FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Strategic Network Inspection using Resource-Constrained sUAS

Mathieu Dahan
Joint with Saurabh Amin and Andrew Weinert (MIT LL)

Massachusetts Institute of Technology

NSF Review Meeting, January 25, 2017

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.
  - Defender: chooses a dispatch of sUAS.

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.
  - Defender: chooses a dispatch of sUAS.
  - Attacker: targets multiple network components.

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.
    - Defender: chooses a dispatch of sUAS.
    - Attacker: targets multiple network components.
- Main contributions

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.
  - Defender: chooses a dispatch of sUAS.
  - Attacker: targets multiple network components.
- Main contributions
  - General sensing model: heterogeneous range.

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Network Sensing: Security Failures (Attacks)

How to operationalize network sensing strategies?

- For a given network that faces adversarial disruptions, design and operationalize (**randomized**) sensing strategies subject to limitations on sensing range and resource constraints.

Malicious attacks

Approach

- Formulate a robust optimization problem over the network.
  - Defender: chooses a dispatch of sUAS.
  - Attacker: targets multiple network components.
- Main contributions
  - General sensing model: heterogeneous range.
  - Solution approach using combinatorial problems.

Randomized defense

M. Dahan, L. Sela, S. Amin. "Randomized Network Sensing under Strategic Disruptions", *Working paper*

Related Work

- Dispatch of sUAS
    - Distance-Constrained Vehicle Routing Problem [Kara '11, Laporte '92]

Related Work

- Dispatch of sUAS
  - Distance-Constrained Vehicle Routing Problem [Kara '11, Laporte '92]

- Network sensing under reliability failures
  - Mixed-integer optimization [Berry '06, Chakrabarti '09]
  - Submodular optimization [Krause '08]

Related Work

- Dispatch of sUAS
  - Distance-Constrained Vehicle Routing Problem [Kara '11, Laporte '92]

- Network sensing under reliability failures
  - Mixed-integer optimization [Berry '06, Chakrabarti '09]
  - Submodular optimization [Krause '08]

- Network security games [Goyal '14]
  - Search games [Gal '14]
  - Inspection games [Avenhaus '12]
  - Patrolling games [Alpern '11]

Related Work

- Dispatch of sUAS
  - Distance-Constrained Vehicle Routing Problem [Kara '11, Laporte '92]

- Network sensing under reliability failures
  - Mixed-integer optimization [Berry '06, Chakrabarti '09]
  - Submodular optimization [Krause '08]

- Network security games [Goyal '14]
  - Search games [Gal '14]
  - Inspection games [Avenhaus '12]
  - Patrolling games [Alpern '11]

(Q) How to allocate a fleet of sUAS for network inspection in an adversarial environment?

Network and Sensing Models

Network and Sensing Models

- E: Set of vulnerable infrastructure components.

Network and Sensing Models

- E: Set of vulnerable infrastructure components.
- N: Set of locations that can be visited by an sUAS.

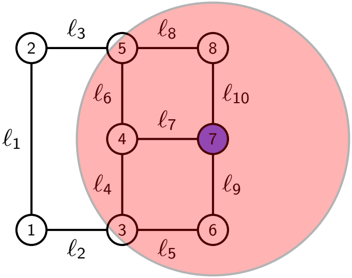
Network and Sensing Models

- E: Set of vulnerable infrastructure components.
- N: Set of locations that can be visited by an sUAS.
- For every location $i \in N$, $\mathcal{C}_i \in 2^E$ represents the subset of components that an sUAS is capable of monitoring when positioned in location i. For example, $\mathcal{C}_i$ may represent:

L. Sela, W. Abbas, X. Koutsoukos, and S. Amin. "Sensor placement for fault location identification in water networks: a minimum test cover approach", *Automatica*, 2016

Network and Sensing Models

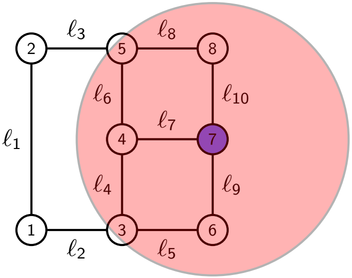
- E: Set of vulnerable infrastructure components.
- N: Set of locations that can be visited by an sUAS.
- For every location $i \in N$, $\mathcal{C}_i \in 2^E$ represents the subset of components that an sUAS is capable of monitoring when positioned in location i. For example, $\mathcal{C}_i$ may represent:
  - The components that are within a certain distance from i.

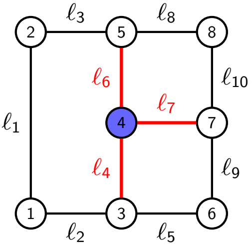


L. Sela, W. Abbas, X. Koutsoukos, and S. Amin. "Sensor placement for fault location identification in water networks: a minimum test cover approach", *Automatica*, 2016

Network and Sensing Models

- E: Set of vulnerable infrastructure components.
- N: Set of locations that can be visited by an sUAS.
- For every location $i \in N$, $\mathcal{C}_i \in 2^E$ represents the subset of components that an sUAS is capable of monitoring when positioned in location i. For example, $\mathcal{C}_i$ may represent:
  - The components that are within a certain distance from i.
  - The adjacent edges of node i.





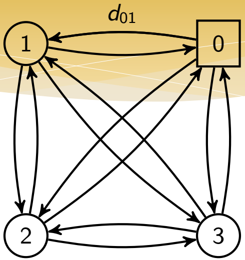
L. Sela, W. Abbas, X. Koutsoukos, and S. Amin. "Sensor placement for fault location identification in water networks: a minimum test cover approach", *Automatica*, 2016

sUAS Model

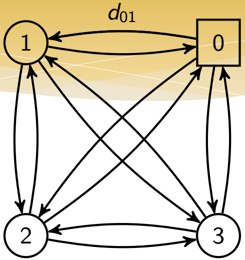
- $0 \in N$: Unique base node from where the sUAS are sent.

sUAS Model

- $0 \in N$: Unique base node from where the sUAS are sent.
- For every pair of locations $(i, j) \in N^2$, let d_{ij} denote the distance to fly from i to j.
  - The d_{ij} can take into account air space restrictions, obstacles, height difference between locations, etc.



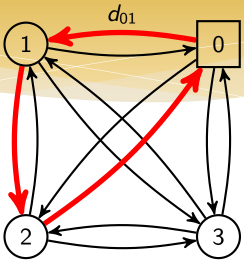
sUAS Model



- $0 \in N$: Unique base node from where the sUAS are sent.
- For every pair of locations $(i, j) \in N^2$, let d_{ij} denote the distance to fly from i to j.
  - The d_{ij} can take into account air space restrictions, obstacles, height difference between locations, etc.
- Homogeneous fuel-constrained sUAS that can fly for up to D_{max} miles before going back to the base node 0.

sUAS Model

- $0 \in N$: Unique base node from where the sUAS are sent.
- For every pair of locations $(i, j) \in N^2$, let d_{ij} denote the distance to fly from i to j.
  - The d_{ij} can take into account air space restrictions, obstacles, height difference between locations, etc.



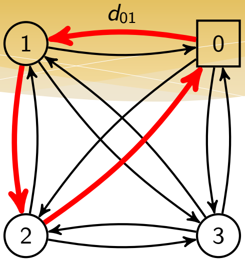
- Homogeneous fuel-constrained sUAS that can fly for up to D_{max} miles before going back to the base node 0.

Feasible Flight Plan

- Feasible flight plan: a 0-closed walk of length at most D_{max}.

sUAS Model

- $0 \in N$: Unique base node from where the sUAS are sent.
- For every pair of locations $(i,j) \in N^2$, let d_{ij} denote the distance to fly from i to j.
  - The d_{ij} can take into account air space restrictions, obstacles, height difference between locations, etc.



- Homogeneous fuel-constrained sUAS that can fly for up to D_{max} miles before going back to the base node 0.

Feasible Flight Plan

- Feasible flight plan: a 0-closed walk of length at most D_{max}.
- Set of feasible flight plans:

$$\mathcal{F} := \{(i_1, \ldots, i_m) \in N^m \mid i_1 = i_m = 0 \text{ and } \sum_{k=1}^{m-1} d_{i_k i_{k+1}} \leq D_{max},\ m \in \mathbb{N}\}.$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network Inspection Problem

(Q) How to maximize the detection performance against a worst case scenario?

Network Inspection Problem

(Q) How to maximize the detection performance against a worst case scenario?

- The operator has $b_1 \in \mathbb{N}$ available sUAS.
  - σ^1: Probability distribution over dispatches, η, of the fleet of sUAS.

Network Inspection Problem

(Q) How to maximize the detection performance against a worst case scenario?

- The operator has $b_1 \in \mathbb{N}$ available sUAS.
  - σ^1: Probability distribution over dispatches, η, of the fleet of sUAS.
- Worst case scenario: Attacker who targets a subset of components
  - μ: Attack of up to b_2 network components.

Network Inspection Problem

(Q) How to maximize the detection performance against a worst case scenario?

- The operator has $b_1 \in \mathbb{N}$ available sUAS.
  - σ^1: Probability distribution over dispatches, η, of the fleet of sUAS.
- Worst case scenario: Attacker who targets a subset of components
  - μ: Attack of up to b_2 network components.

Robust optimization problem

Minimize the maximum number of failure events that remain undetected:

$$(\mathcal{P}_{insp}) \qquad \min_{\sigma^1 \in \Delta(\mathcal{A}_1)} \max_{\mu \in \mathcal{A}_2} \mathbb{E}_{\sigma^1} \left[|\mu| - |\mathcal{C}_\eta \cap \mu| \right].$$

Network Inspection Problem

(Q) How to maximize the detection performance against a worst case scenario?

- The operator has $b_1 \in \mathbb{N}$ available sUAS.
  - σ^1: Probability distribution over dispatches, η, of the fleet of sUAS.
- Worst case scenario: Attacker who targets a subset of components
  - μ: Attack of up to b_2 network components.

Robust optimization problem

Minimize the maximum number of failure events that remain undetected:

$$(\mathcal{P}_{insp}) \qquad \min_{\sigma^1 \in \Delta(\mathcal{A}_1)} \max_{\mu \in \mathcal{A}_2} \mathbb{E}_{\sigma^1} \left[|\mu| - |\mathcal{C}_\eta \cap \mu| \right].$$

- $|\mu| - |\mathcal{C}_\eta \cap \mu|$ is the total number of failures net the number of detected failures.

Solution Approach: Exploration Problem

Auxiliary Problem

Solution Approach: Exploration Problem

Auxiliary Problem

What is the minimum number of fuel-constrained sUAS needed to fully explore all the components?

Solution Approach: Exploration Problem

Auxiliary Problem

What is the minimum number of fuel-constrained sUAS needed to fully explore all the components?

$$
\begin{array}{lll}
(\mathcal{P}_{exp}) & \text{minimize} & m \\
& \text{subject to} & \displaystyle\bigcup_{k=1}^{m} \bigcup_{i \in w_k} \mathcal{C}_i = E \\
& & w_1, \ldots, w_m \in \mathcal{F}.
\end{array}
$$

Solution Approach: Exploration Problem

Auxiliary Problem

What is the minimum number of fuel-constrained sUAS needed to fully explore all the components?

$$
\begin{array}{llcr}
(\mathcal{P}_{exp}) & \text{minimize} & m & \text{(number of sUAS)} \\
 & \text{subject to} & \displaystyle\bigcup_{k=1}^{m} \bigcup_{i \in w_k} \mathcal{C}_i = E & \text{(full coverage)} \\
 & & w_1, \ldots, w_m \in \mathcal{F}. & \text{(feasible flight plans)}
\end{array}
$$

Solution Approach: Exploration Problem

Auxiliary Problem

What is the minimum number of fuel-constrained sUAS needed to fully explore all the components?

$$
\begin{array}{llll}
(\mathcal{P}_{exp}) & \text{minimize} & m & \text{(number of sUAS)} \\
& \text{subject to} & \displaystyle\bigcup_{k=1}^{m} \bigcup_{i \in w_k} \mathcal{C}_i = E & \text{(full coverage)} \\
& & w_1, \ldots, w_m \in \mathcal{F}. & \text{(feasible flight plans)}
\end{array}
$$

- m^*: Optimal value of $(\mathcal{P}_{exp})$.

Solution Approach: Exploration Problem

Auxiliary Problem

What is the minimum number of fuel-constrained sUAS needed to fully explore all the components?

$$\begin{array}{llll} (\mathcal{P}_{exp}) & \text{minimize} & m & \text{(number of sUAS)} \\ & \text{subject to} & \displaystyle\bigcup_{k=1}^{m} \bigcup_{i \in w_k} \mathcal{C}_i = E & \text{(full coverage)} \\ & & w_1, \ldots, w_m \in \mathcal{F}. & \text{(feasible flight plans)} \end{array}$$

- m^*: Optimal value of $(\mathcal{P}_{exp})$.
- Can be formulated as a mixed-integer program.

Detection Guarantees

Theorem

Given an optimal solution of $(\mathcal{P}_{exp})$, *we can construct a randomized strategy* $\widetilde{\sigma}^1$ *such that:*

M. Dahan, A. Weinert, and S. Amin. "Network Exploration and Inspection Using Distance-Constrained sUAS", *Submitted*, 2016

Detection Guarantees

Theorem

Given an optimal solution of $(\mathcal{P}_{exp})$, *we can construct a randomized strategy* $\widetilde{\sigma}^1$ *such that:*

1. *The expected number of undetections in the worst case is upper bounded by:*

$$\max_{\mu \in \mathcal{A}_2} \mathbb{E}_{\widetilde{\sigma}^1}\left[|\mu| - |\mathcal{C}_\eta \cap \mu|\right] \leq b_2 \left(1 - \frac{b_1}{m^*}\right).$$

- b_1: number of available sUAS
- b_2: maximum attack size
- m^*: Optimal value of $(\mathcal{P}_{exp})$

M. Dahan, A. Weinert, and S. Amin. "Network Exploration and Inspection Using Distance-Constrained sUAS", *Submitted*, 2016

Detection Guarantees

Theorem

Given an optimal solution of $(\mathcal{P}_{exp})$, *we can construct a randomized strategy* $\widetilde{\sigma}^1$ *such that:*

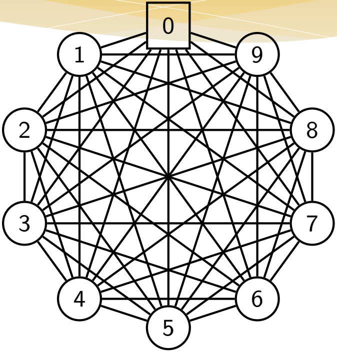
1. *The expected number of undetections in the worst case is upper bounded by:*
$$\max_{\mu\in\mathcal{A}_2}\mathbb{E}_{\widetilde{\sigma}^1}\left[|\mu|-|\mathcal{C}_\eta\cap\mu|\right]\leq b_2\left(1-\frac{b_1}{m^*}\right).$$
2. *The detection rate, defined as the ratio between the number of detections and the total number of failure events, in the worst case, is lower bounded in expectation by:*
$$\min_{\mu\in\mathcal{A}_2}\mathbb{E}_{\widetilde{\sigma}^1}\left[\frac{|\mathcal{C}_\eta\cap\mu|}{|\mu|}\right]\geq\frac{b_1}{m^*}.$$

- b_1: number of available sUAS
- b_2: maximum attack size
- m^*: Optimal value of $(\mathcal{P}_{exp})$

M. Dahan, A. Weinert, and S. Amin. "Network Exploration and Inspection Using Distance-Constrained sUAS", *Submitted*, 2016

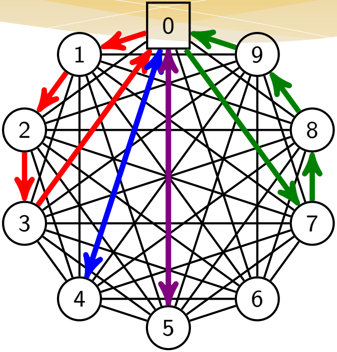
Case Study: Complete Network

- Fully connected network.
- 10 locations uniformly placed on a circle of radius 1 mile.
- The sUAS can travel for 4 miles.
- Vulnerable components are the **network edges** that can be monitored from its end nodes.



Case Study: Complete Network

- Fully connected network.
- 10 locations uniformly placed on a circle of radius 1 mile.
- The sUAS can travel for 4 miles.
- Vulnerable components are the **network edges** that can be monitored from its end nodes.



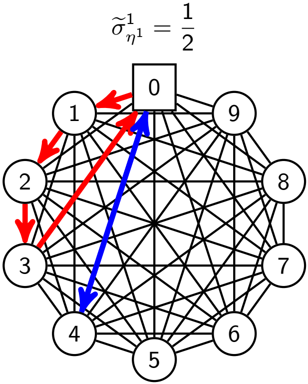
- Optimal solution of $(\mathcal{P}_{exp})$: $w_1^* = (0, 1, 2, 3, 0)$, $w_2^* = (0, 4, 0)$, $w_3^* = (0, 5, 0)$ and $w_4^* = (0, 7, 8, 9, 0)$.

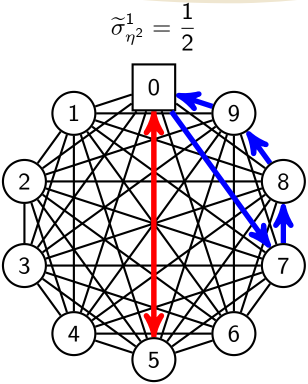
Inspection

- If the operator has 2 sUAS, then $\widetilde{\sigma}^1$ is illustrated as follows:

Inspection

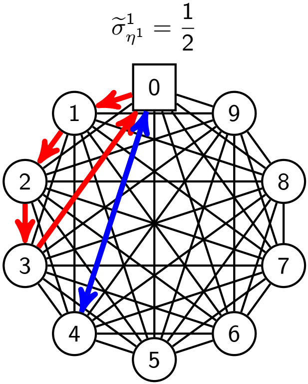
- If the operator has 2 sUAS, then $\widetilde{\sigma}^1$ is illustrated as follows:

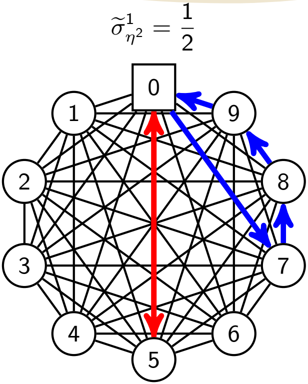




Inspection

- If the operator has 2 sUAS, then $\widetilde{\sigma}^1$ is illustrated as follows:





- At least 50 % of the failures will be detected.

Conclusion

- Summary
  - Resource allocation problem for network inspection using fuel-constrained sUAS.
  - Flexible model that can take into account constraints imposed by the sUAS platform and the environment.
  - Mixed-integer programming formulation for the network exploration problem.
  - Extension to the inspection problem, and performance guarantee on the detection score in worst-case scenarios.

Conclusion

- Summary
    - Resource allocation problem for network inspection using fuel-constrained sUAS.
    - Flexible model that can take into account constraints imposed by the sUAS platform and the environment.
    - Mixed-integer programming formulation for the network exploration problem.
    - Extension to the inspection problem, and performance guarantee on the detection score in worst-case scenarios.
- Future Work
    - Include heterogeneity in the vulnerability or importance of components.
    - Account for imperfect (and noisy) information on network state in designing exploration/inspection strategies.

Acknowledgements

1. NSF FORCES (Foundations Of Resilient Cyber-Physical Systems)
2. MIT Thurber Fellowship

Thank you!

Questions: mdahan@mit.edu

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

References

Andreas Krause, Ajit Singh, Carlos Guestrin (2008)
Near-optimal sensor placements in gaussian processes: Theory, efficient algorithms and empirical studies

J. Berry, W. Hart, C. Phillips, J. Uber, J. Watson (2006)
Sensor placement in municipal water networks with temporal integer programming models.

S. Chakrabarti, E. Kyriakides, D.G. Eliades (2009)
Placement of synchronized measurements for power system observability.

Sanjeev Goyal, Adrien Vigier (2014)
Attack, Defense, and Contagion in Networks.

Shmuel Gal, Jérôme Casas. (2014)
Succession of hide-seek and pursuit-evasion at heterogeneous locations.

Rudolf Avenhaus, Bernhard Von Stengel, Shmuel Zamir (2012)
Handbook of Game Theory with Economic Applications

Steve Alpern, Alec Morton, Katerina Papadaki (2011)
Patrolling games.

Imdat Kara (2011)
Arc based integer programming formulations for the distance constrained vehicle routing problem

Gilbert Laporte (1992)
The vehicle routing problem: An overview of exact and approximate algorithms