RELIABLE CYBER-PHYSICAL SYSTEM DESIGN OVER UNRELIABLE COMMUNICATION CHANNELS

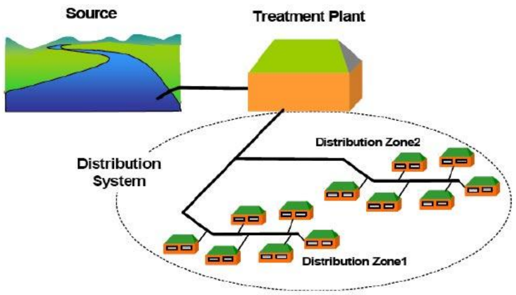
Fardin Abdi Taghi Abad

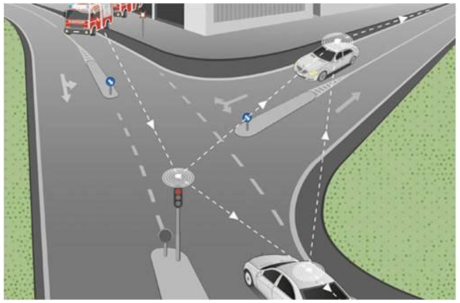
- This work has been submitted to ICCPS2013:

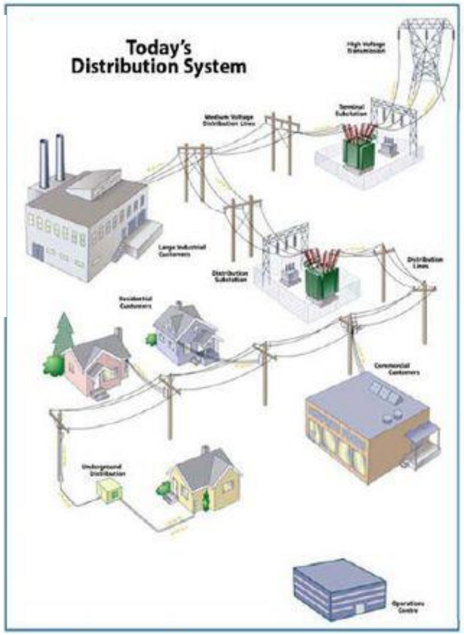
S. Bak, F. Abdi, Z. Huang, and M. Caccamo, “Reliable cyber-physical system design over unreliable communication channels,” Submitted to ACM/IEEE 4th International Conference on Cyber-Physical Systems, 2012.

Distributed Cyber Physical Systems

- **Interconnected** physical plants that **physically** affect each other!
- State of each node is a function of control inputs of other nodes based on system connection graph



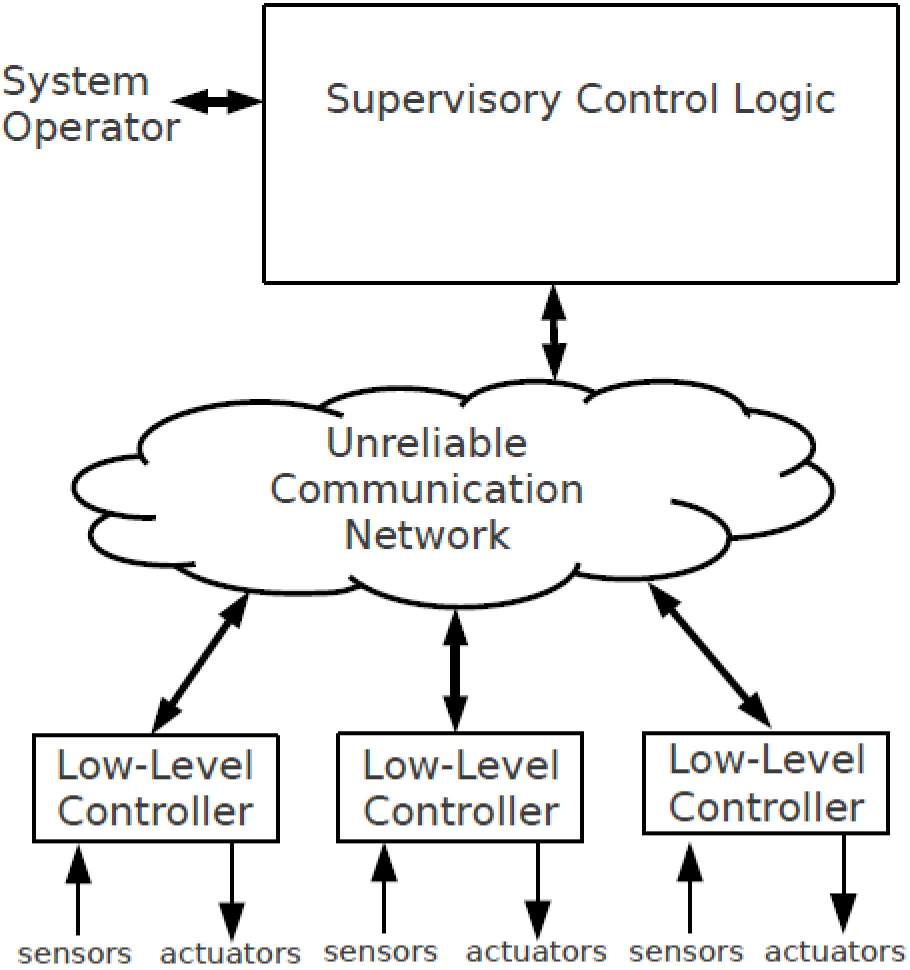




Images :
http://geospatial.blogs.com/geospatial/2009/07/alternative-energy-green-nonemitting-clean-renewable-or-low-carbon-.html
http://www.thewatertreatments.com/water/distribution-system/

System Description

- Central coordinator
- Agents follow the most recent received command and ignore the previous ones
- Each controller locally exponentially stable



Problem Description

- Communication
  - Unbounded Delays
  - Packet Drops
  - Physical failures

- Central controller Errors
  - Software bugs
  - Component malfunctioning
  - Logical bugs

Problem Description

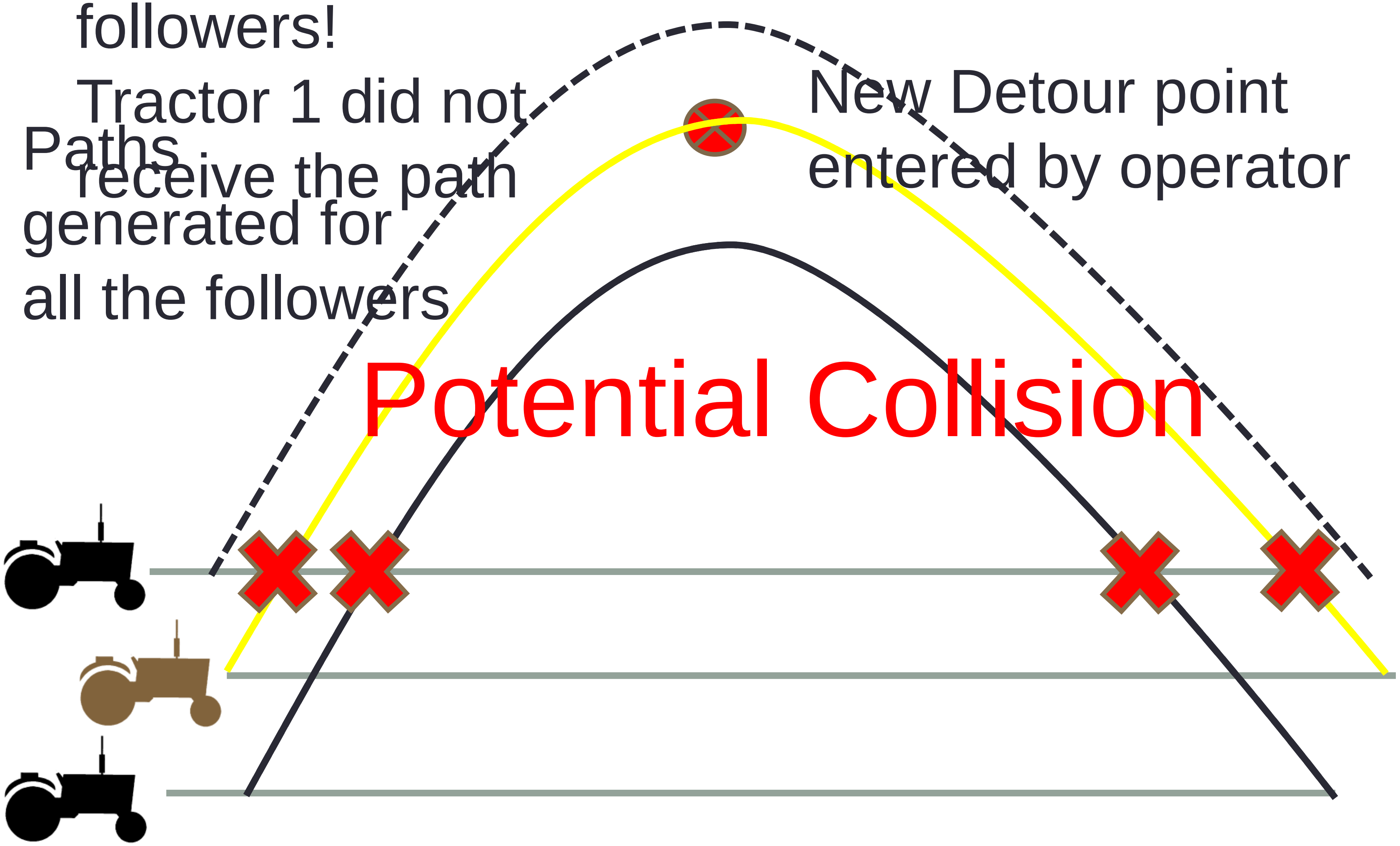
- Distributed controllers coordinate with other nodes in order to:
  - Reach to the desired state for the entire system
  - Maintain functionality and stability of the system

- System relies on Communication!
  - North American Electric Reliability Council report: information system failure is a major reason of cascade failures!

Paths sent to followers!
Tractor 1 did not receive the path

Paths generated for all the followers

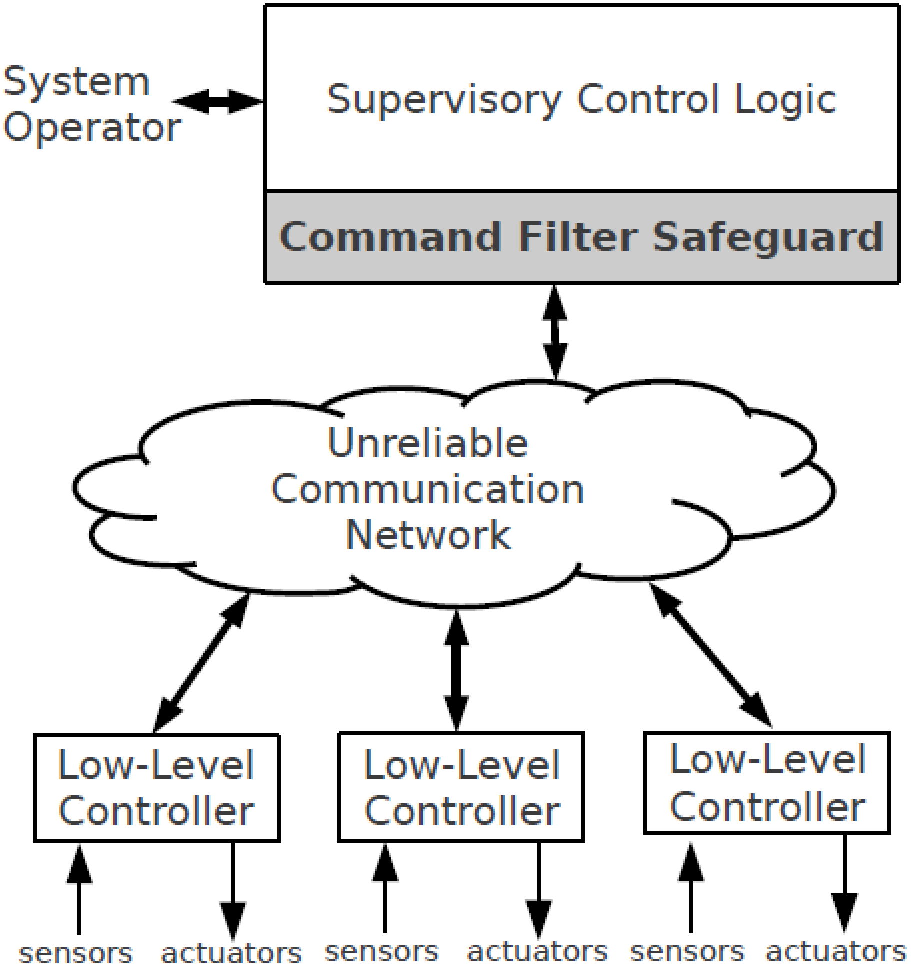
New Detour point entered by operator



Potential Collision

Command Filter

- Performs Run-time checks on outgoing commands
- Drops unsafe commands

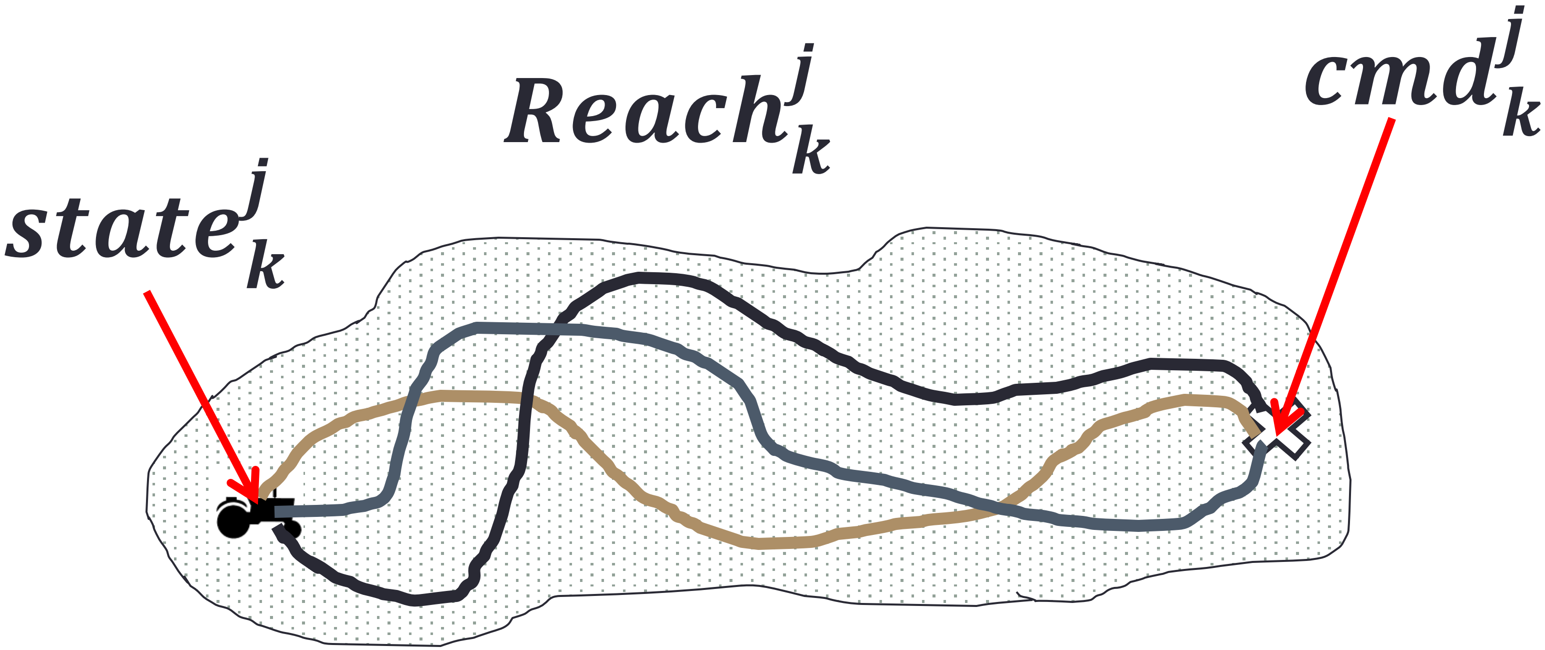


How to perform checks?

- First check that all the agents have received the last command.

How to perform checks?

- Calculate reachable set for each agent based on new and old command
- k : agent ID j: Step number



Lyapnuv inverse theorem:

- if a controller of agent Ai is locally exponentially stable with respect to a set point Si :

i. Vi is continuous
ii. Vi has value 0 only at the set point and is positive anywhere else
iii. along any trajectory of agent i, in the region of attraction, Vi is decreasing

Sub-Level

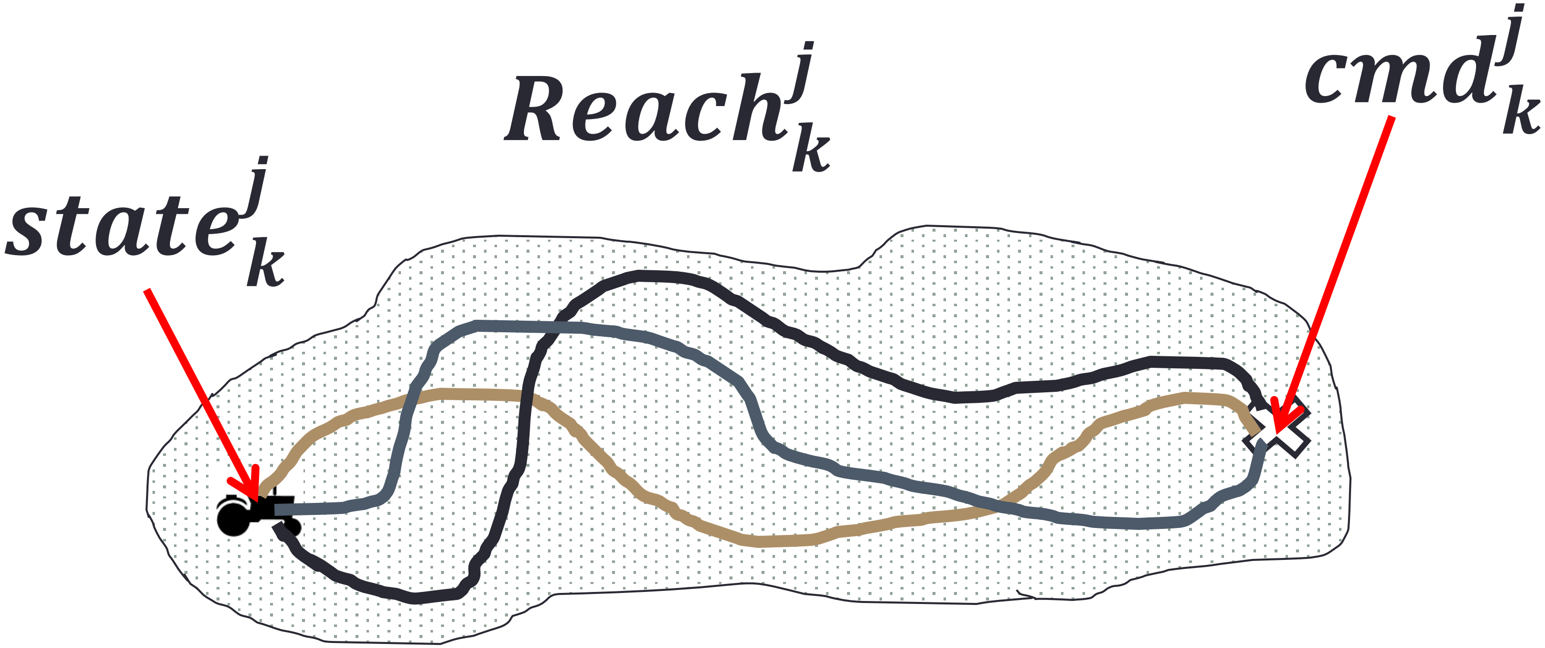
- We define sublevel set of function V as:

$$L_c(V) = \{x \in dom(V) | V(x) \leq c\}$$

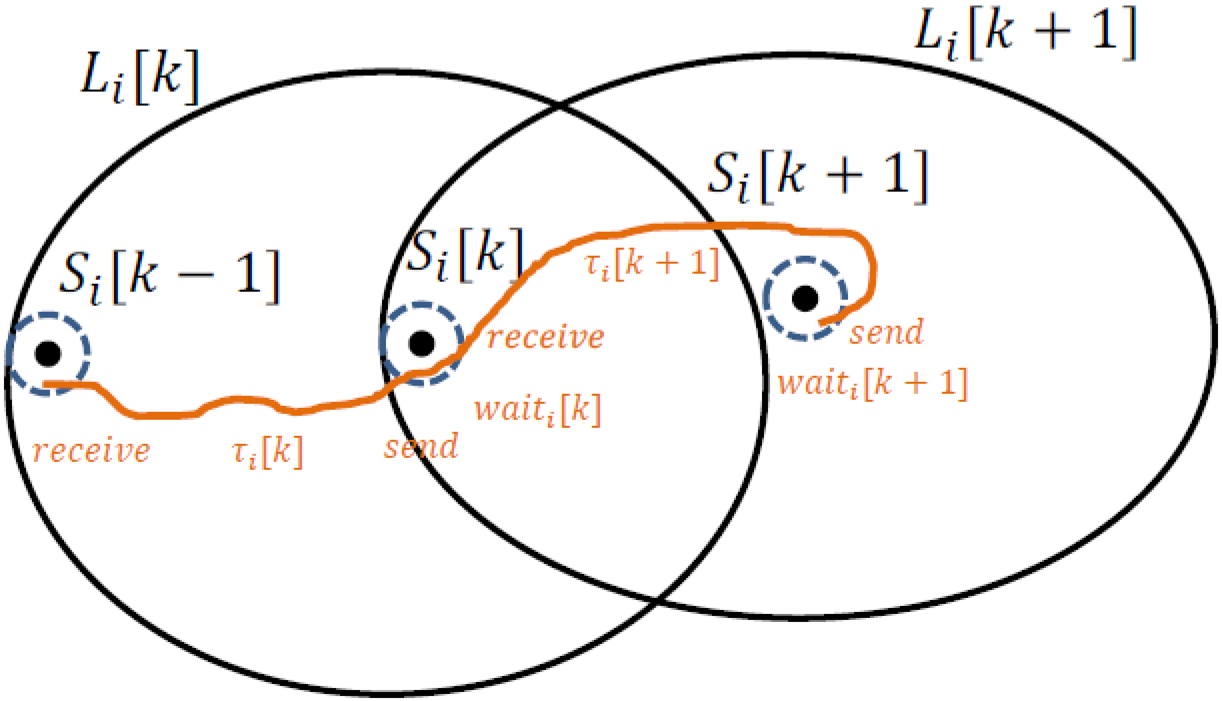
- the value of Vi should not exceed Vi(x0) Thus, the future states should remain inside the sublevel set $L_{Vi(x0)}$(Vi)of the Lyapnuv function Vi.

- Then we can use the sublevel set of Lyapunov function as an over-approximation of the reach set of Ai

Sub-level



Example

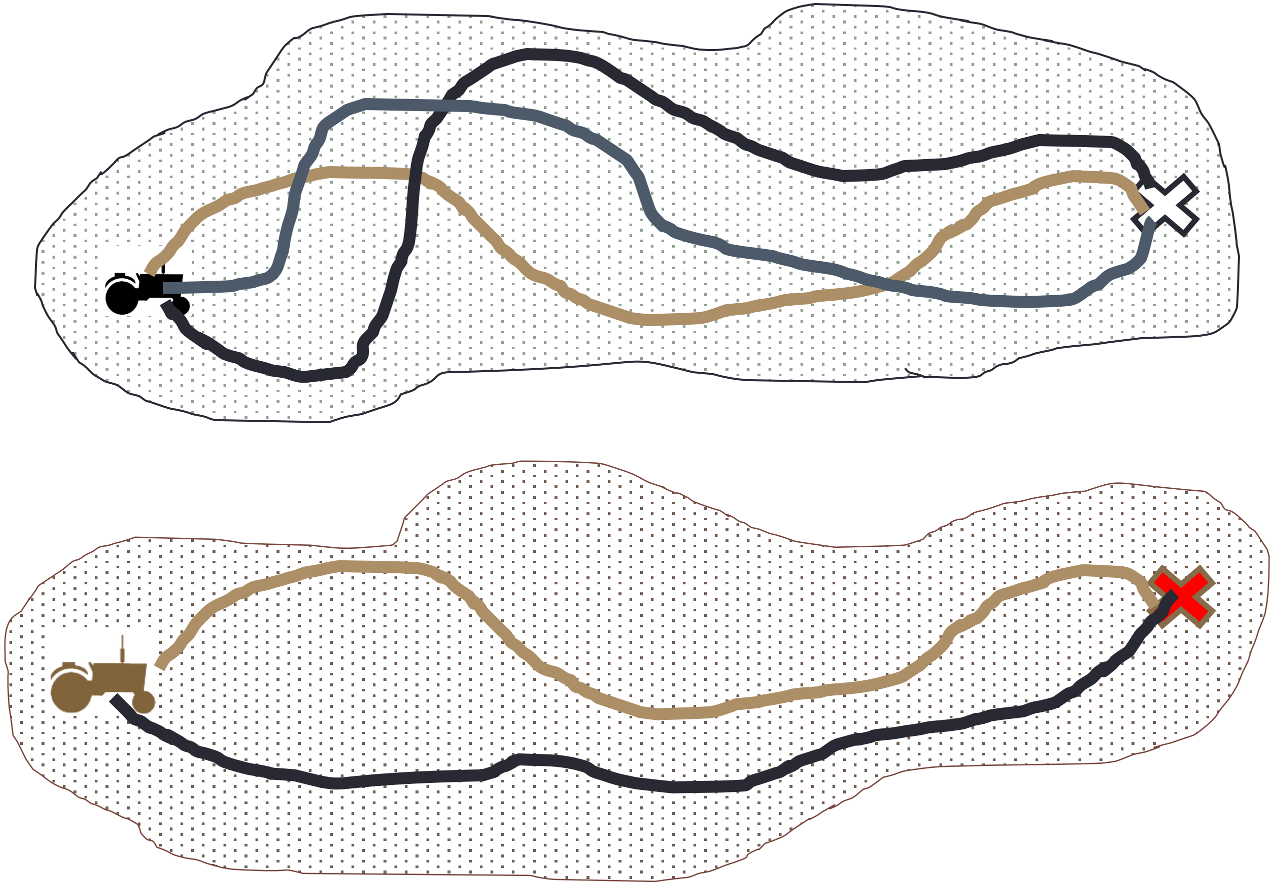

$L_i[k]$
$L_i[k+1]$
$S_i[k+1]$
$S_i[k]$
$\tau_i[k+1]$
$S_i[k-1]$
$receive$
$send$
$wait_i[k+1]$
$wait_i[k]$
$receive$
$\tau_i[k]$
$send$

- Safety:
  - Maintaining invariant P all over the execution period of the system.
- Test:
  - verify that $\forall \mathrm{k} \in [0,\mathrm{n}]$ and $\forall \mathrm{j} \in N$: $\mathbf{Reach}_{\mathbf{k}}^{\mathbf{j}}$ **satisfies the safety invariant.**

Flocking Robots

Invariant is:

No intersection between any two reachable sets.



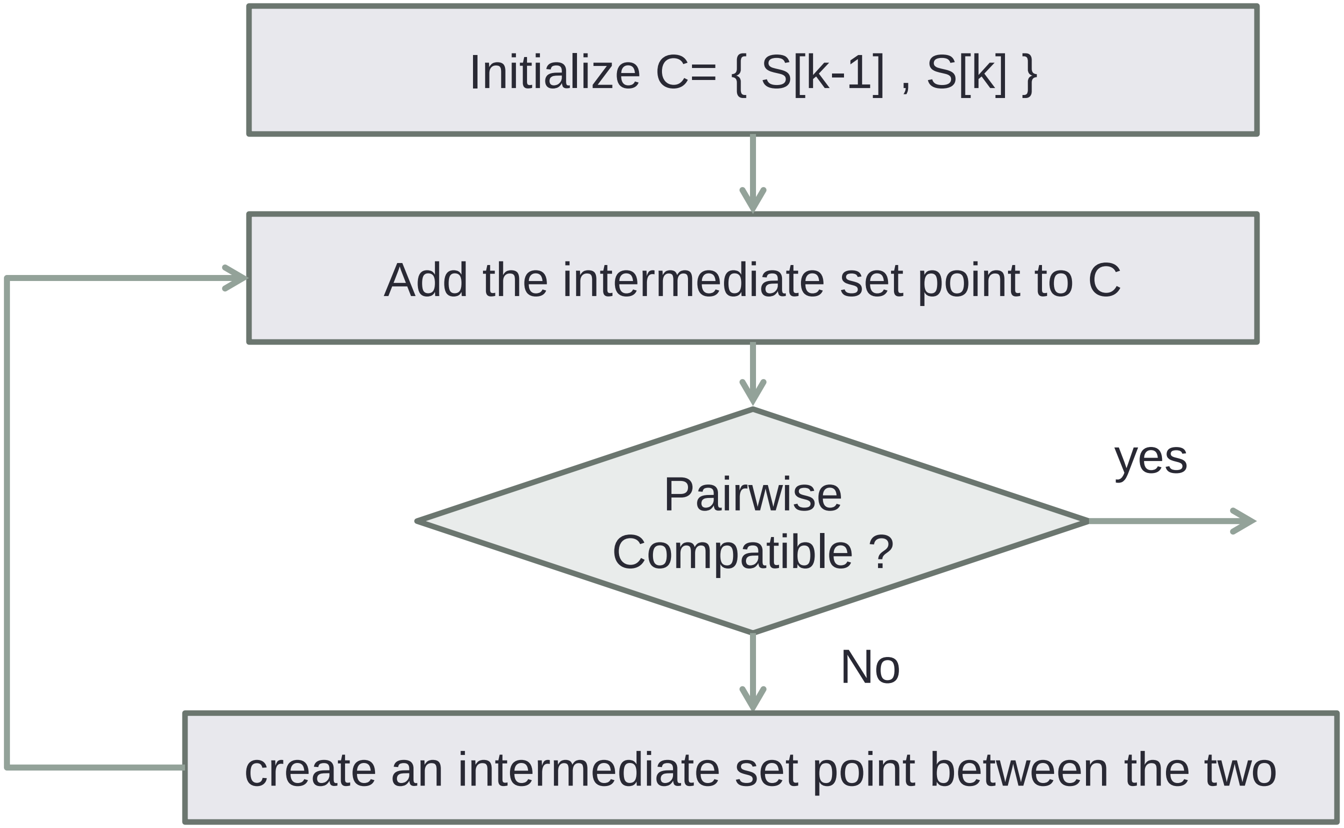
We're Safe!

☺

But, most of the time, We Wont any progress

☹

Compatible Action Chain Algorithm



Initialize C= { S[k-1] , S[k] }

Add the intermediate set point to C

Pairwise Compatible ?

yes

No

create an intermediate set point between the two

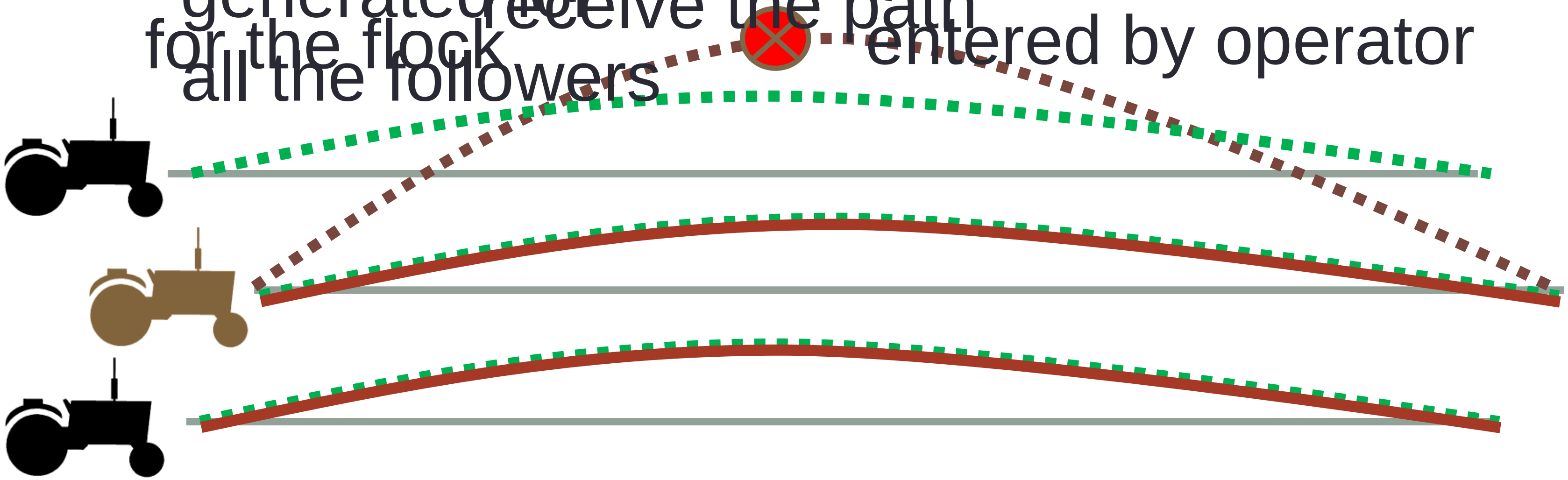
Compatible Action Chain Algorithm

- By recursively splitting pairs of set points, the reach sets can be made smaller and smaller, which increases the chance that the pair of global set points will satisfy the safety predicate PS and therefore be a pair-wise compatible action.
- Not always Convergent. If so, gives us progress guarantee.

Progress Guarantee

- If following conditions are met, we can always guarantee progress:
  1. Messages in the network can only get delayed arbitrarily long but can not be dropped
  2. There is a finite chain of pairwise compatible actions from the current state to the target global set point.
  3. Third, the local controllers for each agent are exponentially stable for each set point in the compatible action chain.

Example



Desired final path generated for the flock

Paths generated for all the followers

Paths sent to followers!

Tractor 1 did not receive the path

Tractor 1 did not receive the new path but safety is maintained!

New Detour point entered by operator

Simulation

- http://fardinabdi.com/node/13