De-Fence

Security System using LoRa-based Hop-to-Hop communication

Team:

Avil Goel (2019UCO1524)

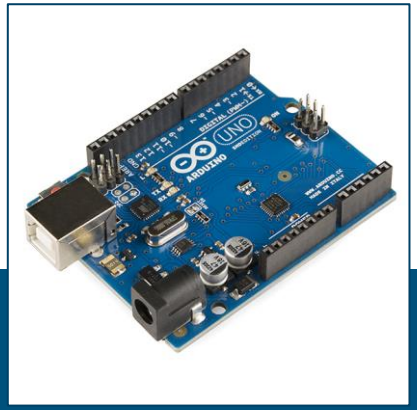
Maanas Talwar (2019UCO1544)

Anav Chaudhary (2019UCO1577)

Problem Statement and Inspiration

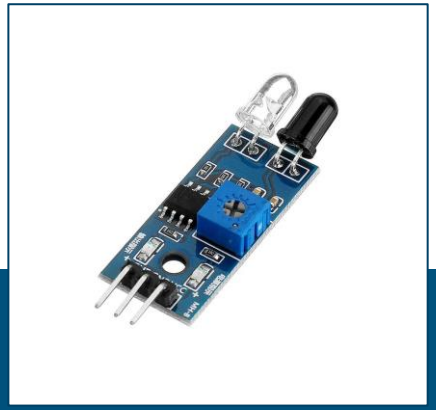
- Limited networking capability in **remote areas**
- Areas with **environment hostile** to long range wireless transmission, **interference** is also involved
- **High Power requirements** of traditional security systems,
- Current system of human-based manual updates is **impractical** and **prone to blind spots**
- Existing infrastructure is fixed and leaves **little room for flexibility**

Hardware Used



Arduino UNO

Arduino Uno is a microcontroller board based on the ATmega328P



IR Sensor

Electronic device that measures and detects infrared radiation in its surrounding environment, most commonly used in motion-based detection

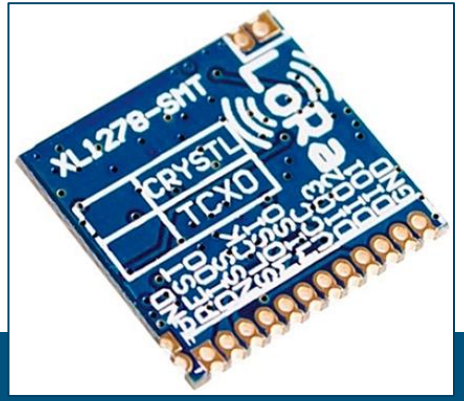
Buzzer

Simple device which can generate beeps and tones, whose working principle is piezoelectric effect

Jumper Wires

Small cables used to connect other components to network cabling

Hardware Used



LoRa XL1278 Module

- Non-cellular, secure, programmable, low-power RF modules, providing long-range IoT data connectivity to sensors and actuators.
- Its **range** is quite high, and can penetrate multiple obstacles.
- Less infrastructure required, making network much cheaper and faster to implement.
- LoRa modules can be recognized accurately even in a low signal-to-noise ratio (SNR) environment. They can be distinguished and identified effectively.

Components of IoT

Buzzer
(Actuator)

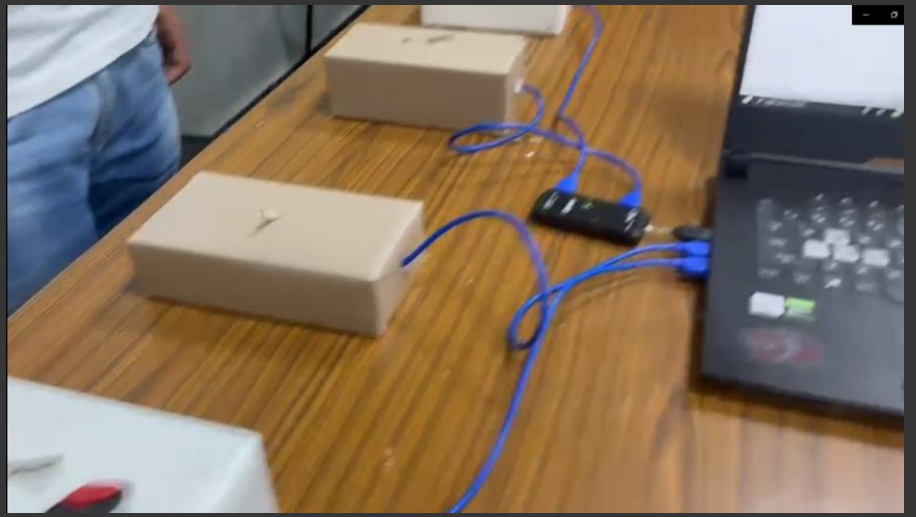
Node
(Thing)

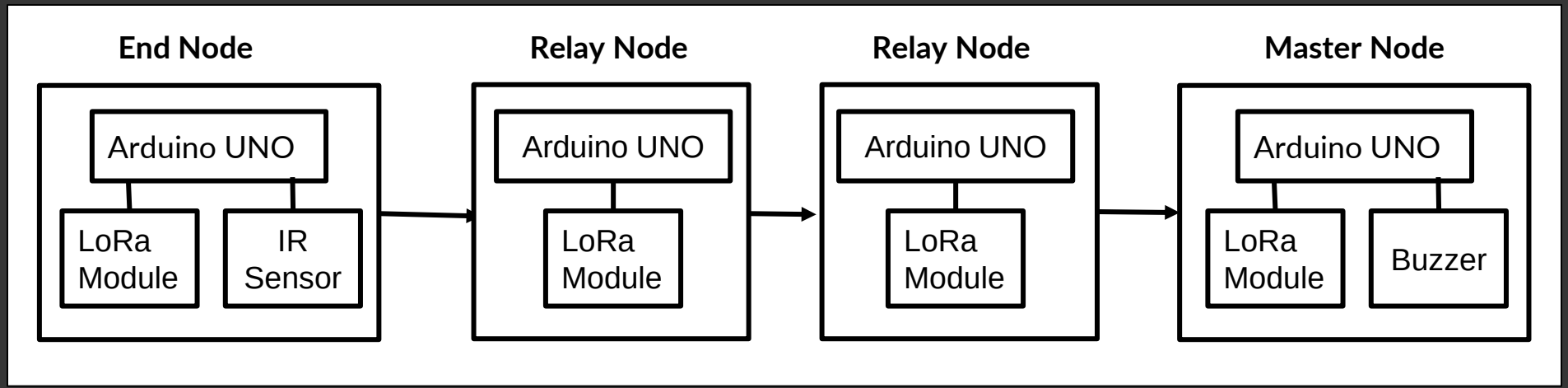
LoRa module
(Communicator)

IR Motion
(Sensor)

Arduino
UNO
(Controller)

Schematic Diagram





Features

Scalability

As the area to be covered increases, more nodes can be added to the network, in order to ensure a smooth expansion.

Reliability

The network does not have a single bottleneck and can keep working even if a few of the nodes fail.

Security

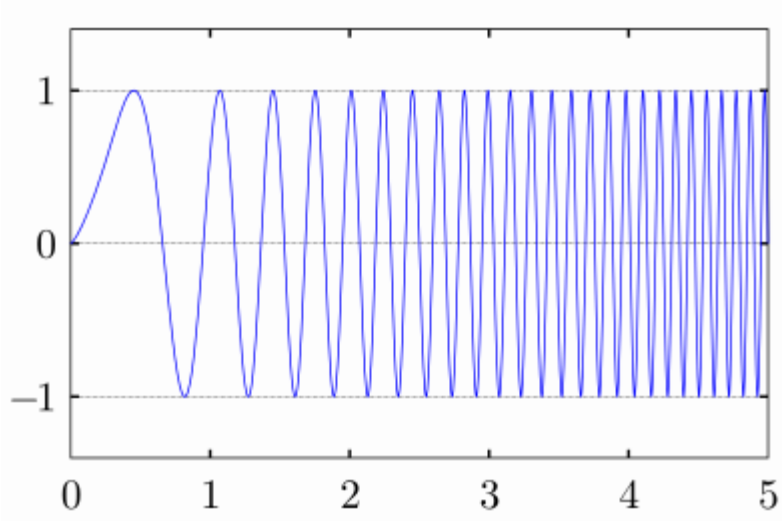
It avoids the risk of cyber threats, especially from the internet, and ensures confidentiality using end-to-end encryption.

Target Audience

- Dense and widespread security coverage under situations where constant and widespread **internet connection** is not available, or **concentrated electric coverage** is not feasible, for example, large compounds or sites in distant locations.
- The stakeholders include agencies/bodies that offer security management systems in remote areas and **high altitude water pipeline defect detection**. It is suitable for an **off-the-grid surveillance** and **intruder-detection** setup.
- This structure is highly versatile and flexible, and it is highly secure against attacks. We can also increase the **speed of communication** by choosing the **optimal path**, as well as special pathways for encrypted transmission.
- This would allow the network to be quickly established and **easily maintained** as **portable** individual sensors can be easily registered or removed from the network.

LoRa Technology

- LoRa, from Long Range, and LoRaWAN together define a long range, low power, low bitrate networking protocol.
- LoRa is the proprietary physical radio modulation technique, derived from Chirp Spread Spectrum technology.
- LoRaWAN defines the software communication protocol and system architecture. The continued development of the LoRaWAN protocol is managed by the open, non-profit LoRa Alliance, of which SemTech, the company currently in possession of the patent for LoRa, is a founding member. The latest LoRaWAN version is 1.0.4, released in October 2020.
- The LoRa alliance is a non profit association created to support LoRaWAN protocol, as well as to ensure interoperability of all LoRaWAN technologies.



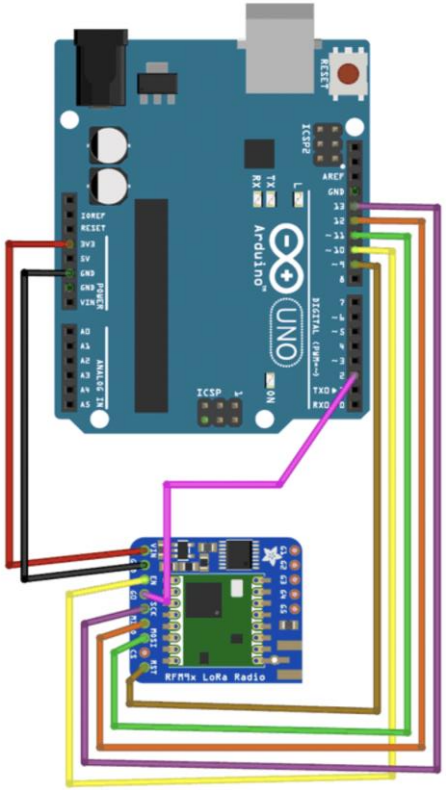
- Chirp spread spectrum (CSS) is a spread spectrum technique that uses wideband linear frequency modulated chirp pulses to encode information.
- A chirp is a sinusoidal signal whose frequency increases or decreases over time.
- Chirp modulation uses the entirety of its bandwidth, so its is robust against channel noise. They are also resistant to multipath fading making them ideal for use in locations with multiple obstacles. It is also resistant to the Doppler effect. However, unlike other spread spectrum techniques, CSS does not include special elements to distinguish itself from the noise.
- Originally developed to compete with ultra-wideband, it is instead now recommended for personal mobile networks.

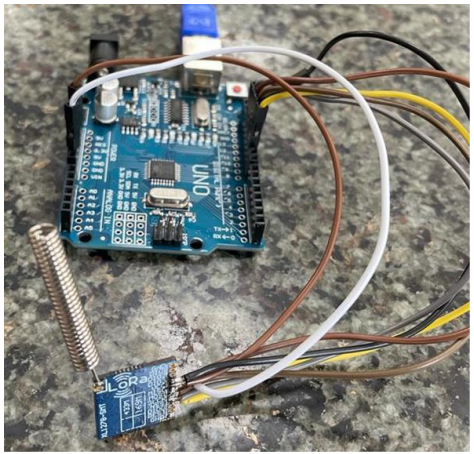
- There is a large variety in LoRa enabling solutions provided by Semtech.
- The LoRa Core portfolio represents the essential capability of Semtech's LoRa devices including long range, low power and cost effective end-to-end communication.
- LoRa Edge is an ultra-low power platform that integrates a long range LoRa transceiver, multi-constellation scanner and passive Wi-Fi AP MAC address scanner targeting GNSS asset management applications.
- LoRa 2.4GHz offers ultra-long range communication in the 2.4GHz band with lowest power and highest reliability connectivity.
- We have used a version of the Semtech SX1278 (LoRa Core), the XL1278, which has simplified circuitry.

Interfacing components with the Arduino Uno

- LoRa XL1278-SMT Module
- IR sensor
- Buzzer

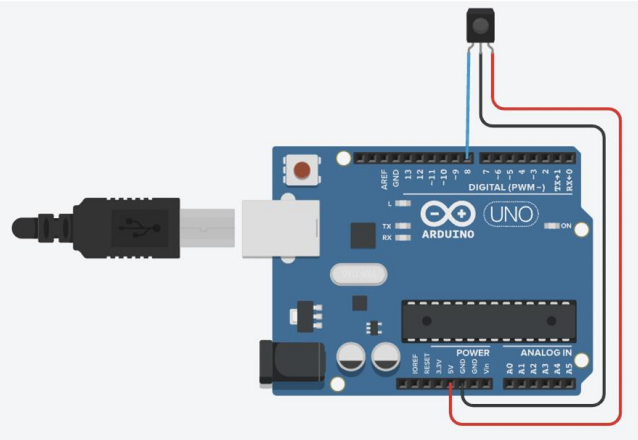
Interfacing LoRa XL1278-SMT





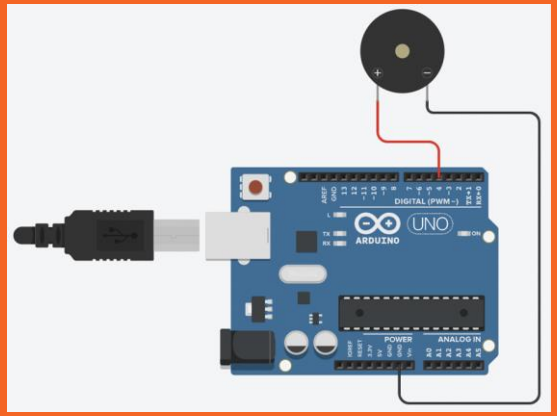
LoRa XL1278 Module	Arduino UNO Board
VCC	3.3V
GND	GND
NSS	D10
DIO0	D2
SLCK	D13
MISO	D12
MOSI	D11
REST	D9

Interfacing IR sensor



IR Sensor	Arduino Uno
VCC	VCC
GND	GND
OUT	D8

Interfacing the Buzzer



Buzzer	Arduino Uno
+	D4
-	GND

Our Prototype

- Path discovery in the ad-hoc network
  - Flooding the network to determine a valid path between the end node and master node
  - Retracing the path to let the end node know about the path
- Sending the payload

- 1 End node to detect objects using sensors and initiate the data transfer
- 2 Relay nodes to relay the data from the end node to the master node
- 1 Master node to process the received information and sound the alarm

Packet Description

[Type] * [MessageID] * [Destination] * [Source] * [Path] * [Payload] *

The whole message can be of maximum 256 bytes.

1. **Type** - Flood (F), Retrace (R), Sending payload (P)
2. **MessageID**
3. **Destination node ID**
4. **Source node ID**
5. **Currently traversed(flood)/remaining(retrace and payload) path**
6. **Payload/message**

End Node

- IR sensor detects a new object in the surroundings
  - Creates a message for the master node
  - Adds self node ID to the path
  - Initiates path discovery by flooding the message
- Retrace message is received
  - Checks if the message is intended for this end node
  - Encrypts the payload
  - Removes the self node from the path
  - Creates the message with encrypted payload and sends

The source and destination IDs are changed as and when required.

Relay Node

- Flood message is received
  - Change the source node ID in the packet
  - Add the self node ID to the path
  - Flood the message again
- Retrace/Payload message is received
  - Checks if the message is intended for this relay node
  - Removes the self ID from the path
  - Sends the message to the next node in the path

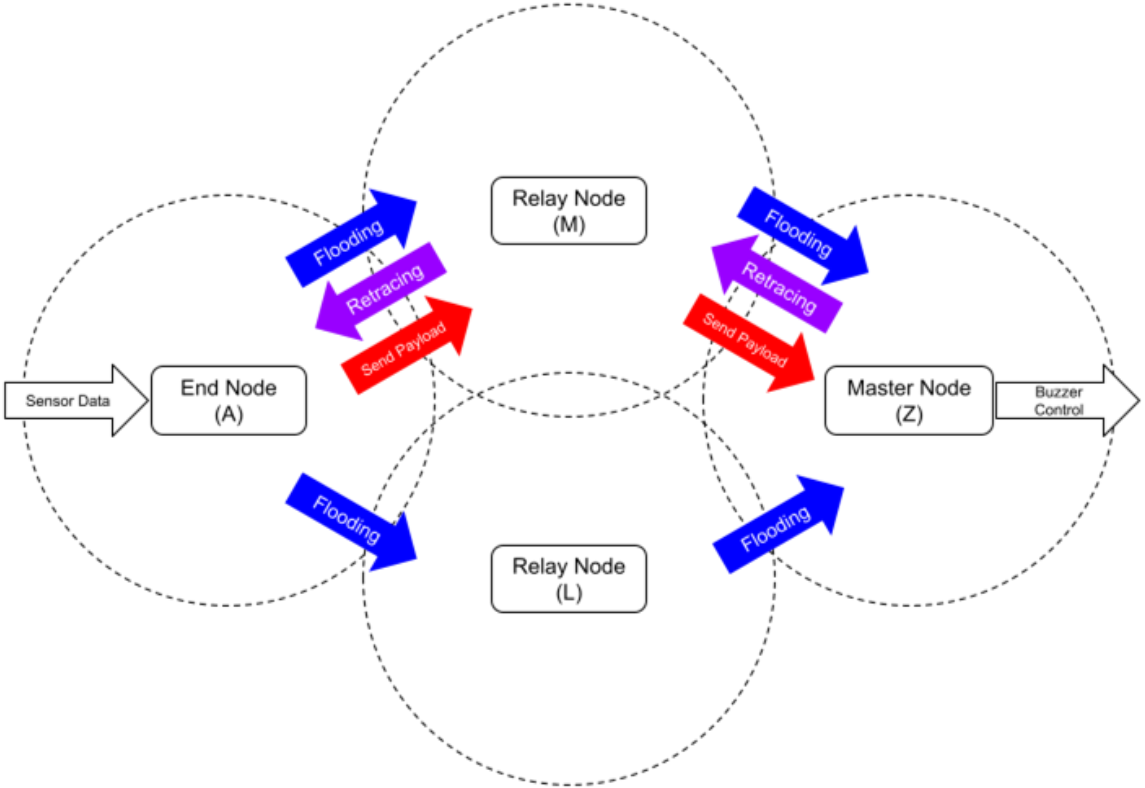
The source and destination IDs are changed as and when required.

Master Node

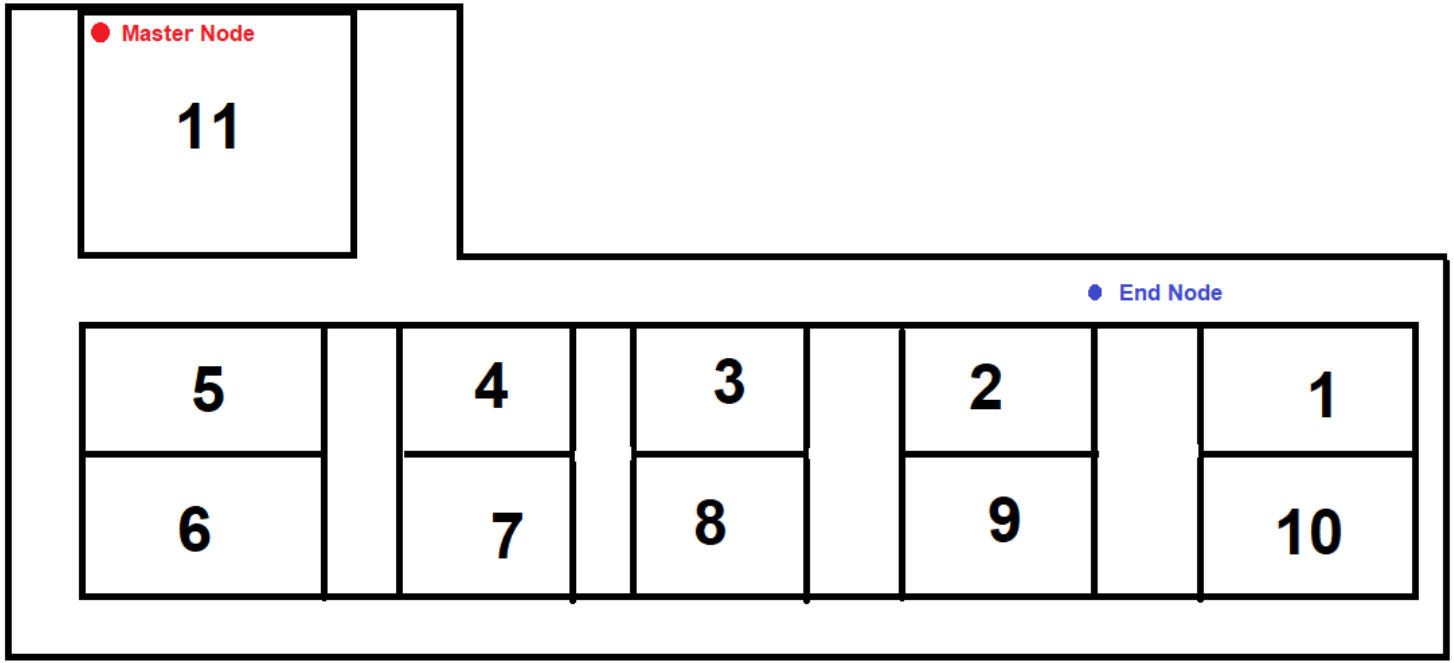
- Flood message is received
  - Add the self node ID to the path
  - Add the path as a payload
  - Send a retrace message
- Payload message is received
  - Checks if the message is intended for this master node
  - Decrypts the payload
  - Sirens the buzzer if “MOTION DETECTED” payload is received

The source and destination IDs are changed as and when required.

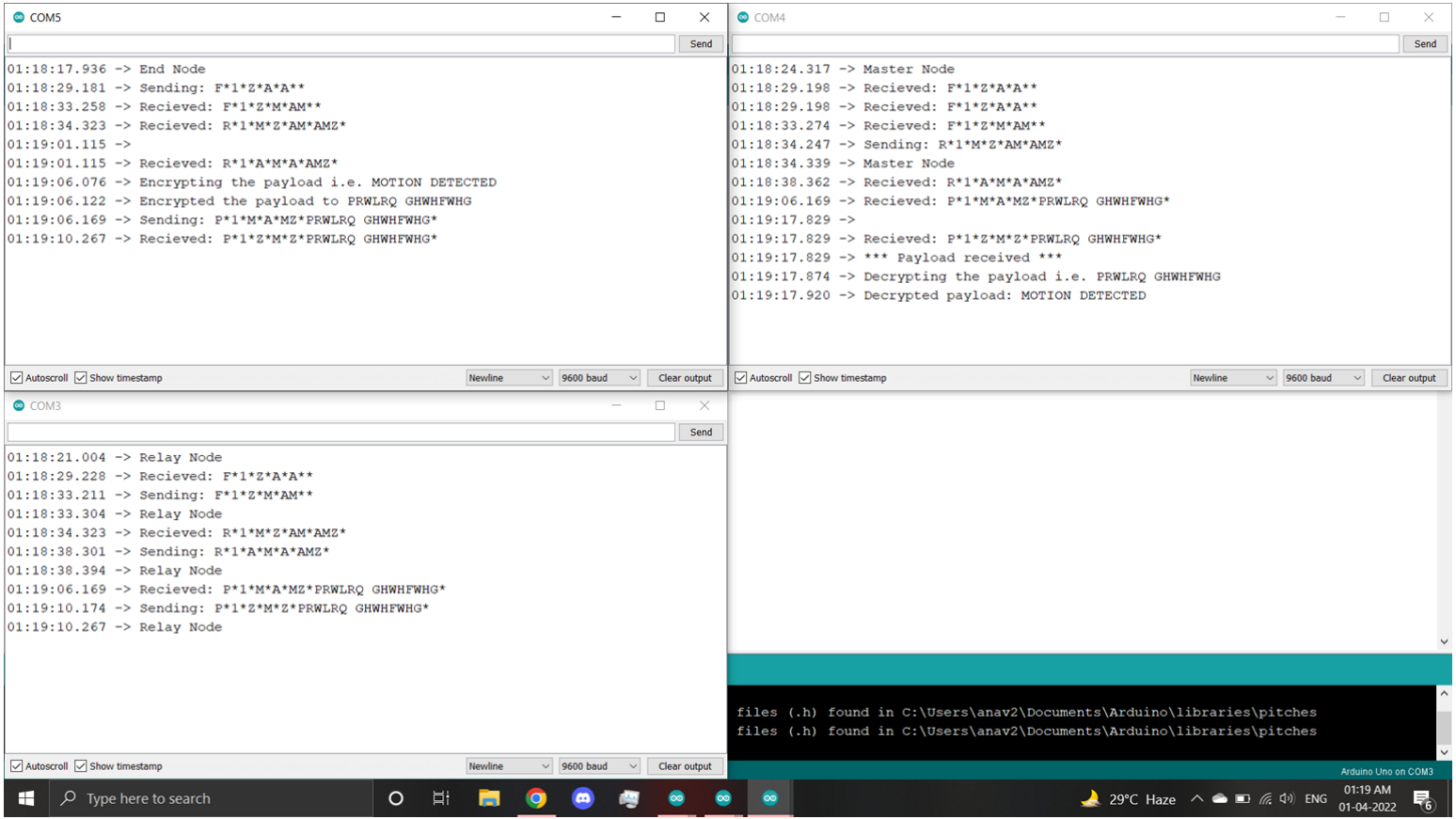
Workflow


Relay Node
(M)
Flooding
Retracing
Send Payload
Flooding
Retracing
Send Payload
Sensor Data
End Node
(A)
Master Node
(Z)
Buzzer
Control
Flooding
Flooding
Relay Node
(L)

Stress Test Results



Demonstration



Future Scope for Improvement & Upgradation

- There is still scope for additions, and upgradations in the project.
- We currently use a basic, inexpensive IR sensor, which does not match capabilities of other industrial grade sensors. Better, stronger and more varied Sensors can be used.
- A better controller can be used to allow more Sensors to be used at a certain time, and more complex encryption algorithms can be run without losing precious processing time. A better antenna can also be used to improve range.
- A more complex packet based streaming protocol can be created to allow transmission of packages greater than the limit allowed on a single LoRa packet (256 Bytes).
- More robust and secure packaging can done to decrease maintenance and increase node security.

Thank you