Security issues of the botnet

One big security issue with the botnet is the fact that none of the messages sent are encrypted. Anybody could intercept the messages and see what people are sending to each other or alter the messages. One way to fix this issue is to have TLS or Transport layer security which encrypts the data. Even with TLS replay attacks would still be a problem. Replay attacks are when a hashed message is intercepted on the way to the recipient and they send it again to try to gain some information. This could be stopped by using the timestamp and only replying to the request with a matching time stamp or using a unique nonce.

Another issue is a vulnerability to DOS attacks (or Denial of Service) which is when an attacker send a large amount of requests, overwhelming it and making it unavailable to the intended users. To mitigate DOS attacks there would have to be pattern recognition to spot when someone shows signs of trying to flood the server and then deny any further request from that person this could be done by logging every request that is sent to each server.

Since there is no authentication, anybody could make a server or a client program and impersonate a group and send and receive messages as if they were a part of that group. To mitigate this every group would have to be verified by either a token or ID verification.

Any group could also make their server send a getmsg request to any server and most likely get a response with the messages that were intended for that group. This would work on any group that does not verify that this request comes from their own group number.