TOPIC - NODE TO NODE EFFICIENT DATA TRANSFER

Major area and domain - Internet of things (IoT) and secure data transmission.

Name of Mentor - Dr. Trina Som

List of Group Members - 1. Aakash Avashthi
2. Bhaskar Dutt
3. Ashish Saini
4. Mohd. Raza

Objective - In this project we are aiming to

1. Reducing Power consumption while there will be transfer of data through multiple nodes.
2. A way using which we can increase the distance between the nodes during data transfer.
3. Providing end to end security to the user's or organisation's data.

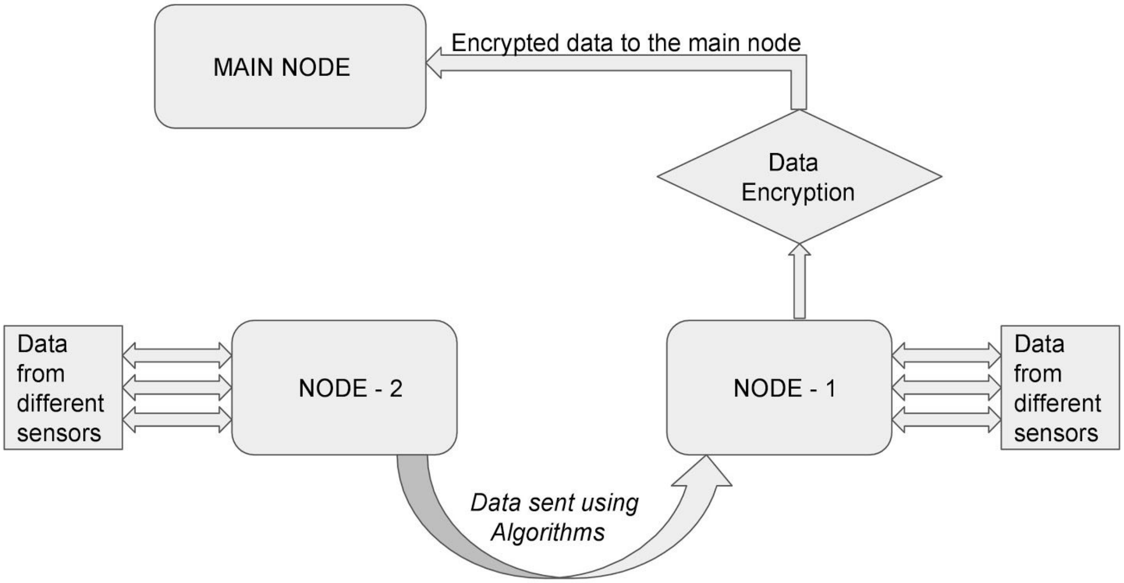
Introduction -

Typical IoT system architectures include devices (or nodes) which are deployed in physical spaces and usually include one or more sensors; hubs (or gateways or edge) which bridge between communication protocols and are located relatively close to the devices; a centralised cloud environment which stores and processes the data, and front-end devices which users can interact with, explore the data and get notifications. Obviously, there are scenarios where the devices communicate directly with the cloud environment and scenarios where the devices act as the frontend device, but logically, this architecture describes the common roles in the setup.

A typical IoT system might include hundreds and even thousands of devices, each with multiple sensors, so it's not a surprise that IoT and big data are two buzz words which are frequently mentioned together[1].

To derive the relevant insight to the users from this huge stream of data we need to process the data, typically, using machine learning and signal processing algorithms. Most of the time, these algorithms require a lot of computational resources such as CPUs, GPUs, and memory which are both power hungry and expensive. It is possible to place computation resources at every component of the system: device, hub and cloud which can then process the data that passes or is stored there. So, it’s the system architect decision on how to split/distribute the processing across these components and how to optimise the “cost” function based on the tradeoff criteria[2].

Derived from the capacity of the battery, the duty cycle between the different power modes (active, standby, off) and the nominal power consumption of the sensors, CPU and communication interface. Where sending the raw data to the cloud will increase the power consumption of the communication interface, processing the data locally will increase the power consumption of the local CPU.


MAIN NODE
Encrypted data to the main node
Data Encryption
Data from different sensors
NODE - 2
NODE - 1
Data from different sensors
Data sent using Algorithms

In some cases, sensors might collect privacy data or commercially sensitive data which we would like to restrict access to. Imagine a camera based occupancy sensor which is placed in a meeting room where sensitive material is presented. Theoretically, we can send the video feed to the cloud and process the data there, but this will expose the system to security risks and might raise ethical concerns. Alexa detects the word "Alexa" locally and doesn't send all of our conversations to the cloud. Only when the word Alexa is detected, the following request is streamed to the cloud. If a corporate needs to process a large amount of sensitive data, the edge might be a good place in the middle between the cloud and the device as it's placed within the corporate walls and also brings some of the benefits of the cloud.

Conclusion -

From the above ideas we are delivering data transmission at different distance between the nodes. For high end to end security, the data transferred will be encrypted from the sender's end and will be decrypted at the receiver's end.

References -

[1]. Lea, Perry. *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security*. Packt Publishing Ltd, 2018.

[2].Forouzan, A., and G. Hill. "Data Communications and Networking, by Behrouz." *Forouzan* (2006).