Ensuring Cybersecurity via Distributed Online Secret Sharing

Bharath Satheesh

UAVs Takeover the world

- Jeff Bezos from Amazon claims that there is going to be little over a **million** UAVs in the sky by 2025.
- Facebook wants to connect the world with its project Aquila
- Lots more hobbyists and recreational flying in the open

With over a million delivery, service and internet connectivity UAVs in the air, **how do we provide safety and robustness to these complex systems against cyber attacks**?

Problem Setup

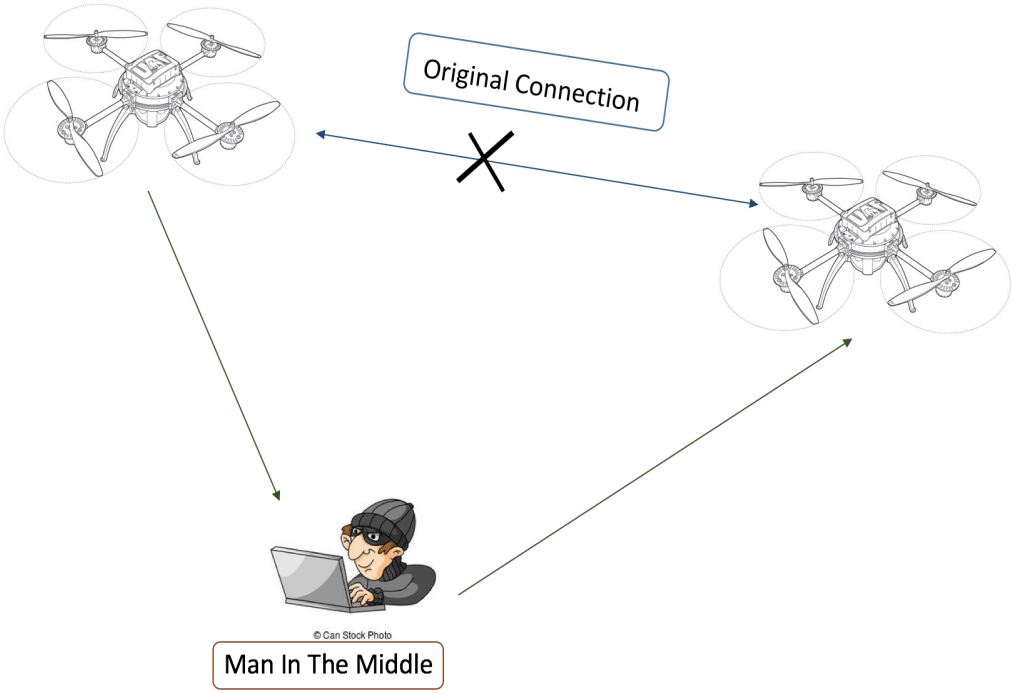
- Suppose we have *n* UAVs flying from point A to point B to deliver goods and cargo, infrastructure surveillance, provide internet connectivity etc.

- The UAVs would communicate states (x, y, z, w, p, r and their derivatives) between each-other:
  - To perform a mutual collision avoidance maneuver
  - To transmit GPS co-ordinates to a remote control center for change of model under increased traffic

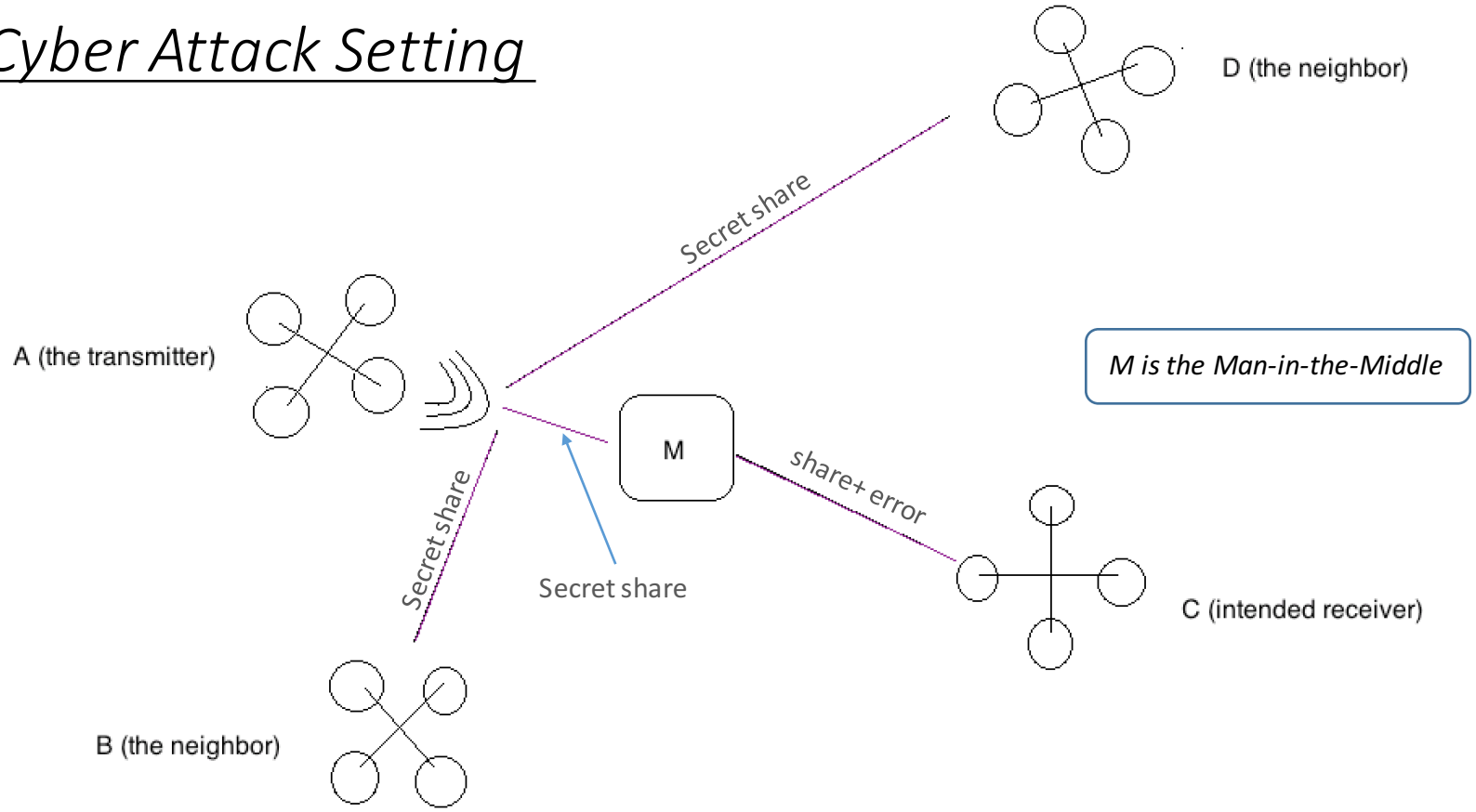
MITM Attacks

- The communication links between the UAVs could be subject to Man-In-The-Middle (MITM) attacks in which a malicious agent spoofs the information being sent and/or received.

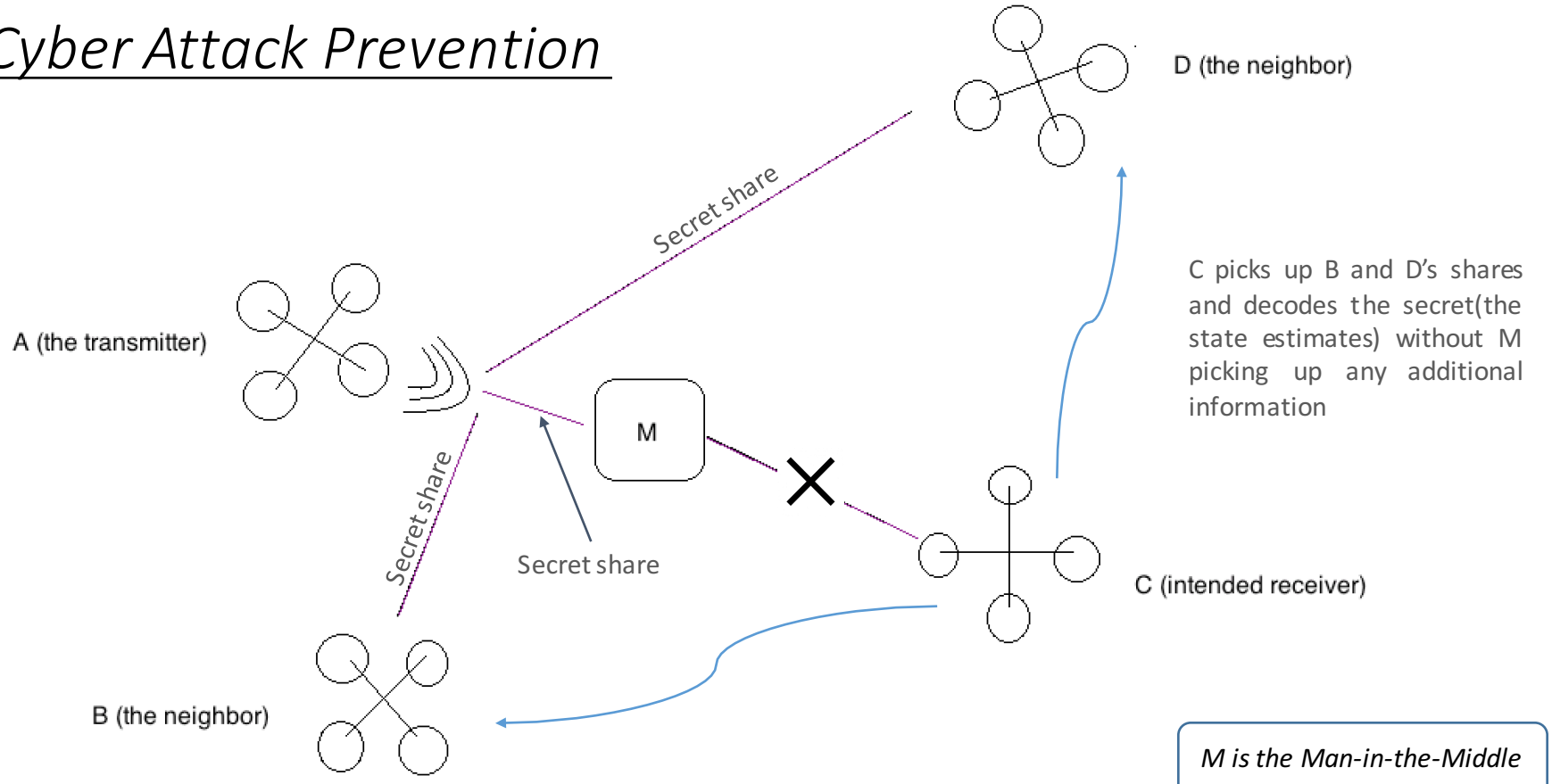
- Successful attacks can lead to collisions of vehicles, economic loss and bodily damage.



Cyber Attack Setting

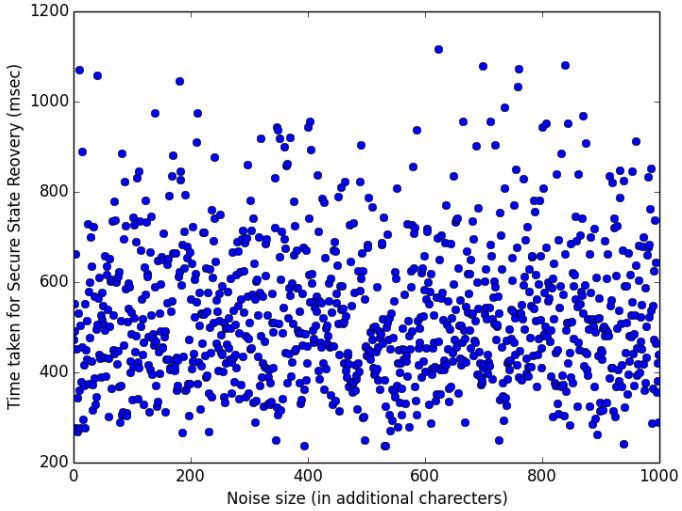


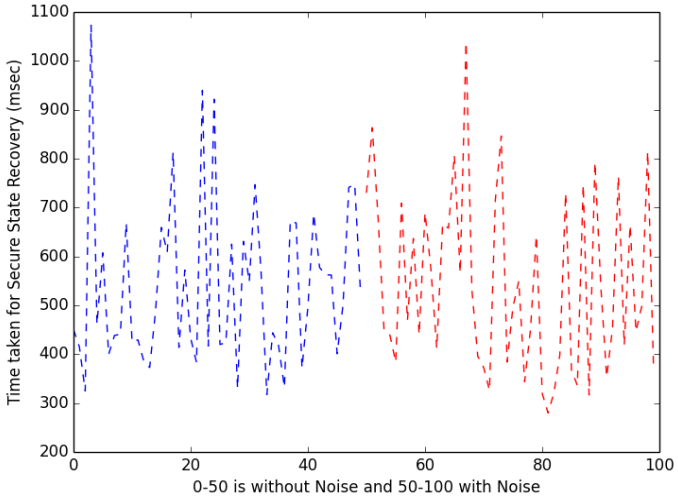
Cyber Attack Prevention



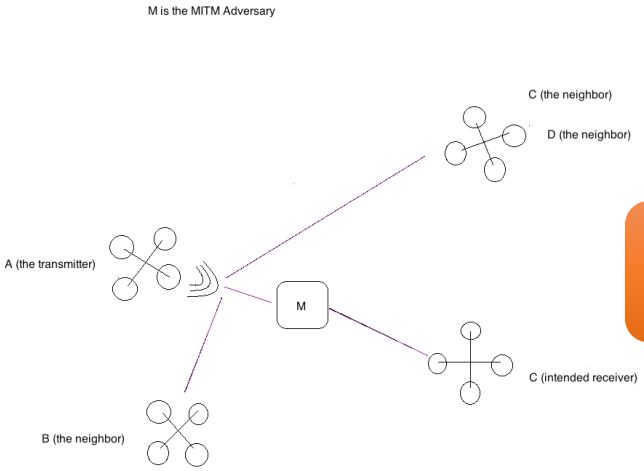
Some Encouraging Results

- We see as expected that regardless of the amount of noise, we attain secure state estimation with a mean time of 532msecs (That's almost 100x faster than compressed sensing)
- We see that the time taken to decrypt the message without noise is very similar to the time taken to retrieve the message via secret sharing
- The message transfer is SECURE and ROBUST i.e. no middle man can crack/ comprehend the message
- We are also guaranteed** complete recovery of the message regardless of the sparsity of the message
- This method can be easily ported into a larger UAV platoon* system using secret sharing schemes





Next Steps



Applying SNEAK

Tuning best (n, k) divide

checking for outside noise (additional KF)