FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Strategic Sensing and Resource Allocation for Pipeline Network Resilience

Saurabh Amin
(joint with Mathieu Dahan and Andrew C. Lee)
MIT

NSF All Hands Meeting, Berkeley
August 23-24, 2017

Berkeley
UNIVERSITY OF CALIFORNIA

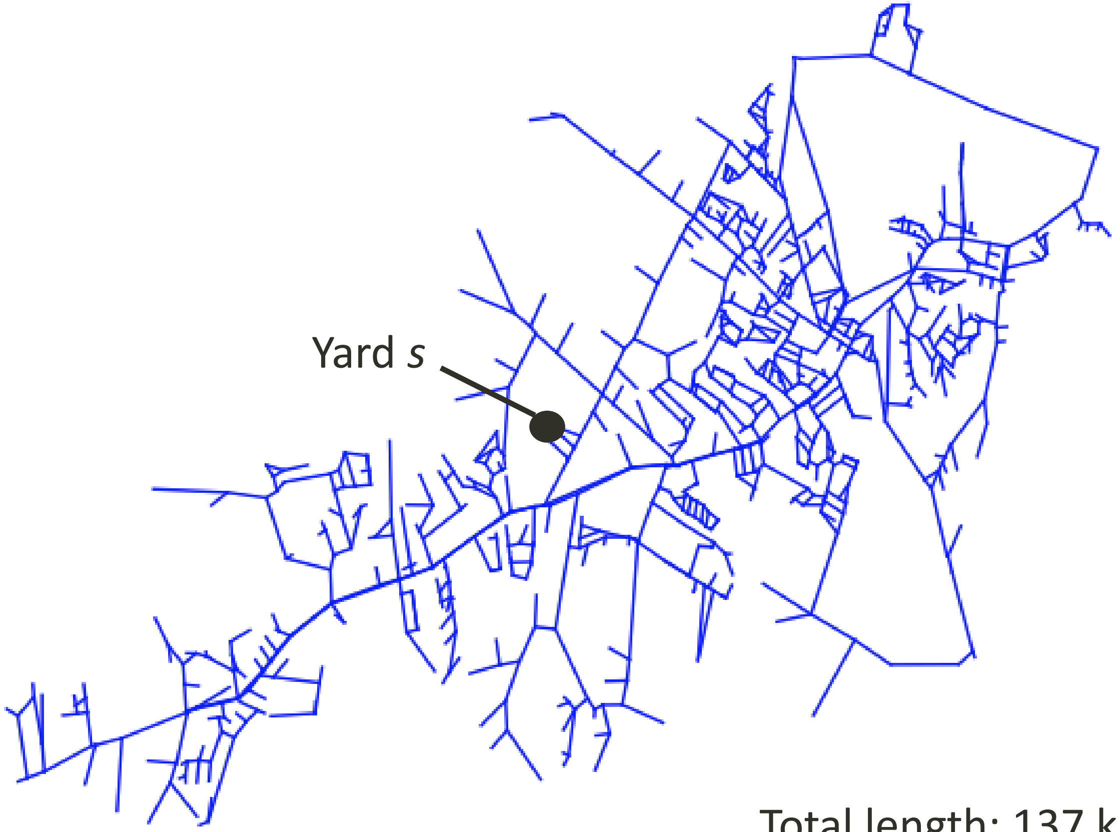
Massachusetts
Institute of
Technology

NSF

MICHIGAN

VANDERBILT
UNIVERSITY

Current Process

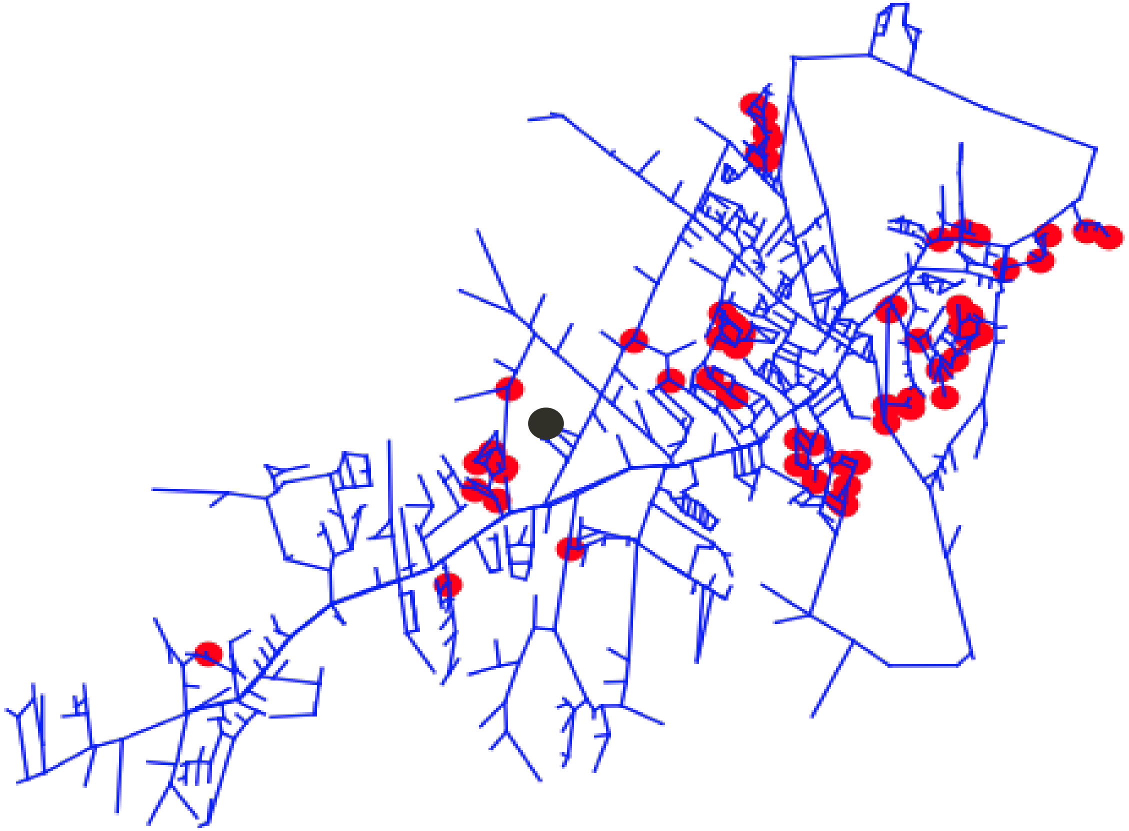


Total length: 137 km

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Current Process

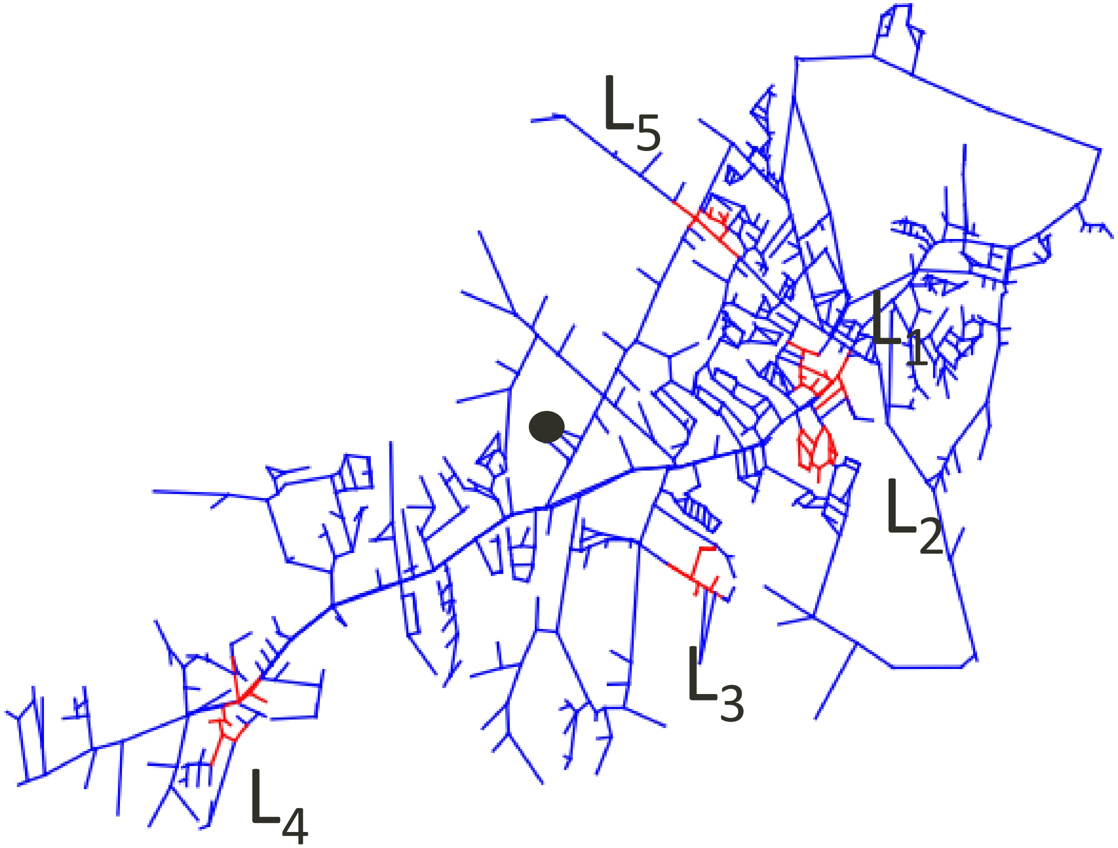
Sensors

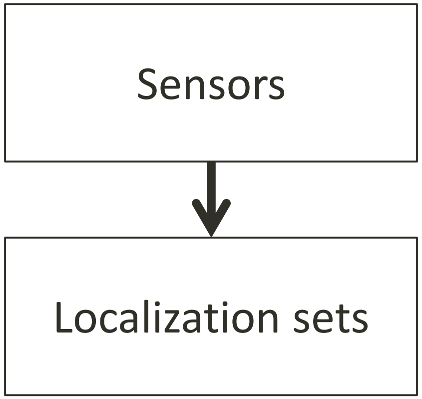


Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Amin

Current Process



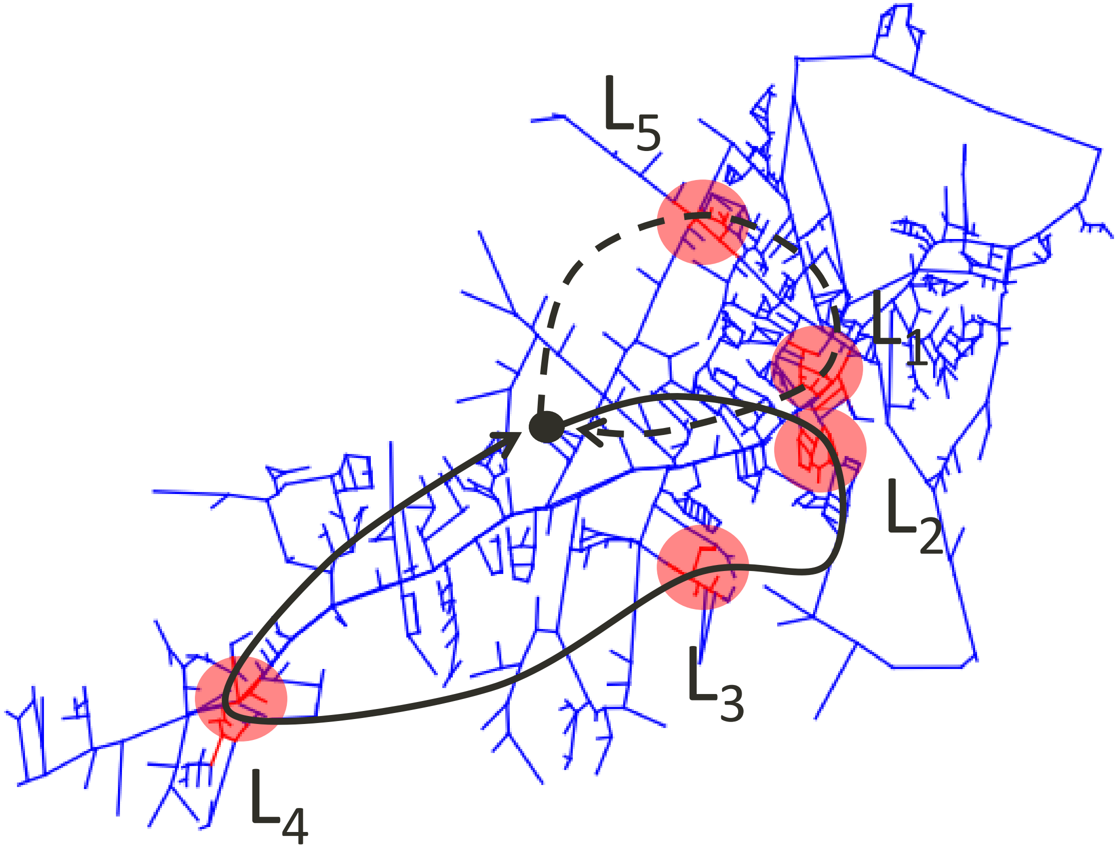


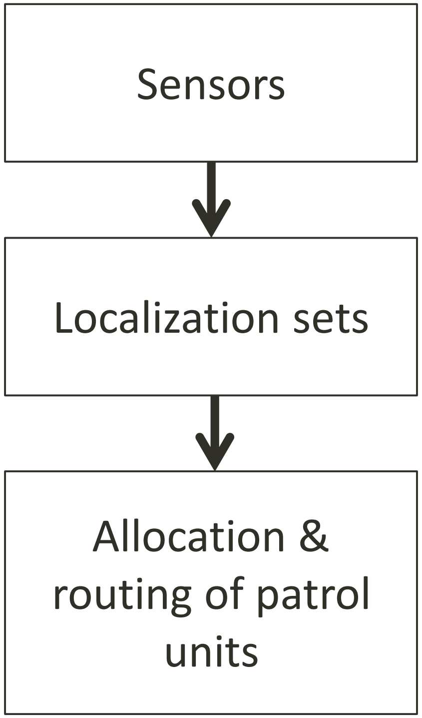
Sensors

Localization sets

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Current Process



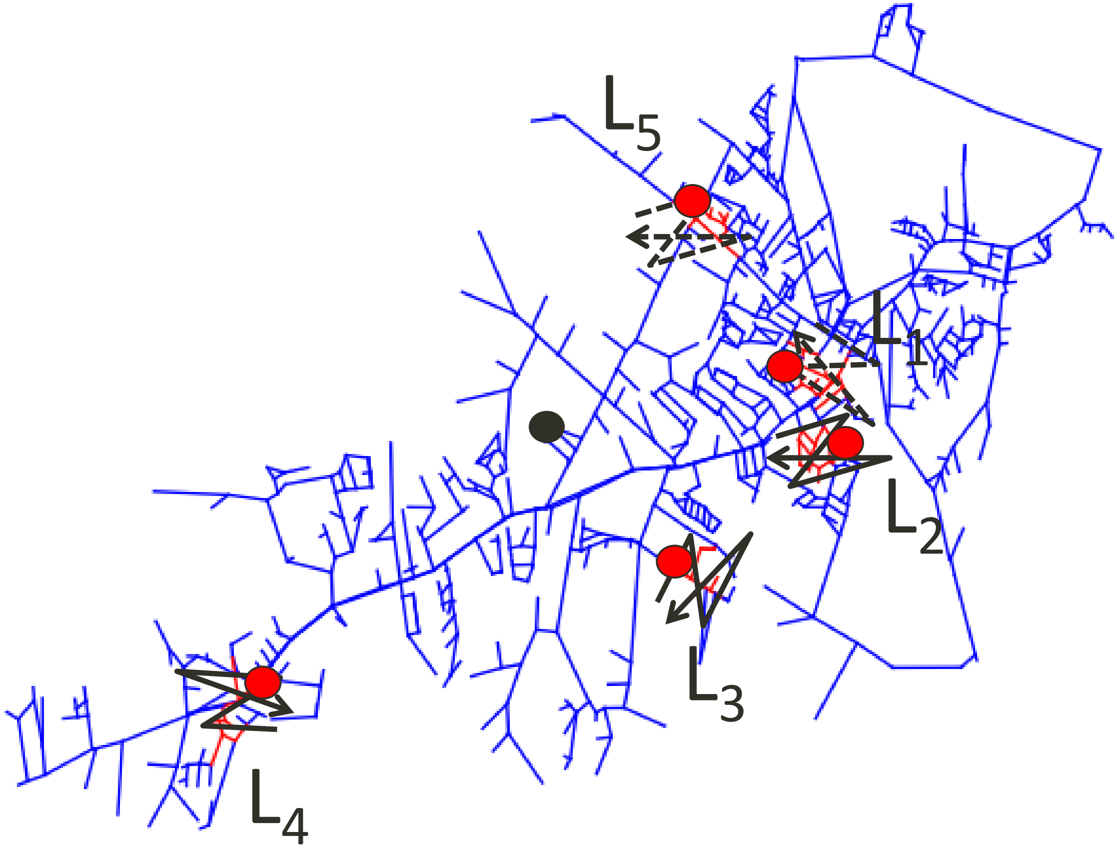

Sensors

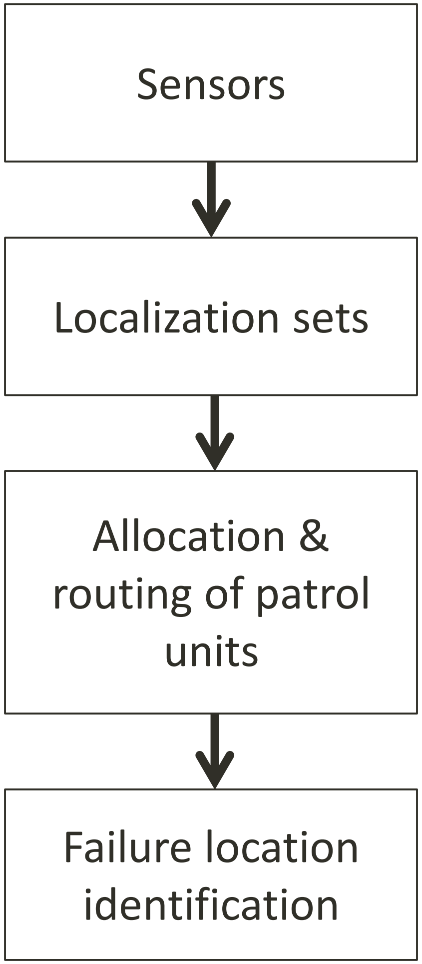
Localization sets

Allocation & routing of patrol units

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Current Process





Sensors

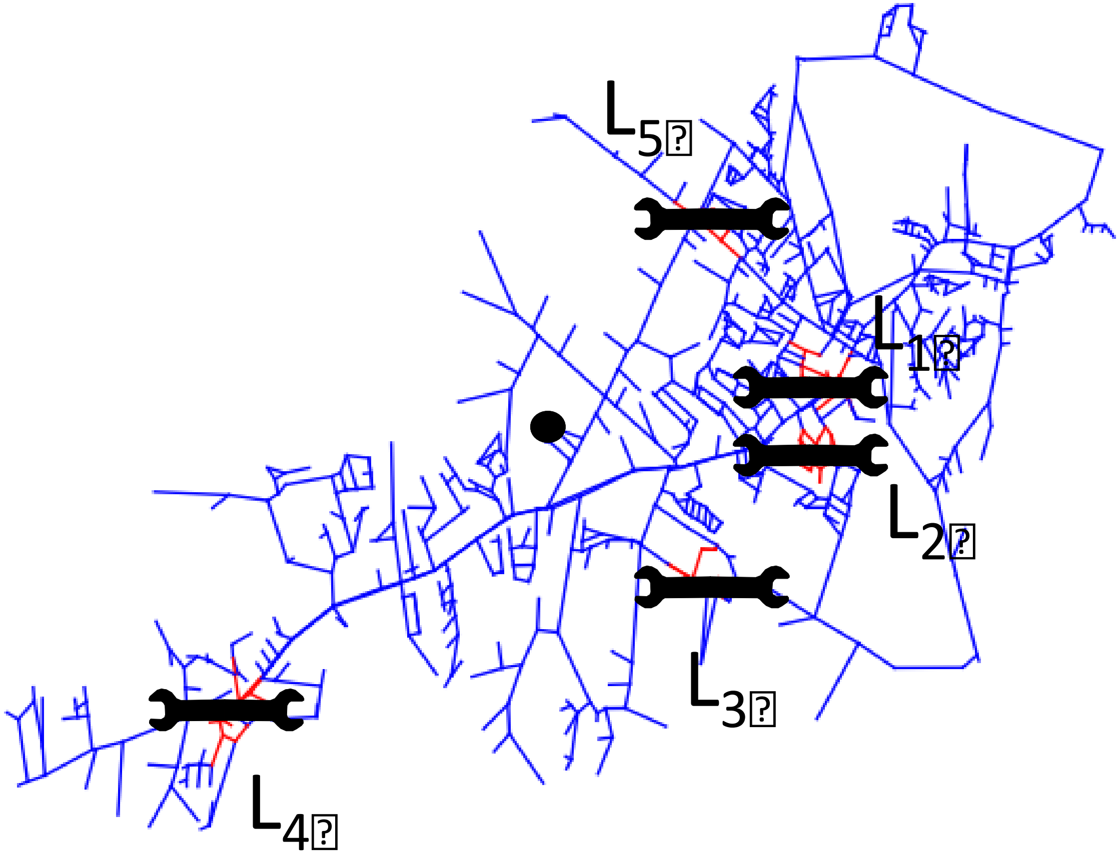
Localization sets

Allocation & routing of patrol units

Failure location identification

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Current Process



Sensors

Localization sets

Allocation & routing of patrol units

Failure location identification

Repair and restoration

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

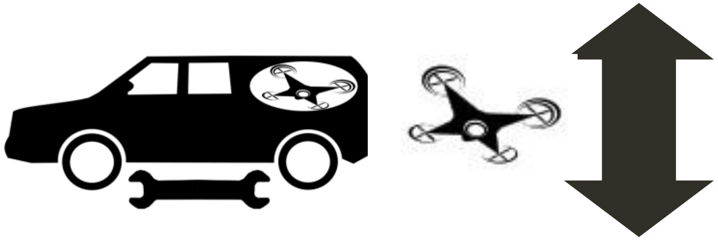
Network Monitoring and Inspection

Monitoring and Inspection	Sensing Accuracy	Scalability	Crew Dispatch	Repair	Costs	Safety
Ideal	Timely detection and precise location identification (ID)	Large-scale monitoring	Efficient dispatch, flexible	Rapid restoration	Minimal loss of resources within budget	No incidents
Current	Mis-detection, False Alarms	Limited Resources	Inefficiencies, suboptimal allocation	Priority-based	Loss of resources and human effort	Safety risks to repair crews, customers

References: PG&E 2016 Gas Safety Plan,
Angalakudati et al. "Business Analytics for Flexible Resource Allocation Under Emergencies" Management Science, 2014

Network Monitoring and Inspection

Monitoring and Inspection	Sensing Accuracy	Scalability	Crew Dispatch	Repair	Costs	Safety
Ideal	Timely detection and precise location identification (ID)	Large-scale monitoring	Efficient dispatch, flexible	Rapid restoration	Minimal loss of resources within budget	No incidents
Current	Mis-detection, False Alarms	Limited Resources	Inefficiencies, suboptimal allocation	Priority-based	Loss of resources and human effort	Safety risks to repair crews, customers



How to use modern sensing technologies (static and mobile sensors) help bridge this gap?

References: PG&E 2016 Gas Safety Plan,
Angalakudati et al. “Business Analytics for Flexible Resource Allocation Under Emergencies” Management Science, 2014

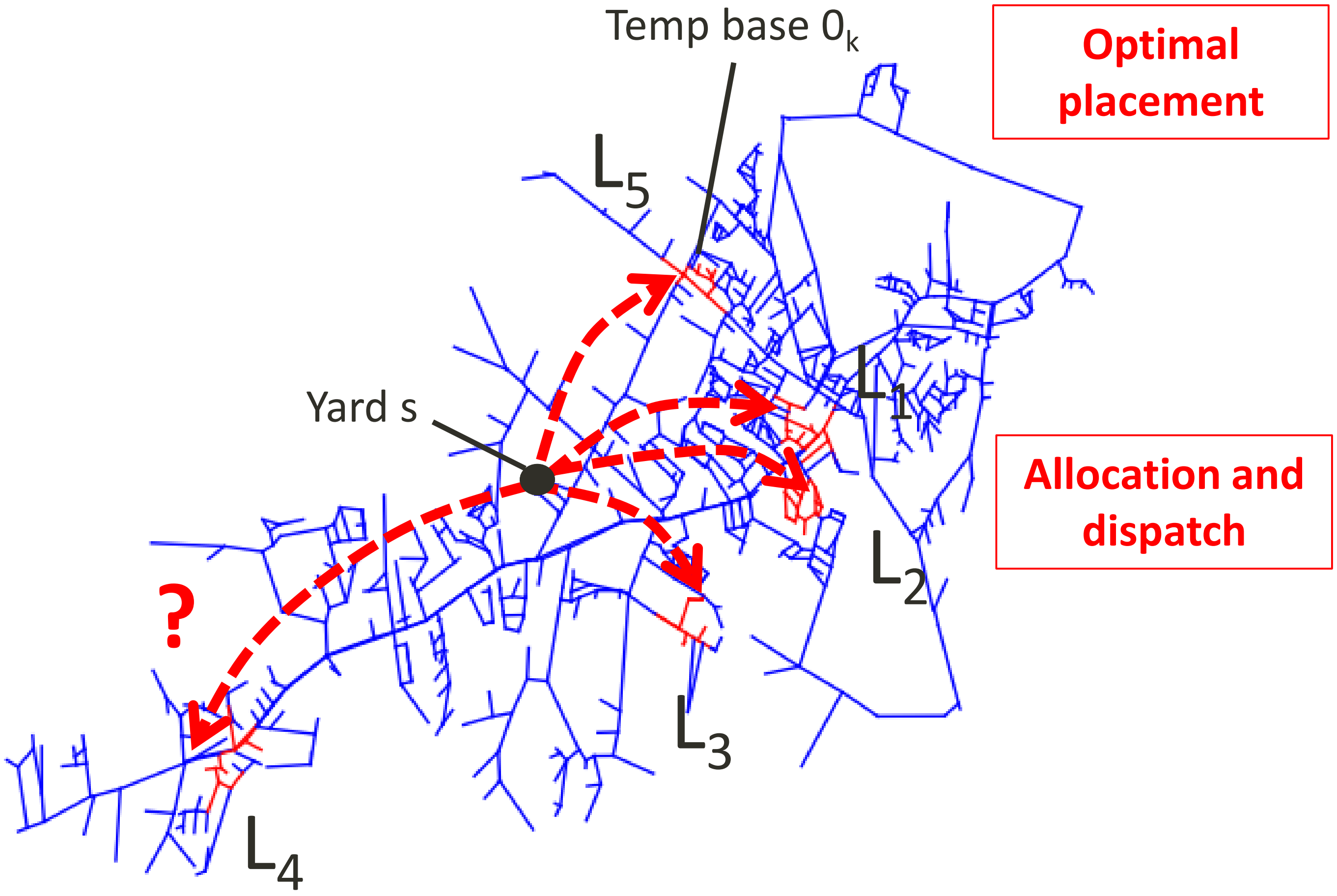
FORCES research

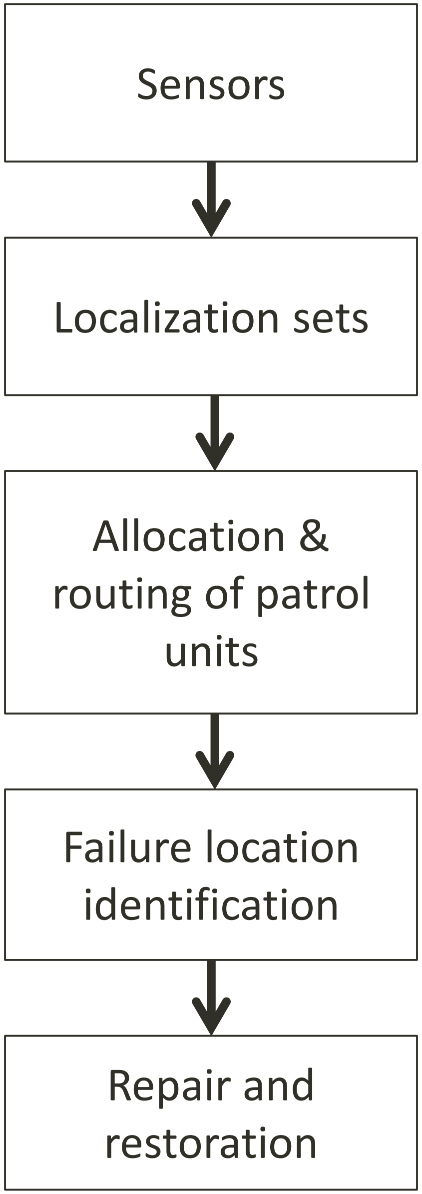
Numerous applications in oil and gas industry

- Optimal sensor placement for failure diagnostics
- UAS-enabled sensing and inspection
- Resilient control in the face of disruptions
- Analytics driven failure models of critical assets

- Related issues:
  - Incentives for utility (regulated monopolist) in investing in monitoring technology and resources
  - Cyber-physical security attacks

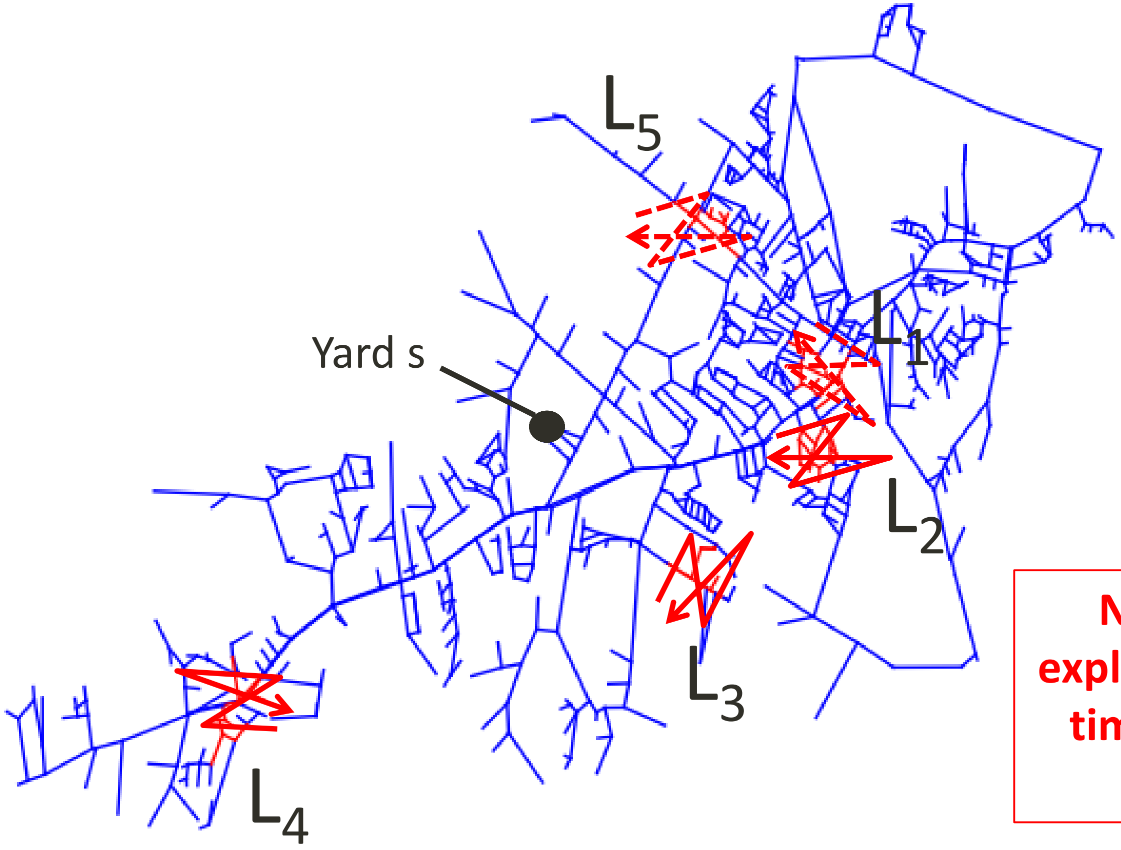
This talk





Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

This talk



Network exploration for timely ID of failure

Sensors

Localization sets

Allocation & routing of patrol units

Failure location identification

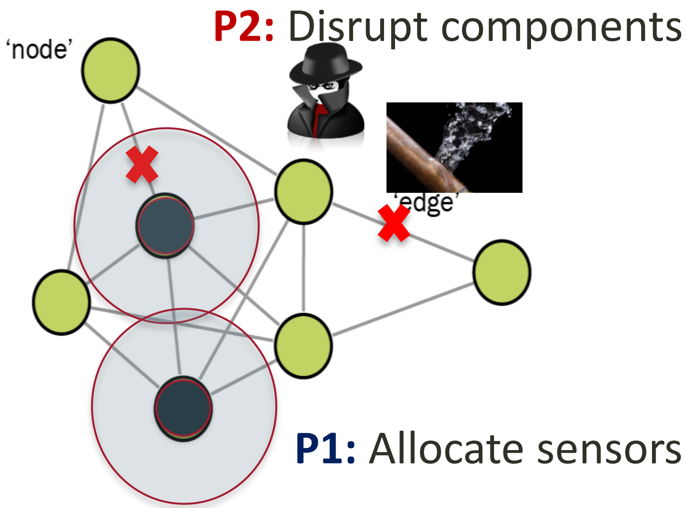
Repair and restoration

Reference: PG&E 2016 Gas Safety Plan, Asset Knowledge & Integrity Management Earthquake Playbook 2015

Monitoring large-scale networks facing disruptions

- Resource allocation problem for monitoring infrastructure networks facing disruptions (both random & adversarial)
- **Students**: Mathieu Dahan (CSE PhD), Andrew Lee (TR PhD)
- **FORCES collaborators**: Lina Sela, Waseem Abbas, Xenofon Koutsokos
- **Papers**: Automatica 16, ACM BuildSys 16, Allerton 16, ICCPS 17, ICUAS 17, Submitted to Operations Research
- **Industry collaboration**: 3 LGO Students interned at PG&E and 1 LGO student interning at National Grid
- **(Potential) Impact**:
  - Allocation and tasking of sensing systems to identify failures and minimize time to repair in large-scale water and gas networks
  - PG&E's seismic damage prediction model by incorporating dynamic information from sensing systems and response crews

Monitoring large-scale networks facing disruptions



- **Key features**
- Strategic interaction
- Resource limitations
- Very large (combinatorial) action sets
- Dynamic and asymmetric information

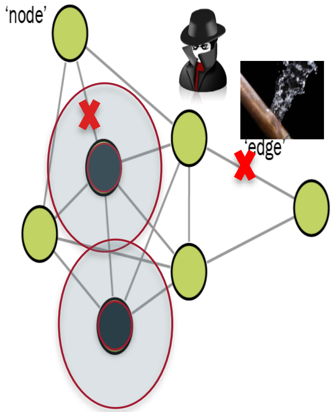
Example settings

- Hide-and-seek games
- Network security
- Search and surveillance
- **Infrastructure defense**

Our focus: Allocation of sensing resources in adversarial environments

- Incorporate a generic sensing model
- Ensure desirable performance guarantee (detection rate)
- Compute optimal (equilibrium) allocation

Network monitoring problem under strategic disruptions



- Large-scale infrastructure network facing strategic disruptions (attacks)
- Sensing model: detect or not based on location of sensor and components
- Attacker: simultaneous edge disruptions
- Operator: (random) sensing over subset of nodes
- **Objective**: Maximize # of detections (operator)
  Maximize # of undetected events (attacker)

Question: How many sensors are required and how to strategically allocate them in the network to detect adversarial attacks?

Formulation: Mathematical Program with Equilibrium Constraints (MPEC)

Minimize # of number of sensors to guarantee that

- Expected detection rate > threshold in *any* equilibrium of induced game
- Find an equilibrium

Our approach

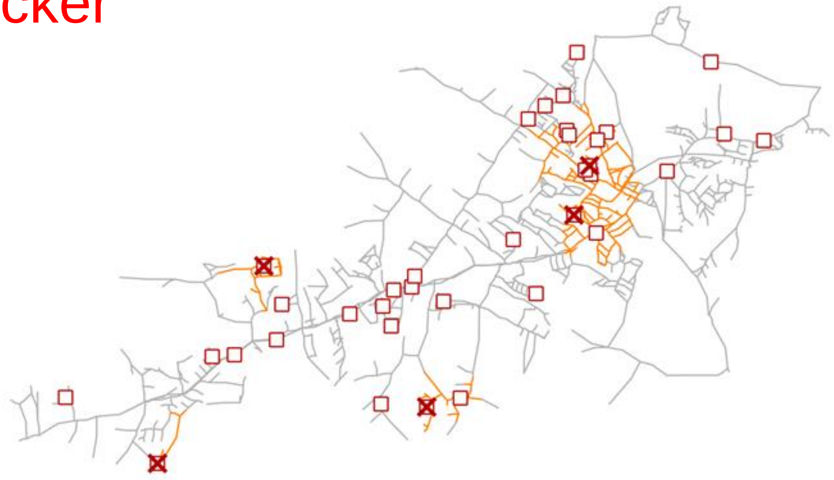
- Study equilibrium properties of operator-attacker game
- Construct an ε-Nash equilibrium based on solutions of
  - Minimum Set Cover [MSC] problem: operator strategy is to randomize over MSC
  - Maximum Set Packing [MSP] problem: attacker strategy is to randomize over MSP
- Compute an approximate solution of the MPEC:
  - # of sensors with optimality gap
  - Guarantee(s) on detection performance

Main advantages:

- Scalable to very large networks
- Small optimality gap in most practical cases
- When |MSC|=|MSP|: We obtain an exact solution, and generalize some classical results on hide-and-seek and network security games
- Does not require an exact knowledge of the attacker's resources

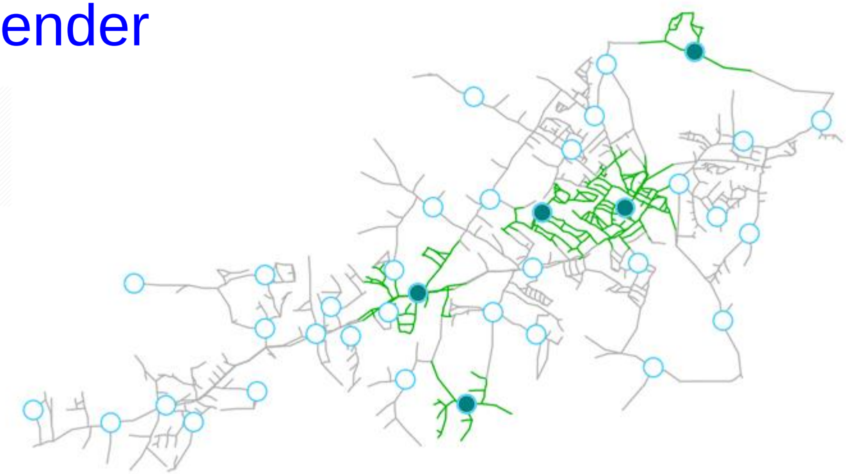
MSC-MSP based strategy profile

Attacker



□ MSP: maximum set of links that are covered by any node at most once

Defender



○ MSC: minimum set of nodes that cover all edges

Main ideas

- **Main case of interest:** large network and limited resources
- (# of sensing resources) < |MSC| *and* (# of attack resources) < |MSP|
- **Two tools:**
- Strategic equivalence of zero-sum games
  - Linear programming (LP) duality, but LPs are too large to compute NE
- MSC (coverage) and MSP (spread)
  - Weak duality; Both problems can be solved using integer programs

Three techniques:

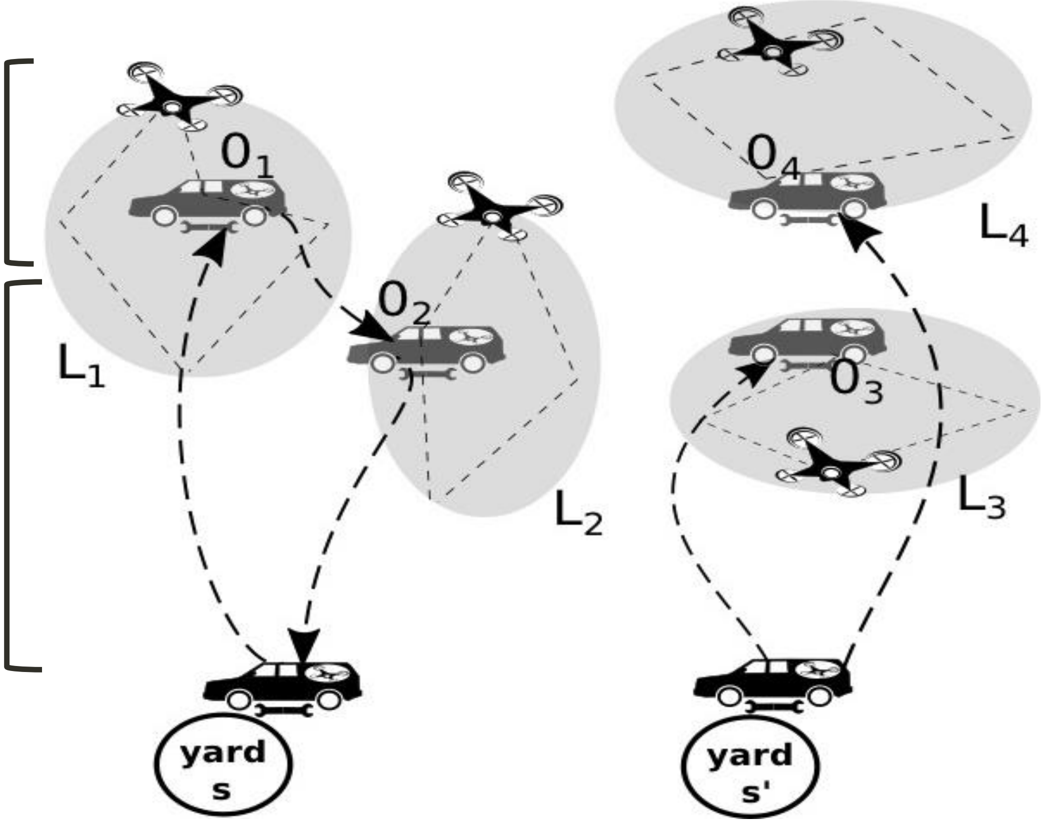
- Construct MSC-MSP based strategy profile
- Exploit properties of sensing model:
  - Monotone submodular (with respect to sensor placements)
  - Additive (with respect to attacks)
- NE properties
  - Both players necessarily randomize
  - Each player uses all available resources
  - Sensing strategies in equilibrium “cover” the entire network

Tasking mobile sensors for network monitoring

How to optimally allocate and route mobile sensing systems to identify failures within localization sets, to minimize the worst case identification time subject to constraints?

sUAS Network Exploration Problem (**SNEP**)

Repair Vehicle Routing Problem (**RVRP**)



Sensors

Localization Sets

RVRP Allocation and Routing of Patrols

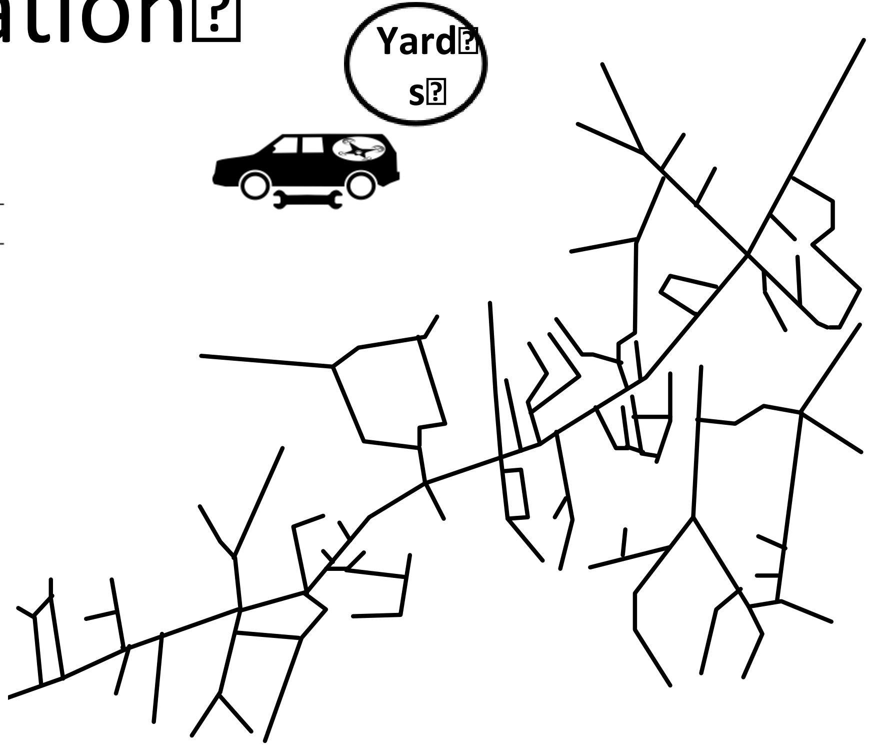
SNEP Failure ID using sUAS

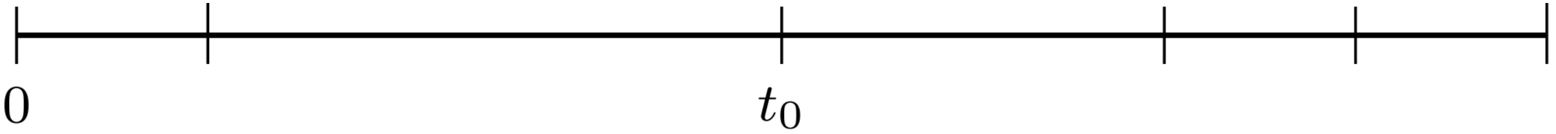
Failure Repair

Illustration

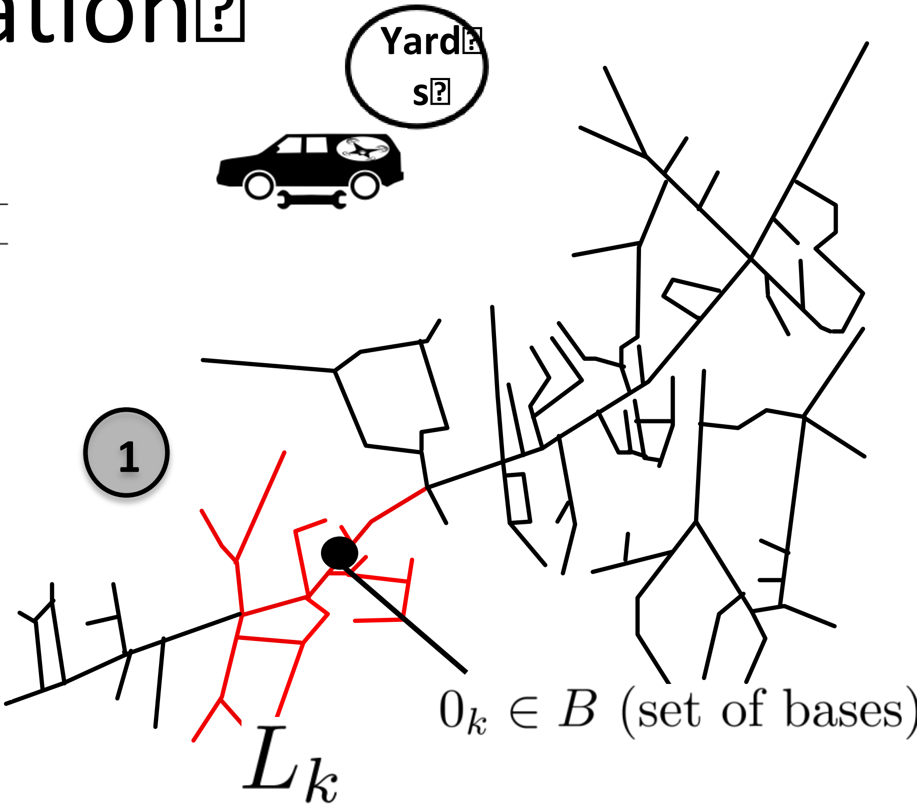
Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$

$s \in S$ (set of yards)

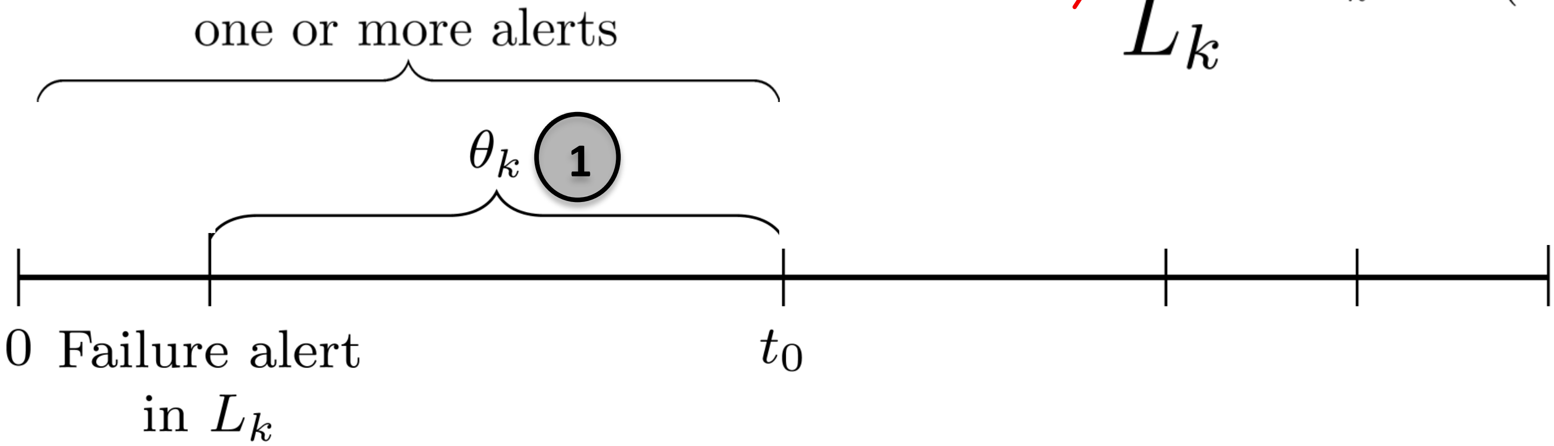




Illustration

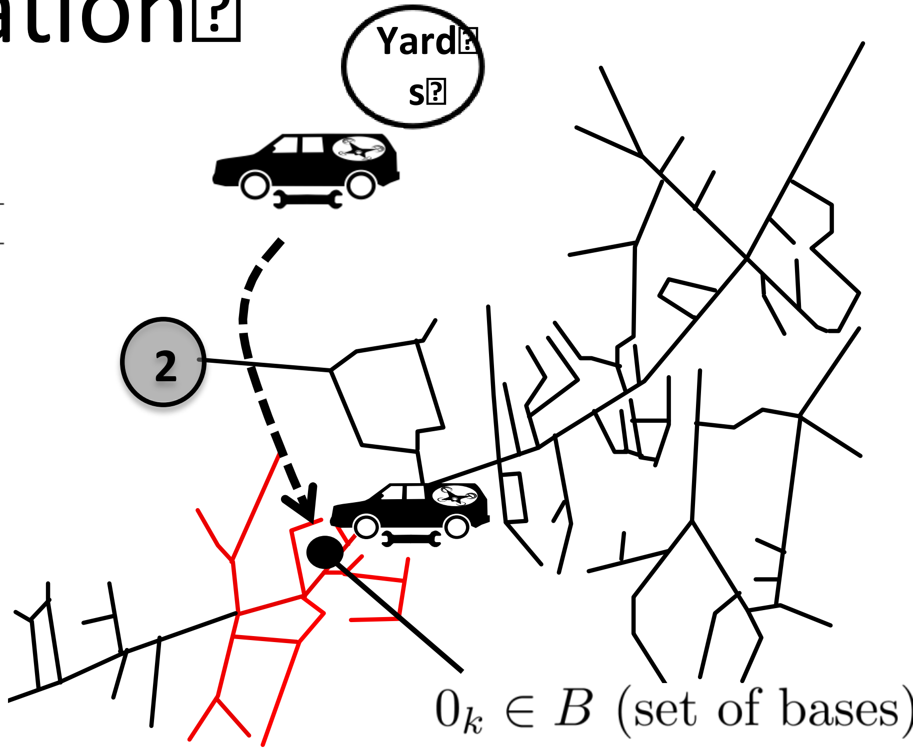


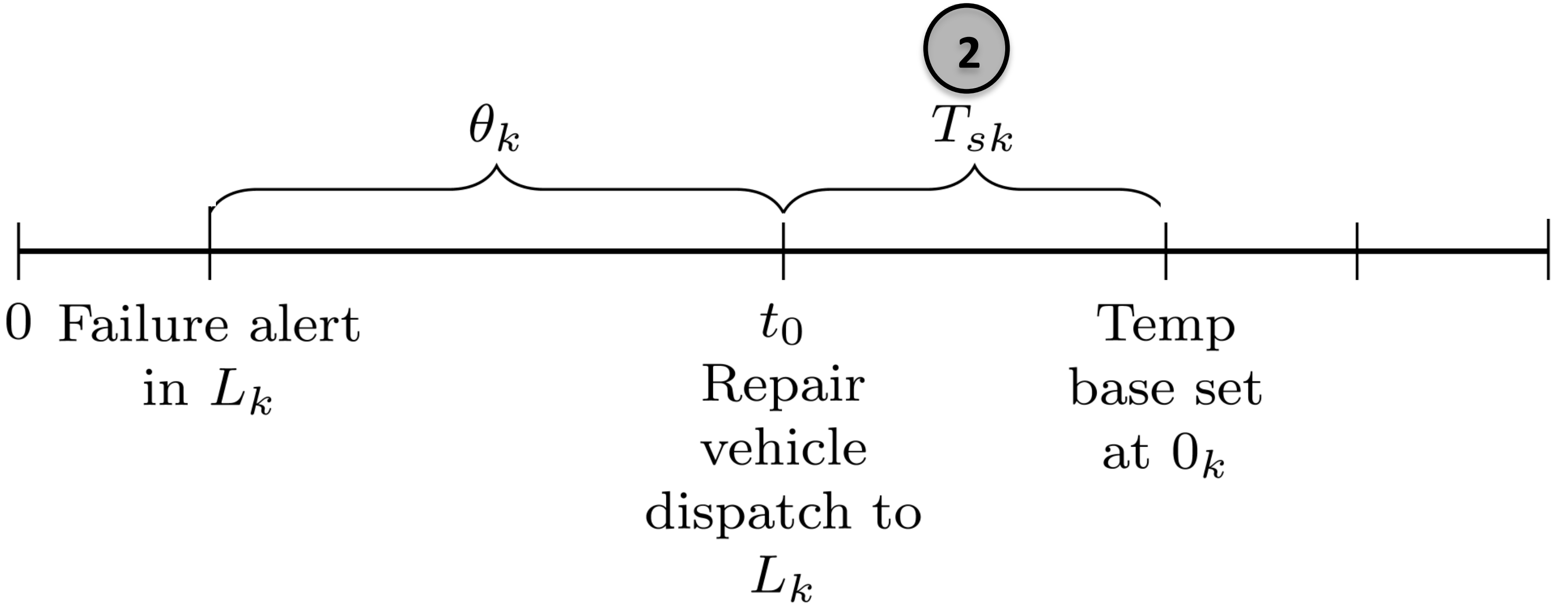
Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$
B	Set of temporary bases
L_k	Localization set k, $k \in B$
θ_k	Time since failure alert in L_k to t_0



Illustration

Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$
B	Set of temporary bases
L_k	Localization set k, $k \in B$
θ_k	Time since failure alert in L_k to t_0
T_{sk}	Time at which repair vehicle arrives at location 0_k, from s





θ_k

T_{sk}

0

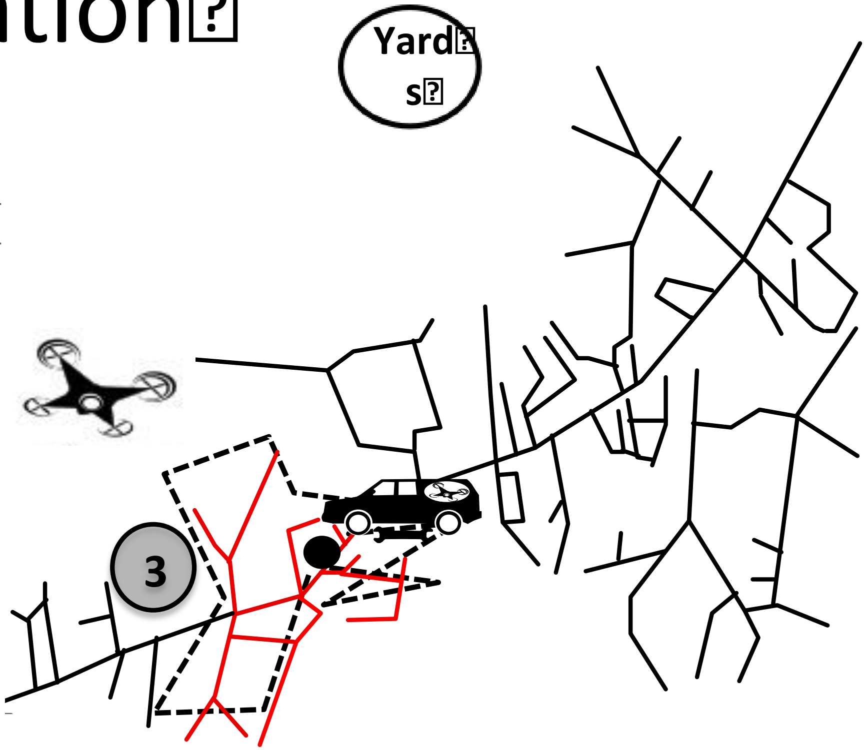
Failure alert in L_k

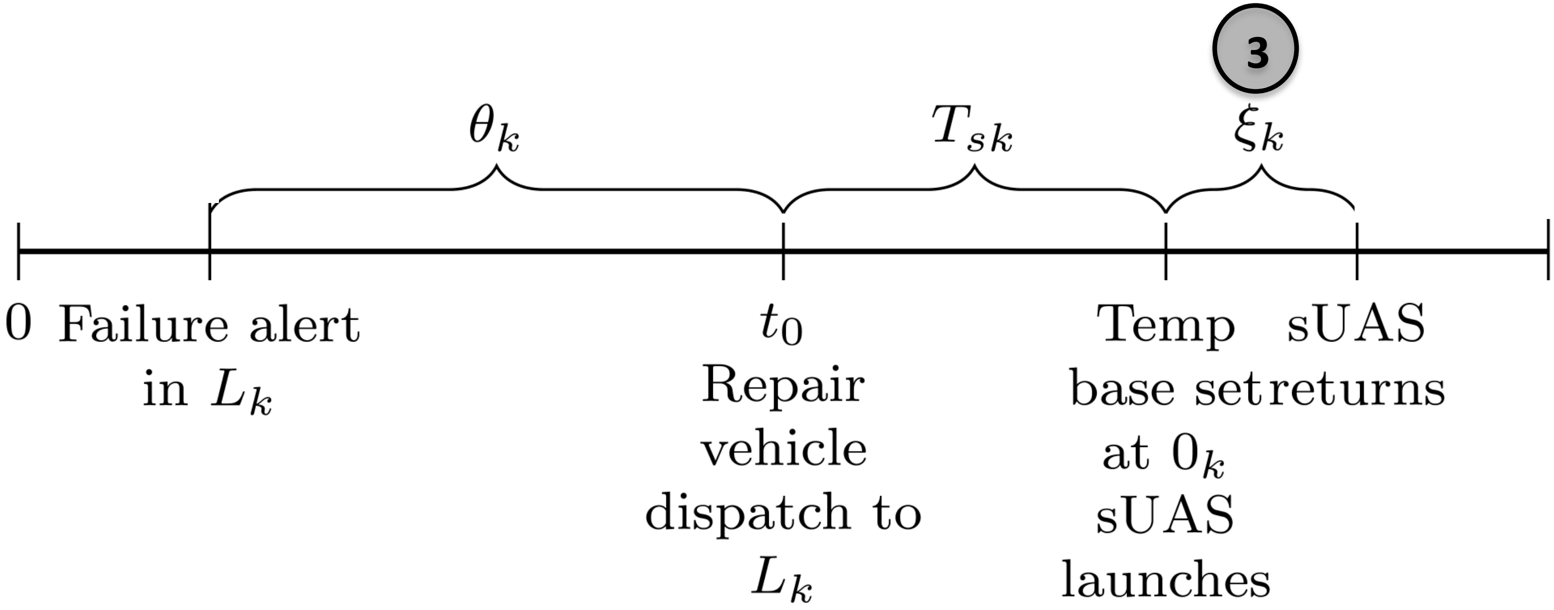
t_0 Repair vehicle dispatch to L_k

Temp base set at 0_k

Illustration

Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$
B	Set of temporary bases
L_k	Localization set k, $k \in B$
θ_k	Time since failure alert in L_k to t_0
T_{sk}	Time at which repair vehicle arrives at location 0_k, from s
0_k	Temporary base location at L_k
ξ_k	sUAS exploration time of L_k





0 Failure alert in L_k

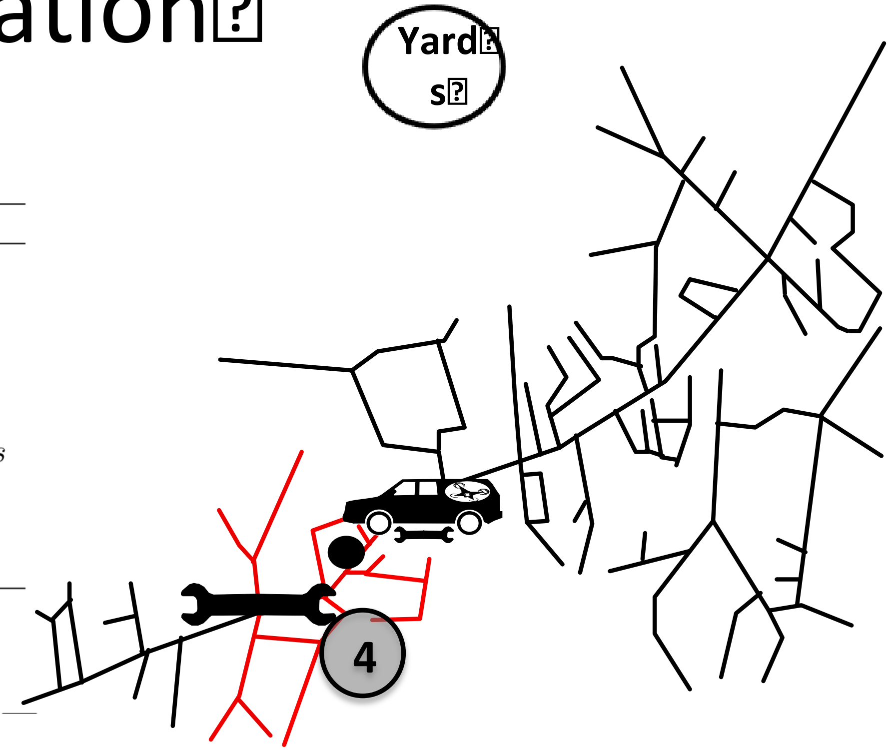
t_0 Repair vehicle dispatch to L_k

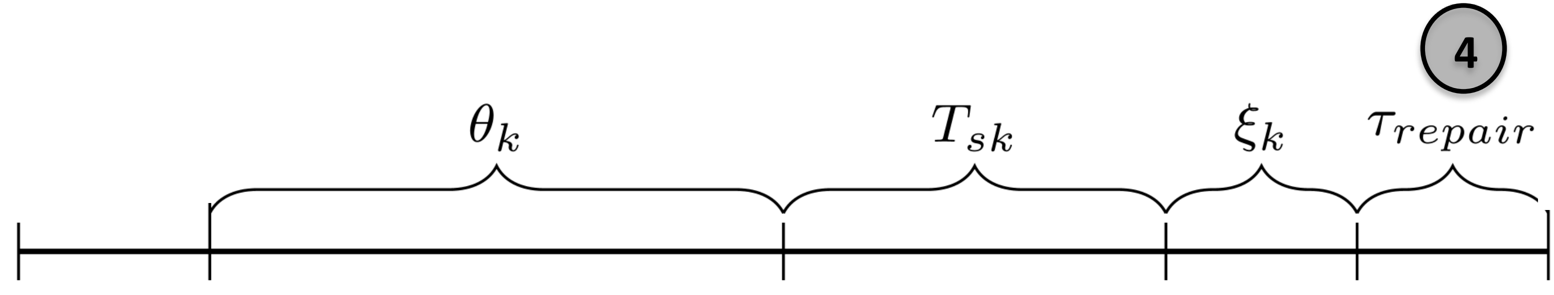
Temp base set at 0_k sUAS launches

sUAS returns

Illustration

Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$
B	Set of temporary bases
L_k	Localization set k, $k \in B$
θ_k	Time since failure alert in L_k to t_0
T_{sk}	Time at which repair vehicle arrives at location 0_k, from s
0_k	Temporary base location at L_k
ξ_k	sUAS exploration time of L_k
τ_{repair}	Time to repair





θ_k T_{sk} ξ_k τ_{repair}

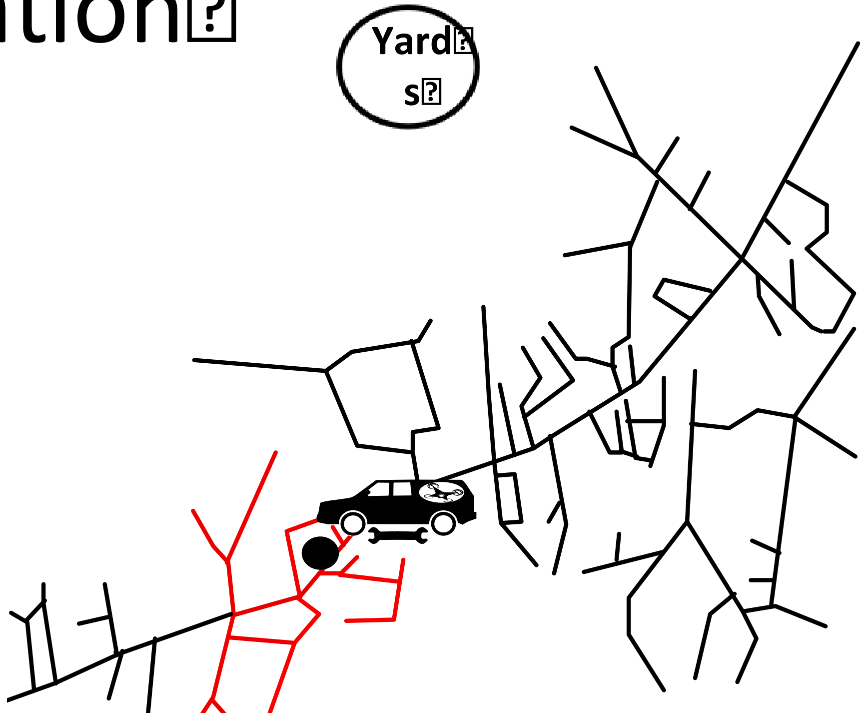
0 Failure alert in L_k

t_0 Repair vehicle dispatch to L_k

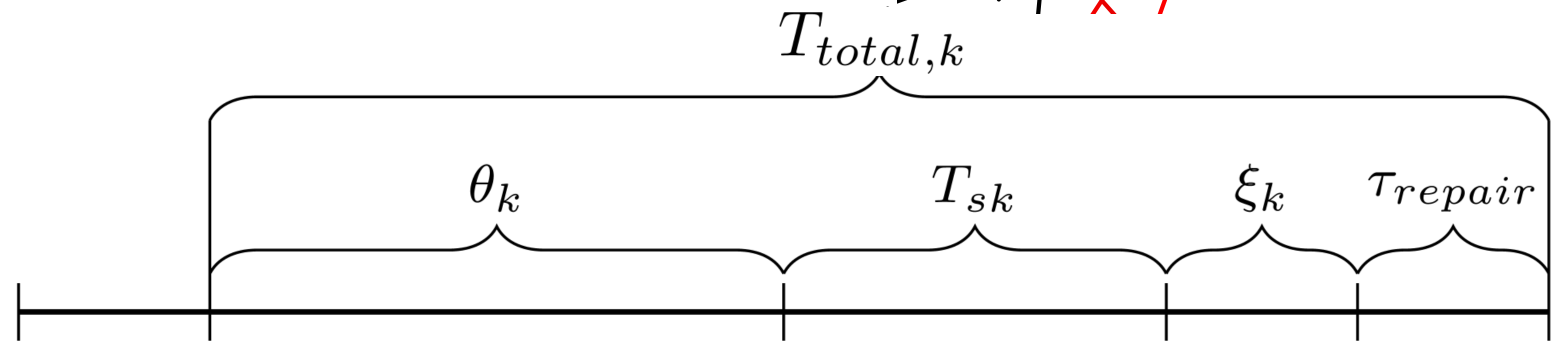
Temp base set at 0_k sUAS launches

sUAS returns

Illustration



Notation	Definition
t_0	Time of dispatch
S	Set of all yards, $s \in S$
B	Set of temporary bases
L_k	Localization set k, $k \in B$
θ_k	Time since failure alert in L_k to t_0
T_{sk}	Time at which repair vehicle arrives at location 0_k, from s
0_k	Temporary base location at L_k
ξ_k	sUAS exploration time of L_k
τ_{repair}	Time to repair



0

Failure alert in L_k

t_0 Repair vehicle dispatch to L_k

Temp base set at 0_k sUAS launches

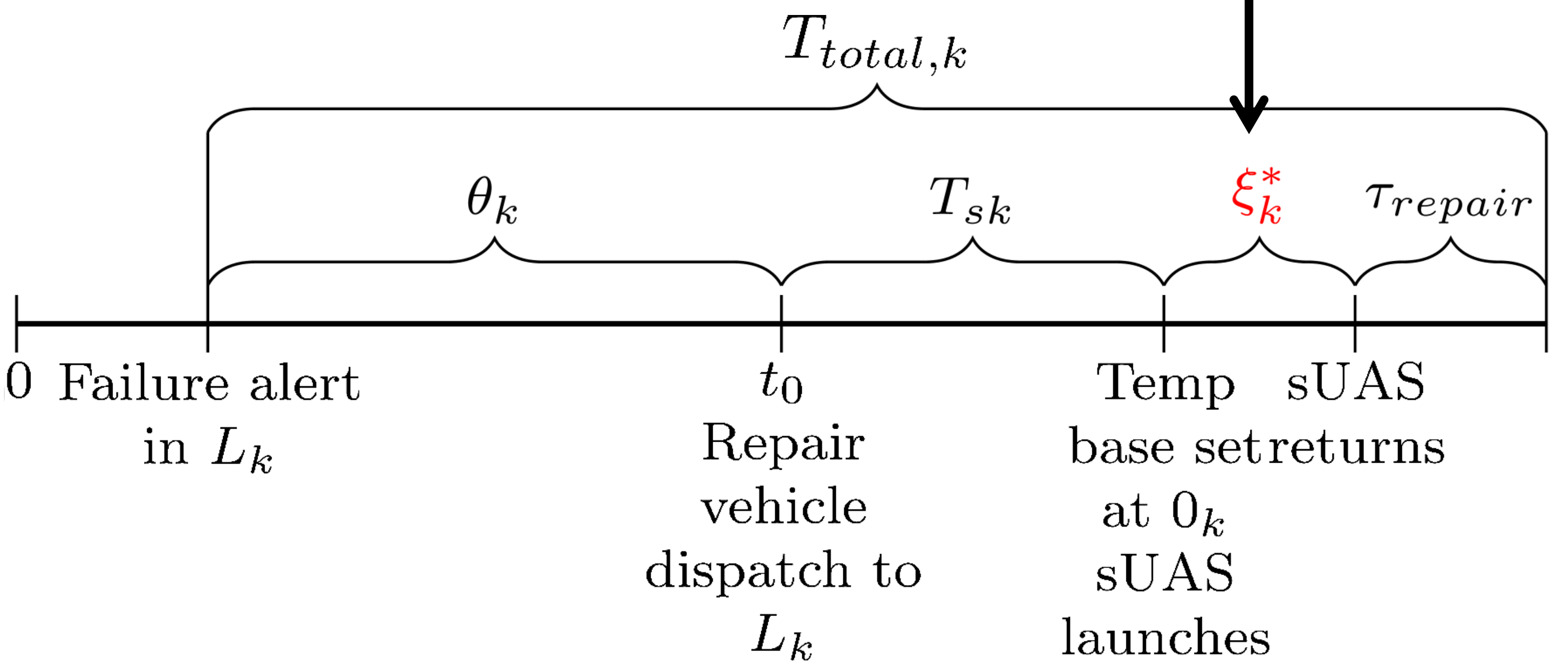
sUAS returns

Two Problems

Repair Vehicle
Routing Problem
(**RVRP**)

$$\underset{X,T}{\text{minimize}} \quad \underbrace{\max_{k\in B}\left(\theta_k + T_{sk} + \xi_k + \tau_{repair}\right)}_{T_{worst}}$$

sUAS Network
Exploration
Problem (**SNEP**)



Formulation for the RVRP

Find optimal route(s) for the repair vehicle(s) to the localization sets.

- **Objective:** Minimize the maximum amount of time elapsed from time of failure alert to time of repair among all localization sets

---

$$\underset{X,T}{\text{minimize}} \quad \overbrace{\max_{k\in B} \left(\theta_k + \left(\sum_{l\in B\cup S\setminus\{k\}} T_{lk}\right) + \xi_k^* + \tau_{repair}\right)}^{T_{worst}}$$

T_{lk}: Time at which repair vehicle arrives at location 0_k from 0_l

X_{lk}^{s}: 1 if a repair vehicle from yard s goes from 0_l to 0_k, 0 otherwise

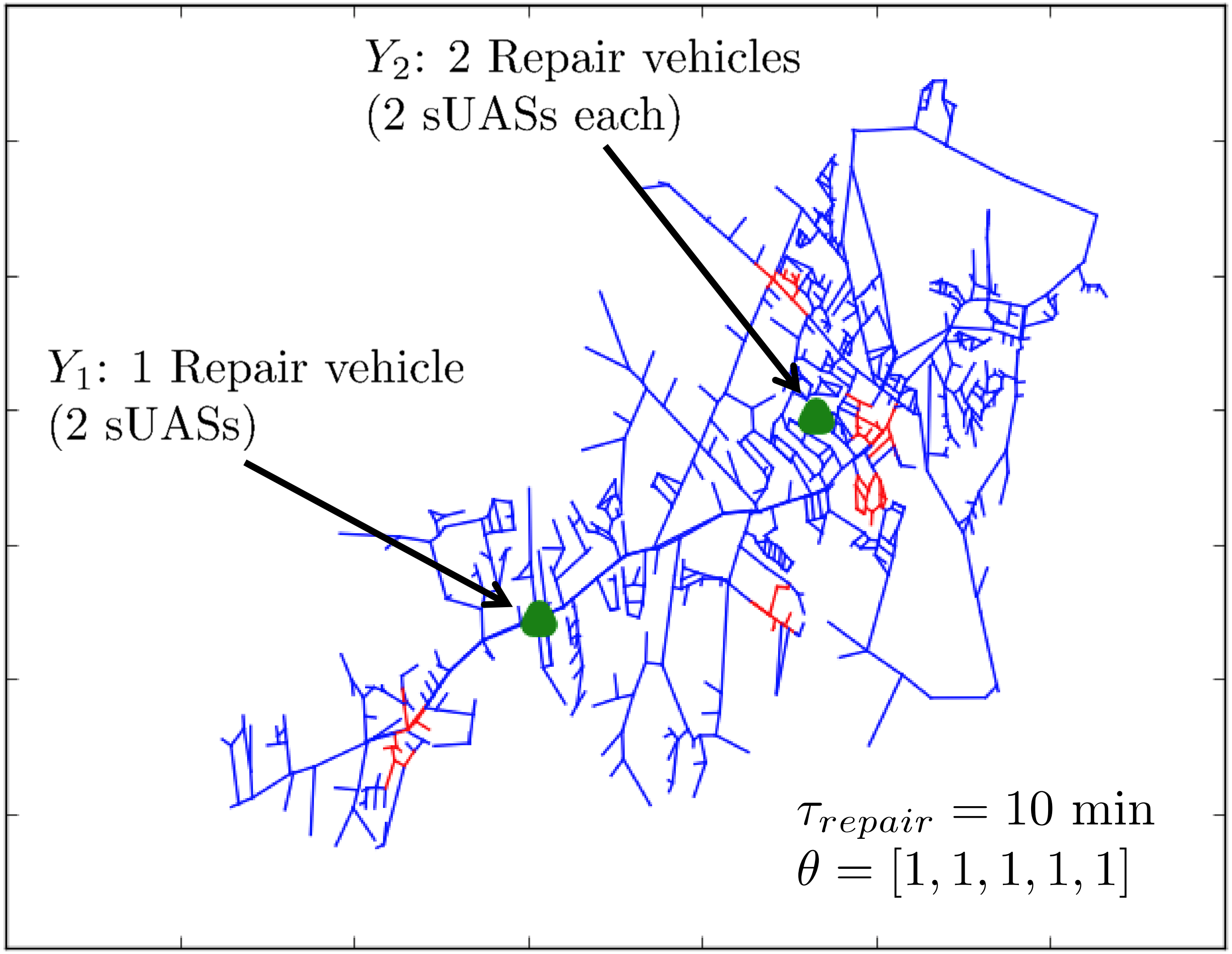
RVRP

- Objective: Minimize the maximum amount of time elapsed from time of failure alert to time of repair among all localization sets
- Subject to:
  - No more than N_s repair vehicles dispatched from each yard
  - Flow conservation constraints
  - Each localization set is visited by only one repair vehicle
  - Constraints to bound the time of arrival at yard or localization set
  - Update time of arrival by taking into account the vehicle travel time as well as the time to repair and the optimal sUAS exploration time for each localization set
  - Routing constraints imposed by transportation network

SNEP

- Objective: Minimize the maximum time to observe all network components, over R available sUASs.
- Subject to:
  - No more than R sUASs are used
  - Depart and return to temporary base 0_k
  - Each monitoring location visited at most once in L_k
  - sUAS can monitor a subset of network components from each monitoring location; each network component is monitored at least once
  - Allow multi-trips; flight travel time constraints for each trip (incorporates recharging)
  - Total cumulative travel time for all trips by each sUAS
  - Airspace restrictions, communication requirements, and other safety considerations

Computational Study

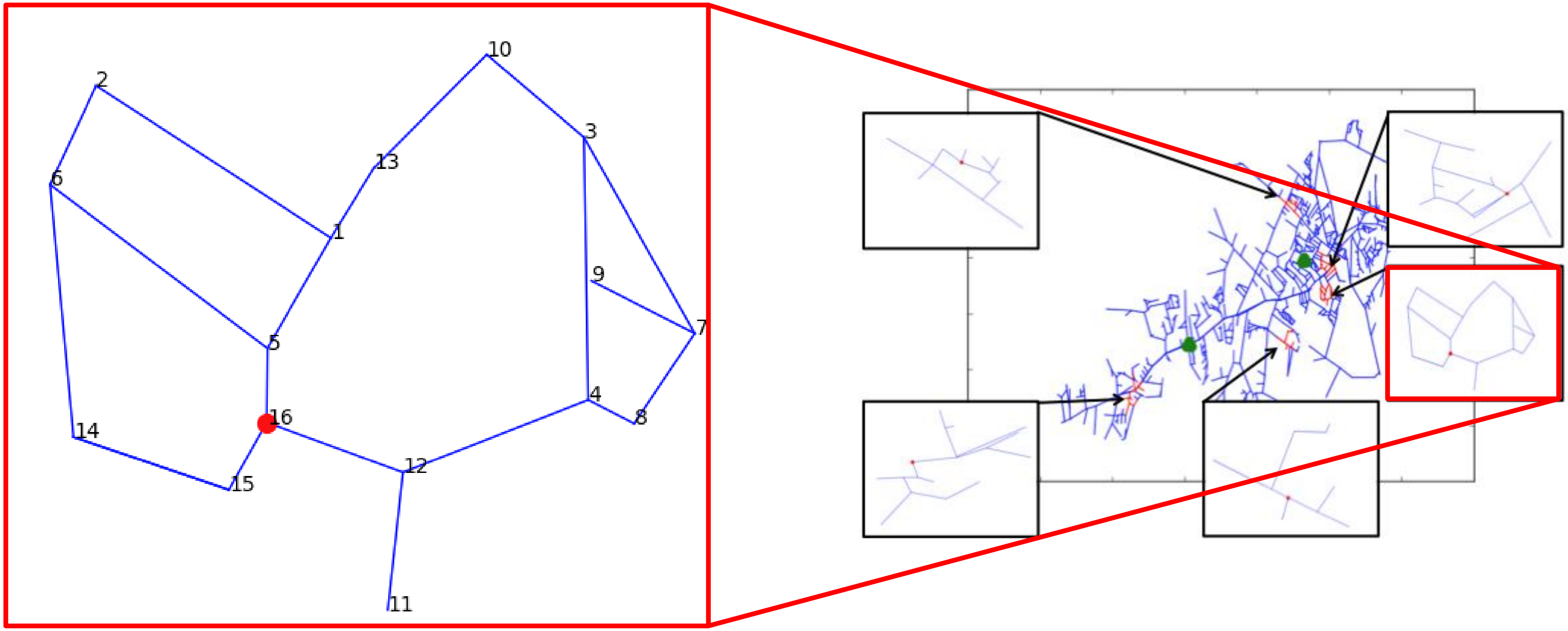


Y_2: 2 Repair vehicles
(2 sUASs each)

Y_1: 1 Repair vehicle
(2 sUASs)

$\tau_{repair} = 10$ min
$\theta = [1, 1, 1, 1, 1]$

SNEP

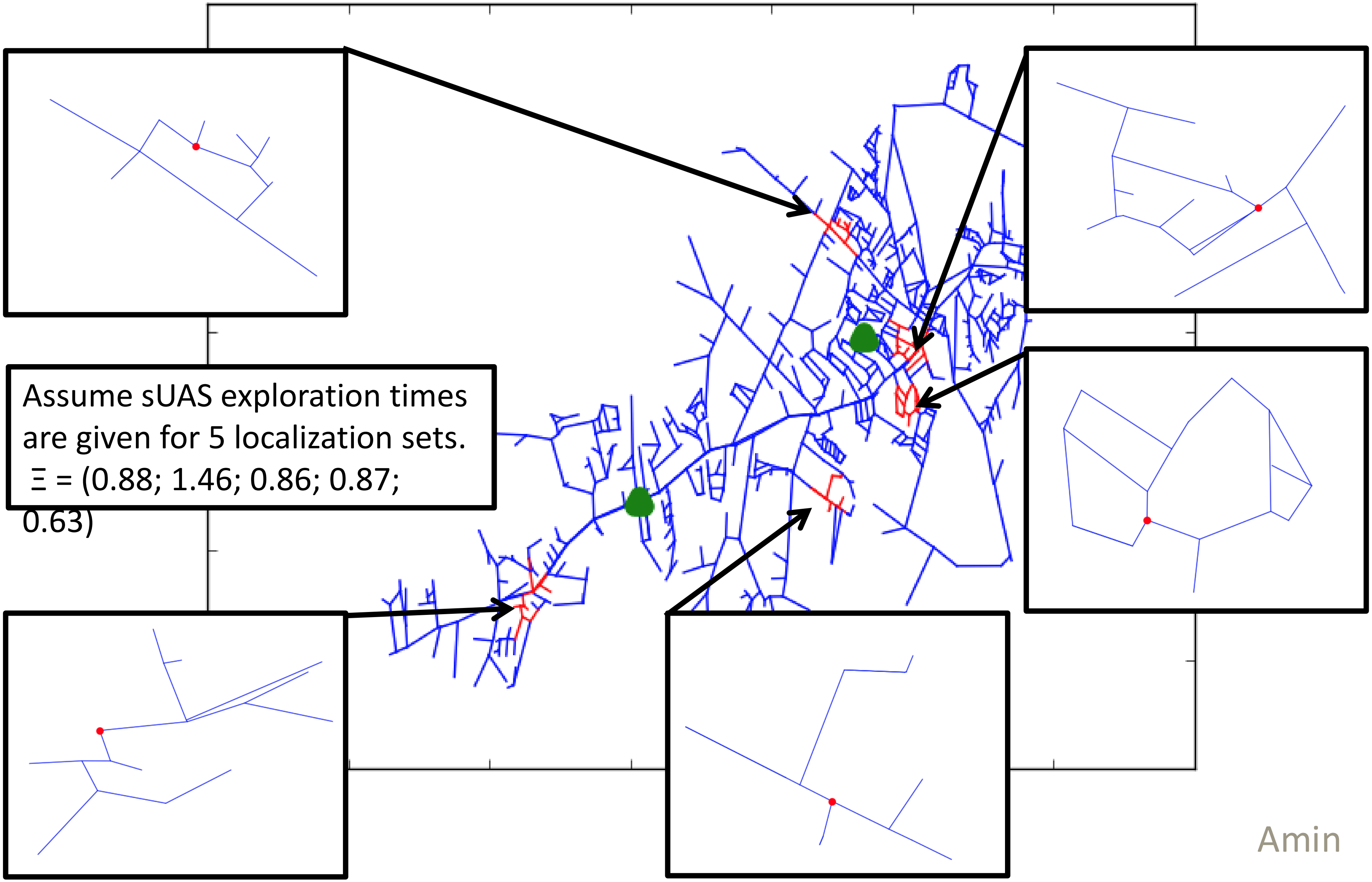


Set up:

- Temporary base 0_k at node 16
- Maximum time for battery life: 1 hour; Time to charge battery (if needed): 5 min
- sUAS can monitor adjacent edges incident to node
- sUAS travels along edges of network (can be generalized)
- Shortest path travel times between each pair of nodes
- Objective is to minimize the maximum amount of time (among all sUASs) to explore L_k

Amin

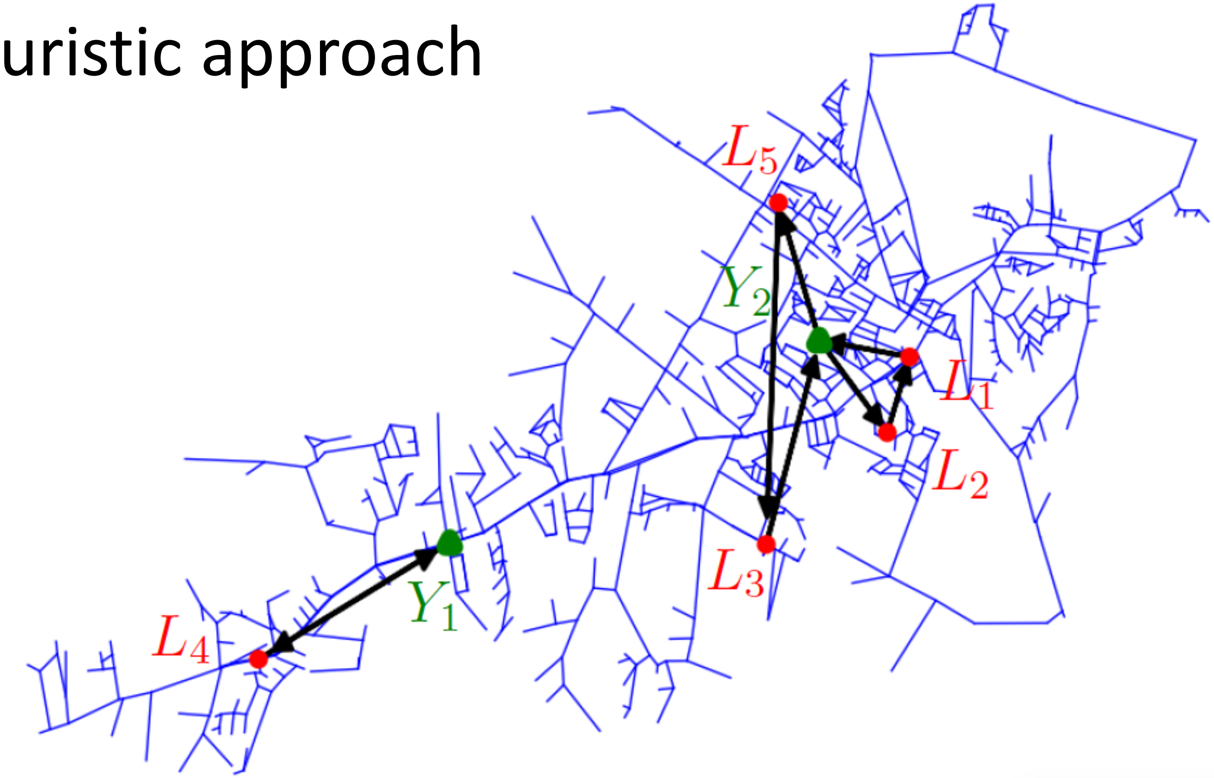
Computational Study



Assume sUAS exploration times are given for 5 localization sets. $\Xi = (0.88; 1.46; 0.86; 0.87; 0.63)$

Results and Insights

- Solutions sensitive to failure alert duration prior to dispatch, θ_k
- RVRP solution sensitive to ξ_k^*.
- Computational bottleneck with determining ξ_k^*
  - Heuristic approach



Amin

Summary

- Main Contributions
  - Operational end to end framework for infrastructure monitoring and inspection using sUASs
  - Development of MIP models for the RVRP and SNEP
- Other applications: Disaster and Emergency Response
- Relation with other FORCES research:
  - Safety preserving learning and control (Tomlin)
  - Airspace regulations (Balakrishnan and Tomlin)
  - Cyber-Physical security (Koutsoukos, Sastry)