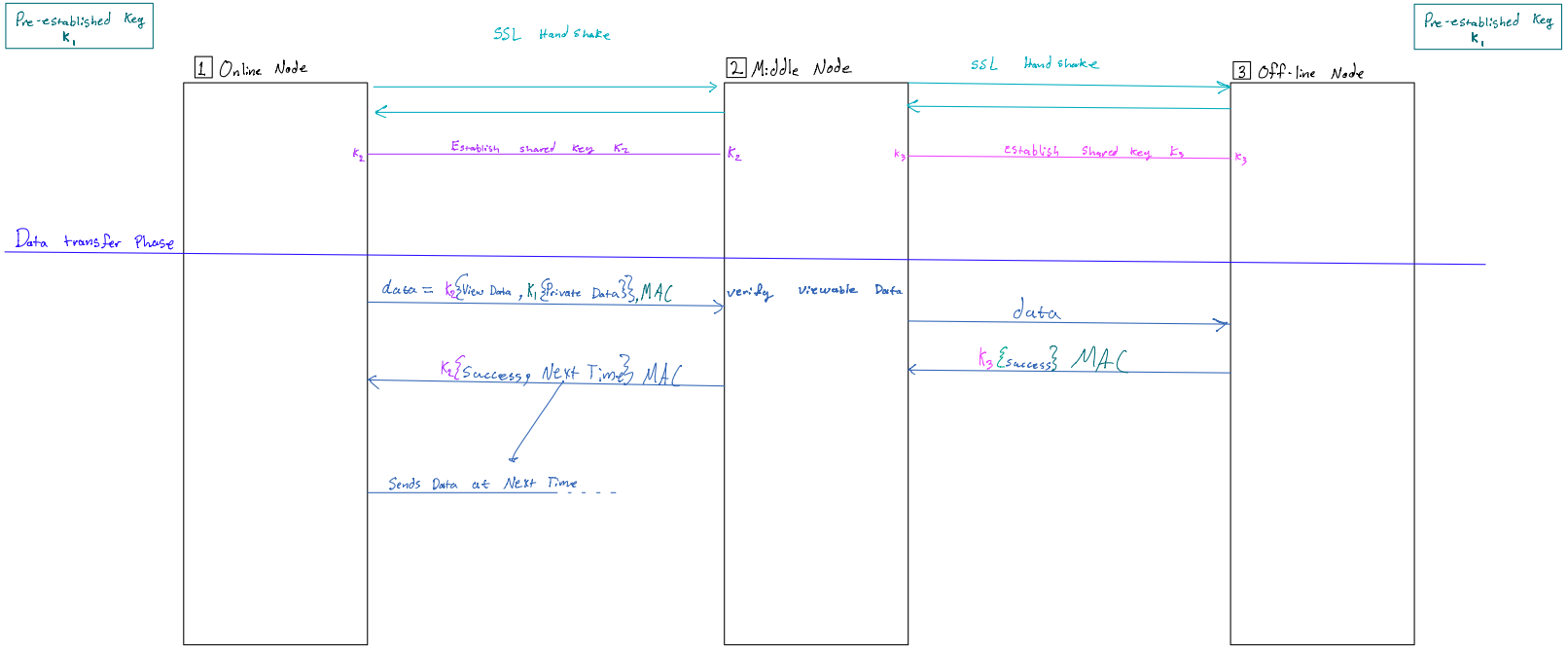
Pre-established Key
K_1
Pre-established Key
K_1
SSL Hand shake
1 Online Node
2 Middle Node
SSL Hand shake
3 Off-line Node
K_2
Establish shared key K_2
K_2
K_3
establish shared key K_3
K_3
Data transfer Phase
data = K_2 {View Data , K_1 {Private Data}}, MAC
verify viewable Data
data
K_2 {Success, Next Time} MAC
K_3 {Success} MAC
Sends Data at Next Time