One major issue

Key distribution

If A1, A2 … A5 want to talk, then **n** public keys must be distributed physically to each user using a secure channel

Why not?