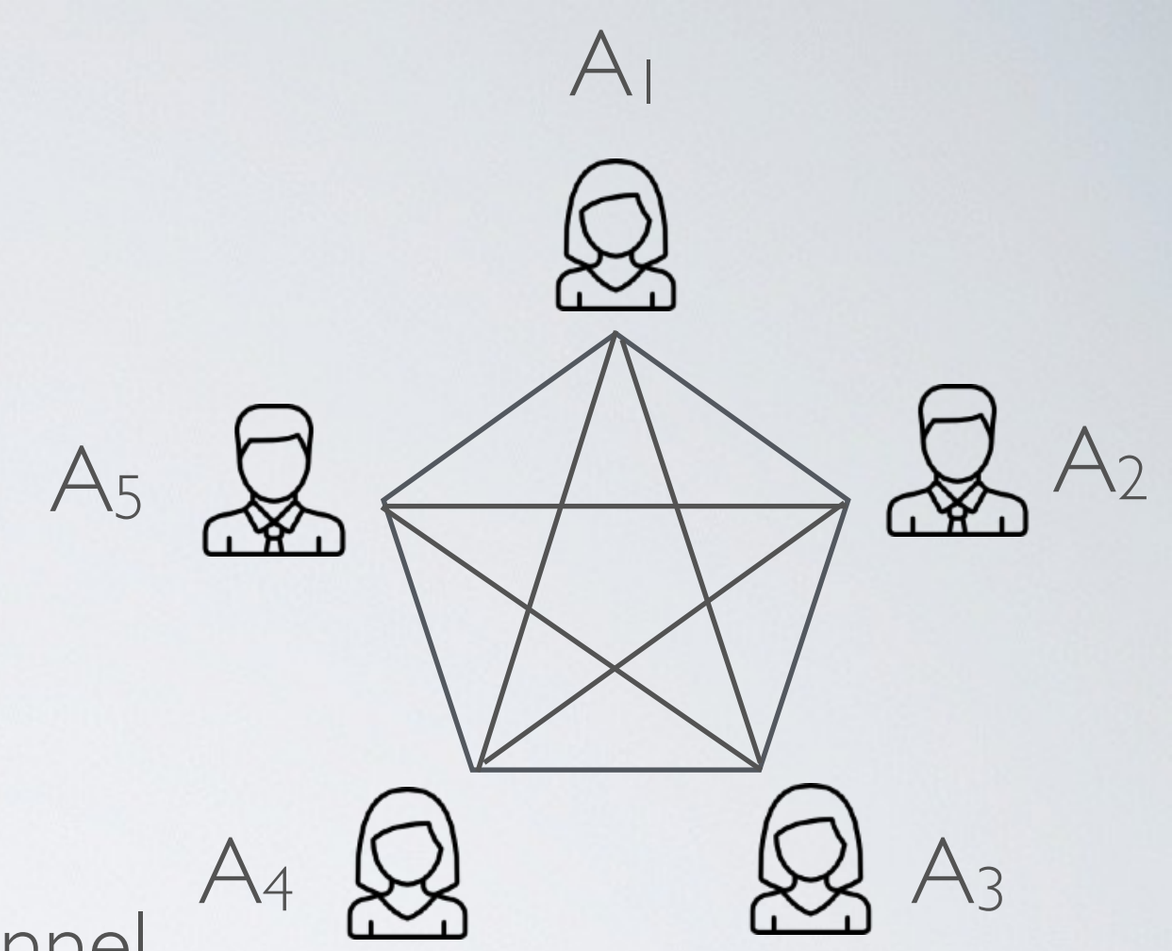
Replay attacks

Interactive Protocol



System Hypothesis

- Synchronous communication channel
- Each participant share a unique symmetric key with each other
- Mallory can read, modify and forge message send over the network

Goals

- When two participant exchange a message, the system should protect the confidentiality and integrity of the message