbed by the moisture in the IR region. Objects are irradiated with light having these wavelengths(1.1 µm, 1.4 µm, 1.9 µm, and 2.7µm) and also with reference wavelengths. The Lights reflected from the objects depend upon the moisture content and is detected by analyzer to measure moisture (ratio of reflected light at these wavelengths to the reflected light at reference wavelength). In GaAs PIN photodiodes, Pbs photoconductive detectors are employed in moisture analyzer circuits.

#### Gas Analyzers

IR sensors are used in gas analyzers which use absorption characteristics of gases in the IR region. Two types of methods are used to measure the density of gas such as dispersive and non dispersive.

1. ULTRASONIC SENSOR

As the name indicates, ultrasonic sensors measure distance by using ultrasonic waves.  
The sensor head emits an ultrasonic wave and receives the wave reflected back from the target. Ultrasonic Sensors measure the distance to the target by measuring the time between the emission and reception.

ultrasonic sensor uses a single ultrasonic element for both emission and reception. In a reflective model ultrasonic sensor, a single oscillator emits and receives ultrasonic waves alternately. This enables miniaturization of the sensor head. The distance can be calculated with the following formula:

### Distance L = 1/2 × T × C

where L is the distance, T is the time between the emission and reception, and C is the sonic speed. (The value is multiplied by 1/2 because T is the time for go-and-return distance.)

### Ultrasonic Sensor Pin ****Configuration****

|  |  |  |
| --- | --- | --- |
| **Pin Number** | **Pin Name** | **Description** |
| 1 | Vcc | The Vcc pin powers the sensor, typically with +5V |
| 2 | Trigger | Trigger pin is an Input pin. This pin has to be kept high for 10us to initialize measurement by sending US wave. |
| 3 | Echo | Echo pin is an Output pin. This pin goes high for a period of time which will be equal to the time taken for the US wave to return back to the sensor. |
| 4 | Ground | This pin is connected to the Ground of the system |

### HC-SR04 Sensor Features

* Operating voltage: +5V
* Theoretical  Measuring Distance: 2cm to 450cm
* Practical Measuring Distance: 2cm to 80cm
* Accuracy: 3mm
* Measuring angle covered: <15°
* Operating Current: <15mA
* Operating Frequency: 40Hz

### Equivalent distance measuring Sensors

US transmitter Receiver pair, IR sensor module, IR sensor pair, IR Analog distance sensor,

### HC-SR04 Ultrasonic Sensor - Working

As shown above the **HC-SR04 Ultrasonic (US) sensor** is a 4 pin module, whose pin names are Vcc, Trigger, Echo and Ground respectively. This sensor is a very popular sensor used in many applications where measuring distance or sensing objects are required. The module has two eyes like projects in the front which forms the Ultrasonic transmitter and Receiver. The sensor works with the simple high school formula that

**Distance = Speed × Time**

The Ultrasonic transmitter transmits an ultrasonic wave, this wave travels in air and when it gets objected by any material it gets reflected back toward the sensor this reflected wave is observed by the Ultrasonic receiver module as shown in the picture below

Now, to calculate the distance using the above formulae, we should know the Speed and time. Since we are using the Ultrasonic wave we know the universal speed of US wave at room conditions which is 330m/s. The circuitry inbuilt on the module will calculate the time taken for the US wave to come back and turns on the echo pin high for that same particular amount of time, this way we can also know the time taken. Now simply calculate the distance using a microcontroller or microprocessor.

**HC-SR04 distance sensor** is commonly used with both microcontroller and microprocessor platforms like Arduino, ARM, PIC, Raspberry Pie etc. The following guide is universally since it has to be followed irrespective of the type of computational device used.

  Power the Sensor using a regulated +5V through the Vcc ad Ground pins of the sensor. The current consumed by the sensor is less than 15mA and hence can be directly powered by the on board 5V pins (If available). The Trigger and the Echo pins are both I/O pins and hence they can be connected to I/O pins of the microcontroller. To start the measurement, the trigger pin has to be made high for 10uS and then turned off. This action will trigger an ultrasonic wave at frequency of 40Hz from the transmitter and the receiver will wait for the wave to return. Once the wave is returned after it getting reflected by any object the Echo pin goes high for a particular amount of time which will be equal to the time taken for the wave to return back to the sensor.

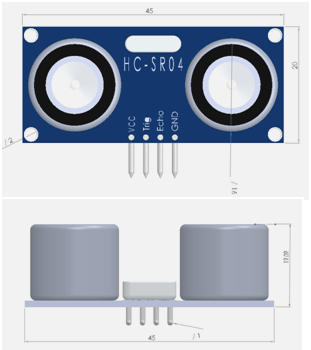
The amount of time during which the Echo pin stays high is measured by the MCU/MPU a

The amount of time during which the Echo pin stays high is measured by the MCU/MPU as it gives the information about the time taken for the wave to return back to the Sensor. Using this information the distance is measured as explained in the above heading.

### Applications

* Used to avoid and detect obstacles with robots like biped robot, obstacle avoider robot, path finding robot etc.
* Used to measure the distance within a wide range of 2cm to 400cm
* Can be used to map the objects surrounding the sensor by rotating it
* Depth of certain places like wells, pits etc can be measured since the waves can penetrate through water

### 2D model of the component

****

1. RAIN SENSOR

The rain sensor module is an easy tool for rain detection. It can be used as a switch when raindrop falls through the raining board and also for measuring rainfall intensity. The module features, a rain board and the control board that is separate for more convenience, power indicator LED and an adjustable sensitivity though a potentiometer. The analog output is used in detection of drops in the amount of rainfall. Connected to 5V power supply, the LED will turn on when induction board has no rain drop, and DO output is high. When dropping a little amount water, DO output is low, the switch indicator will turn on. Brush off the water droplets, and when restored to the initial state, outputs high level.

Specifications

Adopts high quality of RF-04 double sided material.• Area: 5cm x 4cm nickel plate on side,• Anti-oxidation, anti-conductivity, with long use time;• Comparator output signal clean waveform is good, driving ability, over 15mA;• Potentiometer adjust the sensitivity;• Working voltage 5V;• Output format: Digital switching output (0 and 1) and analog voltage output AO;• With bolt holes for easy installation;• Small board PCB size: 3.2cm x 1.4cm;• Uses a wide voltage LM393 comparator• Pin Configuration 1. VCC: 5V DC 2. GND: ground 3.

1. MOISTURE SENSOR

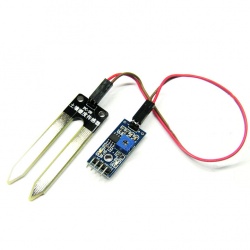
* The **Moisture sensor** is used to measure the water content(moisture) of soil.when the soil is having water shortage,the module output is at high level, else the output is at low level.This sensor reminds the user to water their plants and also monitors the moisture content of soil.It has been widely used in agriculture,land irrigation and botanical gardening.
* Working Voltage:**5V**
* Working Current:**<20mA**
* Interface type:**Analog**
* Working Temperature:**10°C~30°C**
* There is a 2 cm zone of influence with respect to the flat surface of the sensor, but it has little or no sensitivity at the extreme edges.The Soil Moisture Sensor is used to measure the loss of moisture over time due to evaporation and plant uptake,evaluate optimum soil moisture contents for various species of plants,monitor soil moisture content to control irrigation in greenhouses and enhance bottle biology experiments.

## **download (1).jpg**

## **ULTRASONIC SENSOR**



**INFRARED SENSOR**

****

**MOISTURE SENSOR**

## **download.png**

## **RAINDROP SENSOR**



RPI ZERO W

## **TYPES OF RANDOM NUMERS**

## **True random numbers**

The need for true random numbers is needed in many applications, this has resulted in specialized hardware being built to produce a sequence of true random numbers instead of using a software method of producing random like number sequences.

There are many natural occurring events that exhibit true random behaviour. The world of quantum physics is characterized by purely random events as well as natural decay of radioactive material are just two examples of many, truly random events. These processes, although very good sources of random data, are not practical for many computing needs. There are however more practical ways of generating true random data sequences.

 One such method is by allowing a current to flow thought a resistor. Thermal agitation of free electrons causes small voltage fluctuations. It is this random noise that circuit designers try to minimise as much as possible*[Ghausi]*. If the amplitude of the voltage fluctuations across the resistor are made large enough to use practically, a true random number generator could be constructed *[Connor]*. This can be used, together with a comparator and a microprocessor to feed a sequence of “random” bits into the PC via the COM port. This is explained in detail in Chapter 4. This sequence of bits will of course have to be tested statistically to make sure that it does actually exhibit random properties. Another possible way to generate random data is to connect an antenna to an amplifier and measure the noise picked up. This is very similar to measuring the noise from a resistor, except that the sequence collected will have to be analyzed using Fourier analysis to check that there are no dominating frequencies in the data. This does however have its drawbacks, if the antenna is placed next to any device emitting an electro-magnetic field (which all electronic devices do), the data collected will be skewed and hence non-random. To try and reduce this effect, one could pass the random bits through a hashing function (MD5 or SHA). Summing up all that has been said above; if a set of uniformly distributed numbers is selected in a truly random manner, then each possible number has an equal probability of being selected.

## **Pseudo Random Numbers**

Obtaining random numbers from a physical source can often be impractical in many applications such as portable web applications. This led to the development of a mathematical method to create a sequence of numbers that could mimic true random numbers. Because a mathematical source is not a true source of random numbers, it is called a pseudo random number. This is due to the mathematical function being completely deterministic and hence, non-random. In the 1940’s von Neuman developed the first mathematical algorithm to create random numbers. This was known as the middle-square method, and while it could produce seemingly random number sequences, it quickly proved to be a very poor source of pseudo random numbers. These methods of producing pseudo random numbers are known as pseudo random number generators or PRNG for short.

A key feature of a PRNG is that it should be chaotic. Even though they are completely deterministic mathematical functions, their output must be very erratic and non-predictable to an onlooker. Chaitin *[Chaitin]* and Kolmogorov have shown that to produce a random sequence by means of a computer program, then the program has to be approximately the same length as the random sequence itself. This therefore leads to the fact that a true random sequence can never be produced by a computer program.  This is because a true random sequence of numbers can be infinite in length and never repeat themselves after a set period. PRNGs however do begin to repeat themselves after a set period which leads to the fact that infinite space is needed if one wants a computer program to produce a true random data sequence.

Hardware random number generators are commercially available which in some applications are essential. But in many applications issues due to availability, performance and especially portability, make the use of a hardware random number generator an impractical option. PRNGs also have the defect that in a set of uniformly distributed numbers selected by a PRNG, as is discussed above, each possible number does not have an equal probability of being selected. This is due to the process of generating pseudo random numbers is flawed by the method of using the previous result in generating the next number. Hence giving rise to its deterministic nature.

**Field Programmable Gate Array**

**A field-programmable gate array (FPGA)** is an integrated circuit created to be configured by the customer after manufacturing—hence "field-programmable". The FPGA configuration is generally defined using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC) (circuit diagrams were previously used to specify the configuration, as they were for ASICs, but this is increasingly rare). FPGAs can be used to implement any logical function that an ASIC can perform. The ability to update the functionality after shipping, partial re-configuration of the portion of the design and the low non-recurring engineering costs relative to an ASIC design, offer advantages for many applications. [16] FPGAs contain programmable logic components called "logic blocks", and a hierarchy of reconfigurable interconnects that allow the blocks to be "connected together"—somewhat like a one-chip programmable breadboard. Logic blocks can be configured to perform complex combinational functions, or merely simple logic like AND and NAND. In most FPGAs, the logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory.

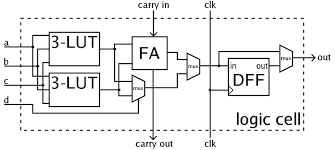
**Architecture:**

The most common FPGA architecture consists of an array of logic blocks (called Configurable Logic Block, CLB, or Logic Array Block, LAB, depending on vendor), I/O pads, and routing channels. Generally, all the routing channels have the same width (number of wires). Multiple I/O pads may fit into the height of one row or the width of one column in the array.

In general, a logic block (CLB or LAB) consists of a few logical cells. A typical cell consists of a 4-input Lookup table (LUT), a Full adder (FA) and a D-type flip-flop, as shown. The LUT are in this figure split into two 3-input LUTs. In normal mode those are combined into a 4-input LUT through the left mux. In arithmetic mode, their outputs are fed to the FA. The selection of mode is programmed into the middle mux. The output can be either synchronous or asynchronous, depending on the programming of the mux to the right, in the figure above. In practice, entire or parts of the FA are put as functions into the LUTs in order to save space.

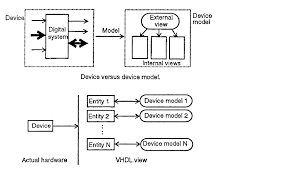
**FPGA Design and Programming**: To specify the behavior of the FPGA, the user provides a hardware description language (HDL) or a schematic design. The HDL form is more suited to work with large structures because it's possible to just specify them numerically rather than having to draw every piece. However, schematic entry can allow for easier imagination of a design. Then, using an electronic design automation tool, a technology-mapped netlist is generated. The netlist can then be fitted to the actual FPGA architecture using a process called place-androute, usually performed by the FPGA company's proprietary place-and-route software. The user will validate the map, place and route results via timing analysis, simulation, and other verification methods. Once the design and validation process is complete, the binary file generated is used to reconfigure the FPGA. The most common HDLs are VHDL and Verilog. Though these two languages are similar but we prefer VHDL for programming because of its widely in use.

**VHDL** is an acronym for VHSlC Hardware Description Language (VHSIC is an acronym for Very High Speed Integrated Circuits). It is a hardware description language that can be used to model a digital system at many levels of abstraction ranging from the algorithmic level to the gate level. The complexity of the digital system being modeled could vary from that of a simple gate to a complete digital electronic system, or anything in between. The digital system can also be described hierarchically. Timing can also be explicitly modeled in the same description. The language not only defines the syntax but also defines very clear simulation semantics for each language construct. Therefore, models written in this language can be verified using a VHDL simulator. It is a strongly typed language and is often verbose to write. It inherits many of its features, especially the sequential language part, from the ADA programming language. Because VHDL provides an extensive range of modeling capabilities, it is often difficult to understand.



**Hardware Abstraction**

VHDL is used to describe a model for a digital hardware device. This model specifies the external view of the device and one or more internal views. The internal view of the device specifies the functionality or structure, while the external view specifies the interface of the device through which it communicates with the other models in its environment. Figure shows the hardware device and the corresponding software model.



**FPGA Design and Programming**

To specify the behavior of the FPGA, the user provides a hardware description language (HDL) or a schematic design. The HDL form is more suited to work with large structures because it's possible to just specify them numerically rather than having to draw every piece. However, schematic entry can allow for easier imagination of a design. Then, using an electronic design automation tool, a technology-mapped netlist is generated. The netlist can then be fitted to the actual FPGA architecture using a process called place-androute, usually performed by the FPGA company's proprietary place-and-route software. The user will validate the map, place and route results via timing analysis, simulation, and other verification methods. Once the design and validation process is complete, the binary file generated is used to reconfigure the FPGA. The most common HDLs are VHDL and Verilog. Though these two languages are similar but we prefer VHDL for programming because of its widely in use.

**Process Statement**

A process statement contains sequential statements that describe the functionality of a portion of an entity in sequential terms. The syntax of a process statement is [17] [ process-label: ] process [ ( sensitivity-list ) ] [process-item-declarations] begin sequential-statements; these are -> variable-assignment-statement signal-assignment-statement wait-statement loop-statement null-statement exit-statement.

**Code**

library IEEE;

use IEEE.STD\_LOGIC\_1164.ALL; entity rng is generic ( wd : integer := 32 );

port ( clk : in std\_logic; random\_num : out std\_logic\_vector (wd-1 downto 0) --output vector );

end rng; architecture Behavioral of rng is begin process(clk) variable rand\_temp : std\_logic\_vector(wd-1 downto 0):=(wd1 => '1',others => '0');

variable temp : std\_logic := '0';

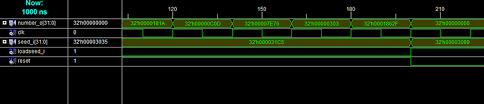
begin if(rising\_edge(clk)) then temp := rand\_temp(wd-1) xor rand\_temp(wd-2);

rand\_temp(wd-1 downto 1) := rand\_temp(wd-2 downto 0);

rand\_temp(0) := temp; end if; Page | 29 random\_num <= rand\_temp;

end process;

end rng;



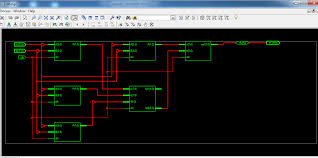


Fig :random number generator and rtl schematic

**APPLICATIONS OF RNG**

### Cryptography

This area of computer science is probably the most critical when it comes to the need of good random number sources. A poor source of predictable pseudo random numbers would lead to the break down of the entire cryptographic process, leaving ones encrypted data open to any malicious activity. In cryptographic terms, it is important that the PRNG produces pseudo-random numbers that are statistically indistinguishable from true random numbers. In many other applications it is not too critical if it is found out exactly how a sequence was generated. But in cryptography special care must be taken at all stages of the sequence generation process.

Issues such a seeding, reseeding, entropy and generation process must all be considered and dealt with *[Kelsey]*. In the design of the Yarrow cryptographic PRNG all these issues were dealt with resulting in an extremely safe cryptographic PRNG. Yarrow uses a very “intelligent” system for generating seeds whereby it has a system monitor that captures data with known levels of entropy. This can include keyboard events, mouse movement events and even “into using the random fluctuations in hard-disk access time caused by turbulence inside the enclosure” *[Ferguson]*.

Another PRNG that has very good cryptographic properties is the Blum-Blum-Shub generator. This generator is very similar to the LCG PRNG, except it is of the form:

Text Box: xn+1 = xn2 mod M  

**Equation – Blum-Blum-Shub**

where M is the product of two large distinct prime numbers. The output is the least significant bit (or parity) of xn+1. What makes this PRNG so cryptographically strong is the fact that its parameters are not polynomial time computable. It has been shown that trying to crack this PRNG is as hard as trying to break RSA public-key encryption *[Blum]*.

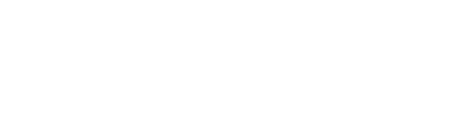
In 1995 the security offered in the Netscape Navigator web browser was compromised. The success of this attack was due to the fact that it was aimed at the PRNG *[Schneier]*. More specifically it was aimed at the algorithm used to seed the PRNG. The algorithm implemented to create a seed value depended on three values, namely: the time of day, the process ID, and the parent process ID. These values can be easily predicted by an adversary. Once the seed was known, assuming the attacker knew the PRNG algorithm (which he/she did), the internal state of the PRNG could be recreated making the attack fairly trivial *[Dobb’s]*.

### Network Security

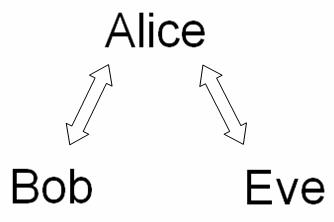
Over the recent few years network security has become one of the most important areas of focus of a network administrators. If the network security can be broken, an intruder can obtain sensitive information or perform malicious activities. The implementation of Transmission Control Protocol (TCP) requires that an Initial Sequence Number (ISN) be selected at the beginning of every new TCP connection. The ISN must also be unique as to avoid an overlap of connections which would result in packets of data being reassembled in the wrong order *[CIAC]*. During a connection, if multiple packets are sent, the original ISN is incremented sequentially.

The original implementation of TCP used a simple linear method of generating ISN’s. A 32 bit clock was used which was incremented every four microseconds. The value of this clock was then used as an ISN when needed. This led to ISN’s to begin repeating after only 4.55 hours *[RFC 793]*. A security flaw was discovered in the TCP/IP protocol suite, initially using 4.2BSD Unix, that if an intruder could cause a packet to be dropped, sent by a host machine to a connecting machine and the intruder could forge a return packet in which the correct ISN is guessed, the intruder could gain control of the connection and data may be injected *[Morris]*.

A typical TCP connection is created using the three way handshake. Below shows how the three way handshake normally should take place. Following this, data transmission can take place.



C, the client, selects an ISN and sends it to S, the server. S receives this, and selects its own ISN and sends it together with an acknowledgement to C. C then sends an acknowledgement of this back to S, after which data transmission can take place.



**Figure  – Example of ISN attack**

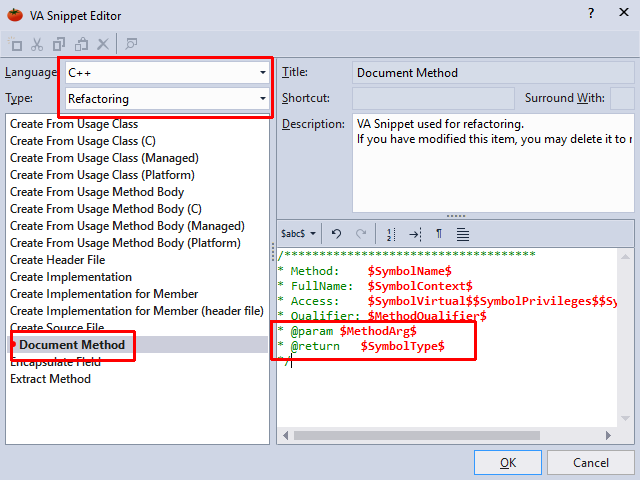
In a connection between Alice, the client and Bob, the trusted host packets will only be accepted if, amongst other reasons, they have the correct ISN. If an intruder, Eve (eavesdropper), forges a packet so that Alice “sees” it as coming from Bob and is able to predict the correct ISNS, it is possible for Eve to send any data in the packet with the possibility that Alice executes code that was in the malicious packet. This type of attack is known as spoofing. Together with this discovered flaw and the original implementation of the TCP ISN generator, an attacker could very quickly and easily predict the next ISN and successfully launch an attack.

In 2001 Michael Zalewski released a paper highlighting obvious flaws in the then current operating systems’ TCP/IP implementation. In this paper a method of plotting the ISNs was described which allowed one to visualise the ISNs. This method resulted in attractors forming which would allow any hacker to exploit this fact and obtain control of the TCP/IP connection with relevant ease *[Michael]*. The first method of plotting sequences of numbers in a Phase Space, described in this paper is the method that was used in Michael Zalewski’s paper.

Another type of attack is the TCP reset attack. If two machines, host A and host B have an established TCP connection. Host C (a malicious host) can cause the TCP connection to be terminated by forging a packet from one host (A or B) to the other and setting the reset (RST) bit. If enough bandwidth is available to C, then it is easy enough to try all possible ISNs or a smaller subset if the generation algorithm is known. But in most cases bandwidth is limited resulting in the fact that host C must also be able to predict the correct ISN that is being used in the connection for the forged packet to be accepted by one of the hosts. This is an easy task if host C is directly in between, and can “sniff” packets, the communicating hosts. But in most cases, host C cannot do this. So if either hosts are using a system that has predictable ISNs, host C can easily predict the ISN and terminate the connection.

It has been shown that the more random an ISN is chosen, the less likely it is for this type of attack to occur. This is because an attacker has to guess the next ISN by monitoring previous ISN’s and discover the ISN generation method. His paper shows how easy it can be to create a set of ISNs which can be used to create a spoofing set. By implementing a PRNG in the generation of ISN’s results in the prediction of ISN’s to become a lot more tedious and/or difficult.

Proposed fixes to this problem has been to use a function to generate ISN which can be of the following form:



|  |
| --- |
|  |
|  | |  | | --- | |  | |

 It is essential that the function F is not computable by an outside source, or it would allow an attacker to still predict the ISN’s. It has been recommended that the function F be some secure cryptographic hashing function that takes [localhostIP, localport, remotehost, remoteportIP] together with some random data. The inclusion of random data is to ensure that there is and element of unpredictability in the ISN. Although, when a sample of ISN’s, created according to RFC 1948, is plotted using Lattice Space, the resulting image will suggest that the ISN generator is using a completely linear ISN generator as described in RFC 793. The Phase Space and Noise Sphere will highlight the fact that the increment used between ISN’s is linear or not. This is where the need for a good PRNG is necessary and the use of a poor PRNG would make this method of cause the implementation of TCP/IP providing a false sense of security *[RFC 1948]*. It is however noted that using random increments to increase the ISN over time will not, according to the central limit theorem, introduce enough variance in the ISN’s *[CERT]*.

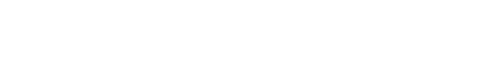
Another proposal has been to use a PRNG to generate the ISN, with no use of localhostIP, localport, remotehost and remoteportIP. The PRNG used for this method should be in accordance with RFC 1750. Although, problems can arise using a PRNG as the ISN generator. If the generator, by “chance”, happens to generate the same number in close succession, then it is possible for packets to become intermixed and the data stream to be incorrectly reassembled.

### Monte Carlo/Statistical (physical) simulations

Scientific computing has, since 1945, relied on random numbers to solve many complex problems that cannot be solved analytically. The worlds first super computer, MANIAC, used Monte Carlomethods to solve intense numerical problems for the design of the atomic bomb. The maths behind Monte Carlo is too advanced for the needs of this paper. However, the driving force behind Monte Carlo simulations are good random numbers. As has been said earlier, obtaining true random numbers can be a difficult affair. Hence the need for a good PRNG. The only requirement here is that the PRNG exhibits good statistical properties and that the same set of pseudo-random values can be reproduced multiple times using the same initial seed value every time (this allows for results to be validated) *[Liu]*. The integral, which is essential to many scientific problems, can be solved computationally by mean of Monte Carlo simulation.

Given:

            I = ∫Dg(x)dx, can be approximated by computational methods if we have independent and uniformly distributed [pseudo] random numbers over D using the following identity:



Now if m → infinity, then Ĭ → I. This is the basic principal behind the Monte Carlo method and more advanced methods do exist *[Liu].*

This is the basic method behind Monte Carlo, and as one can see if a poor PRNG is used (one which yields poor statistical results), the results from this simulation can be disastrous *[Buslenko]*.

An example of this can be shown by using the Monte Carlo method to find an estimate value of PI. This is done by generating random (x,y) coordinates in the range [0,1). If the point has a distance greater than one, it lies outside the quarter circle of radius one, it does not get counted. Otherwise, all other point get counted.

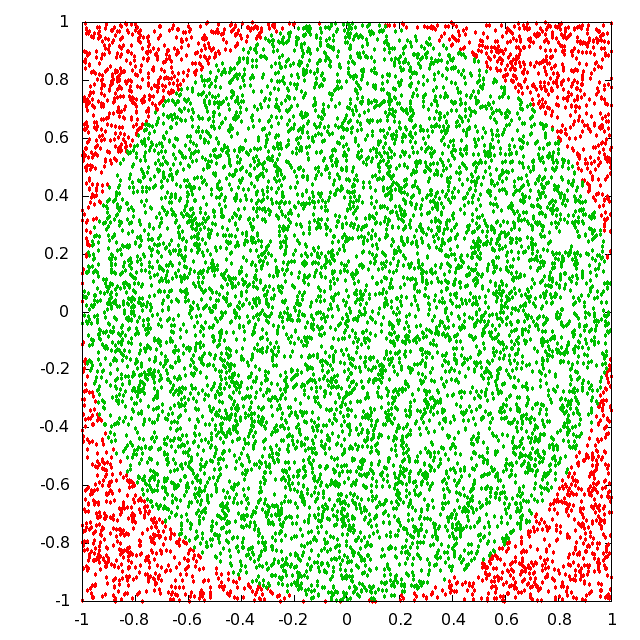
            Now:    total points = n

                        Points inside circle = x

                        Estimated PI = 4 \* x / n

This is a crude example, but it does show how poor pseudo random numbers can lead to a breakdown in a physicists experiments.

  Below figure shows how Pi can be estimated using this method.



**Figure  – Monte Carlo Estimate of Pi**

**REFERENCES**

[1] M. Nesa Sudha, M.L. Valarmathi, Anni Susan Babu, Energy efficient data transmission in automatic irrigation system using wireless sensor networks, Computers and Electronics in Agriculture, Volume 78, Issue 2, September 2011, Pages 215-221, ISSN 0168-1699, http://dx.doi.org/10.1016/j.compag.2011.07.009.

[2] Man Zhang, Minzan Li, Weizhen Wang, Chunhong Liu, Hongju Gao, Temporal and spatial variability of soil moisture based on WSN, Mathematical and Computer Modelling, Volume 58, Issues 3–4, August 2013, Pages 826- 833, ISSN 0895-7177.

[3] J. Gutiérrez, J. F. Villa-Medina, A. NietoGaribay and M. Á Porta-Gándara, "Automated Irrigation System Using a Wireless Sensor Network and GPRS Module," in IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 1, pp. 166-176, Jan. 2014.

[4] Sherine M. Abd El-kader, Basma M. Mohammad El-Basioni, Precision farming solution in Egypt using the wireless sensor network technology, Egyptian Informatics Journal, Volume 14, Issue 3, November 2013, Pages 221-233, ISSN 1110-8665.

[5] A. Nayak, G. Prakash and A. Rao, "Harnessing wind energy to power sensor networks for agriculture," Advances in Energy Conversion Technologies (ICAECT), 2014 International Conference on, Manipal, 2014, pp. 221-226.

[6] Y. Kim, R. G. Evans and W. M. Iversen, "Remote Sensing and Control of an Irrigation System Using a Distributed Wireless Sensor Network," in IEEE Transactions on Instrumentation and Measurement, vol. 57, no.7,pp1379-1387,July2014.

[7] B. Balaji Bhanu, M. A. Hussain and P. Ande, "Monitoring of soil parameters for effective irrigation using Wireless Sensor Networks," 2014 Sixth International Conference on Advanced Computing (ICoAC), Chennai, 2014, pp. 211-215.

[8] S. Khriji, D. E. Houssaini, M. W. Jmal, C. Viehweger, M. Abid and O. Kanoun, "Precision irrigation based on wireless sensor network," in IET Science, Measurement & Technology, vol. 8, no. 3, pp. 98-106, May 2014.

[9] T. C. Meyer and G. P. Hancke, "Design of a smart sprinkler system," TENCON 2015 - 2015 IEEE Region 10 Conference, Macao, 2015, pp. 1-6.

[10] R. K. Kodali and L. Boppana, "Irrigation with grid architecture sensor network," Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, New Delhi, 2014, pp. 2110-2116.

[11] N. Sales, O. Remédios and A. Arsenio, "Wireless sensor and actuator system for smart irrigation on the cloud," Internet of Things (WFIoT), 2015 IEEE 2nd World Forum on, Milan, 2015, pp. 693-698.

[12] S. Ameer, S. S. Chaubey, M. Joseph, P. Rajasekhar, S. Abhinav and R. Ravikiran, "Automatic irrigation system through a solar power,"Electrical,Electronics, Signals, Communication and Optimization (EESCO), 2015International Conference on, Visakhapatnam, 2015, pp. 1-5. doi: 10.1109/EESCO.2015.7254015.

[13] J. Gutiérrez Jagüey, J. F. Villa-Medina, A. López-Guzmán and M. Á Porta-Gándara, "Smartphone Irrigation Sensor," in IEEE Sensors Journal, vol. 15, no. 9, pp. 5122-5127, Sept. 2015.

[14] Y. z. Li and Yang Shan-shan, "Application of SVM optimized by genetic algorithm in forecasting and management of water consumption used in agriculture," Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on, Singapore, 2010, pp. 625- 628.doi:10.1109/ICCAE.2010.5451325

[15] Jaume Casadesús, Mercè Mata, Jordi Marsal, Joan Girona, A general algorithm for automated scheduling of drip irrigation in tree crops, Computers and Electronics in Agriculture, Volume 83, April 2012, Pages 11-20, ISSN 0168-1699.

[16] P. Alagupandi, R. Ramesh and S. Gayathri, "Smart irrigation system for outdoor environment using Tiny OS," Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on, Chennai, 2014, pp. 104-108. [16] Zeng, K., C. Yang, D. Wei and T. Rao. 1991. Pseudorandom Bit Generators in Stream-Cipher Cryptography. *IEEE Computer.* February. 8-17.

[17] D. Anurag, S. Roy and S. Bandyopadhyay, "Agro-sense: Precision agriculture using sensorbased wireless mesh networks," Innovations in NGN: Future Network and Services, 2008. KINGN 2008. First ITU-T Kaleidoscope Academic Conference, Geneva, 2008, pp. 383-388. doi: 10.1109/KINGN.2008.4542291.

[18] S. Wan, "Research on the Model for Crop Water Requirements in Wireless Sensor Networks," Management of e-Commerce and eGovernment (ICMeCG), 2012 International Conference on, Beijing, 2012, pp. 234-237.

[19] B. G. Jagyasi, A. K. Pande and R. Jain, "Event based experiential computing in agroadvisory system for rural farmers," 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Wuhan, 2011, pp. 439-444. doi: 10.1109/WiMOB.2011.6085362.

### 