**Service Provider**

In this module, the Service Provider browses the required file and uploads their data files to the Specified End User and with their DIP (Destination IP) of End User.

**Watch Dog Router**

The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts in channel assignment. The local watchdog can generate the following events about neighbor nodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt Channel (negative event) when the watchdog detects that a node is not selfish, and NoDetEvt Channel (no detection event) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on neighborhood packet overhearing; thus, when the watchdog overhears packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module.

Malicious Nodes and Attacker Model

Malicious nodes attempt to attack the CoCoWa system by generating wrong information channel assignment about the nodes. Thus, the attacker model addresses the behavior of channels or capabilities of these malicious nodes. A malicious node attack consists of trying to send a positive about a node that is not a selfish node, or a negative about a selfish node, with the goal of producing false positives and false negatives on the rest of nodes. In order to do this, it must have some knowledge about the way CoCoWa works.

**End User(Destination)**

In this module, the End user is responsible to receive the file from the Service Provider via Watch dog router after overcoming the attackers.