**TITLE OF THE PROJECT:**

PHYSICAL LAYER SECURITY FOR INTERNET OF THINGS: AUTHENTICATION AND KEY GENERATION

**PROJECT MEMBER’S NAMES:**

1. NARAYANAN B – 2016105053
2. VENKAT KRISHNAN B K J – 2016105077
3. ASHOK KUMAR M – 2016105513

|  |  |
| --- | --- |
| **GUIDE NAME** | **SIGNATURE** |
| MRS. N. VIJAYA |  |

**OBJECTIVE:**

To overcome the difficulties of current cryptographic key exchange schemes on IoT devices and to provide a less complex yet secure authentication system for the IoT devices.

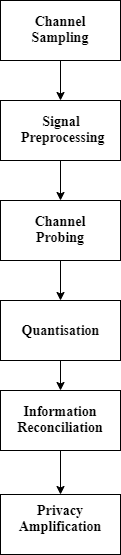
**PROBLEM STATEMENT:**

The IoT provides transparent and seamless incorporation of heterogeneous and different end systems. The connected devices will spread highly sensitive personal data. Sending this type of data represents a serious risk for people’s privacy, since malicious interests could lead to an illegitimate use of personal information. Although the cryptographic schemes such as ECDH have been efficient in protecting modern communication and computer networks, their applications in IoT have been challenged. This is because conventional schemes are based on complex mathematical problems and protocols. These schemes work well for devices having powerful capabilities, such as smartphones. There is a large amount of IoT devices that are of low cost, small size, and battery-powered. These lightweight devices may not be able to support computationally complex algorithms needed to perform the complex cryptography. Hence, a new system is required which is secure but at the same time less complex so that it can be supported by these lightweight IoT devices.

**TOOLS REQUIRED:**

1. Matlab
2. Raspberry Pi

**FLOWCHART:**



**TIME FRAME CHART:**

|  |  |
| --- | --- |
| **TIME** | **WORK SCHEDULE** |
| Week 1 | Problem Analysis |
| Week 2 | Study and Analysis of existing systems and their disadvantages. |
| Week 3 |  |
|  |  |
|  |  |
|  |  |
|  |  |

REFERENCE: