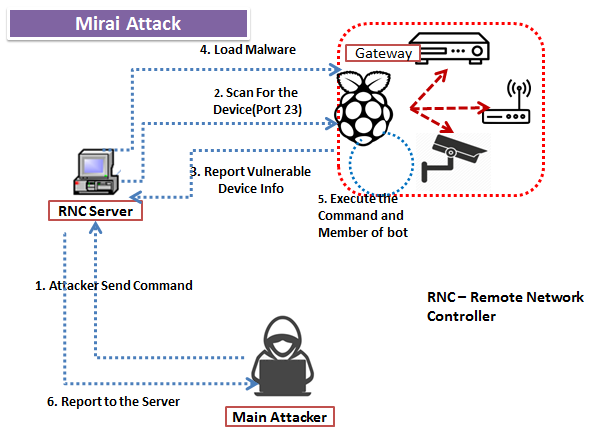
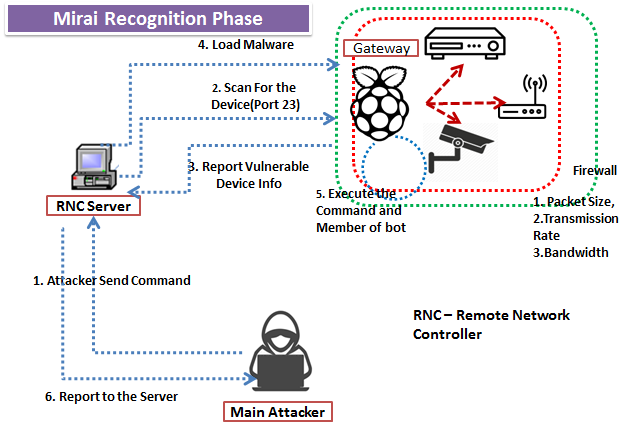
Mirai relies on default telnet username and password to infect other devices, so the best and the easiest way to protect device from being infected is to change its default remote access settings. The figure 1 shows the how Mirai attack takes place for infecting the particular device.



**Figure 1:** Mirai Attack

The main concern of the proposed system is to analyze the traffic generated by the devices for detection of presence of Mirai. Figure 2 gives the detection of the Mirai attack by extracting the features like from transmission of the packet. The firewall represent from where we have to extract the transmission features for the Mirai detection.



**Figure 2:** Detection of Mirai Attack

The detailed explanation of the proposed system is given below.

* **Searching New vulnerable device**: Attacker gives the command through RNC (**Remote Network Controller**) server to finds a new IoT device member’s open port (In our case it is raspberry Pi) for attacking. Here it finds the new member’s **username, password, IP and port number** for attacking the particular node (Mostly port 23 and 101 by default is used for attacks on any device). It finds new nodes telnet port to identify possible targets. The report is all sent to the main attacker via the CNC server.
* **Infecting the device by running the malware:** After receiving the vulnerable node information i.e. Username, password, and IP and port number successfully, the report is sent to the RNC server and it first checks for the architecture of the device.
* **Load Malware:**Once the RNC server gets all the information related to the node which is being attacked, then the RNC server sent malware (Executable code) to the raspberry pi (**Target Node)**. As soon as the raspberry pi runs the code then it will become a member of the botnet and ready to infect the other bots in its network. A continuous communication takes place in between RNC and Raspberry pi. All the device information is reported to the main attacker via RNC server. Transmission Control Protocol (TCP) is used to establish a connection first with RP and then with rest of the devices.

**Example:**In our figure, the raspberry pi can infect the devices i.e Router, DVR recorders or CCTV cameras in its network.On RNC command raspberry pi executes the attack and send traffic as fast as no rate limiting.

* **Attack Detection:**For detecting the existence of Mirai, first we extract the features of the transmitted packets**such as transmission** frequency of the packets generated by devices (in our case RP), Bandwidth, and Packet size. Then by analyzing the extracted features, we can detect the existence of the Mirai attack and notify it to the local network administrators.