Probabilistic Mission Defense and Assurance

NATO STO IST-148
Symposium on Cyber Defence Situation Awareness

Alexander Motzek* Ralf Möller*

*Universität zu Lübeck
Institute of Information Systems
Ratzeburger Allee 160, 23562 Lübeck, Germany
{motzek,moeller}@ifis.uni-luebeck.de

October, 3rd 2016

Summary: Defending and Assuring the Mission

- situation: **mission is threatened**.
- task: need to **respond** adequately.
- goal: **assure mission success.**
- constraint: **without sacrificing** mission for security.

Challenges

- understand how a **threat affects a mission**.
- understand **countermeasures diminishing threats**.
- understand the **bad sides of countermeasures** causing **negative side-effects** on the mission.

Current Approaches & Problems

- **holistic approaches** deliver **intransparent** "optimal" solution.

  exaggeratedly "Response XYZ is best with metric 4589.32".

- require **unacquirable information**, do not encompass **unforeseeable events**

  complex ACTs. manually intractable. automatic generation⇔single missing links.

- optimize cost, **without** considering **negative side** of countermeasures.

  shutdown of central control server is very cheap!

Our Approach & Outline

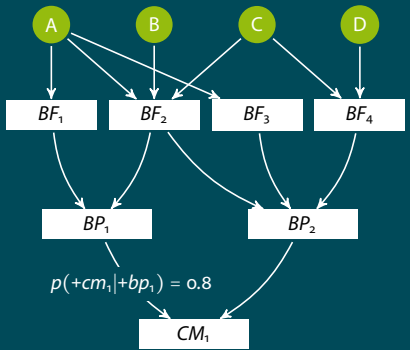
- paradigm shift. **model the mission**, not the attacker.
- **model the good and the bad** sides encompassing **uncertainty**.
- reduce problem to **mathematically well-defined** probabilistic inference **problem**.
- **decouples** assessments from generation of responses and from selection.
- delivers **directly understandable** and validated results.

The probability that our mission becomes adversarially impacted is 58% (⚀⚂⚂⚃⚃⚄).
We can reduce this by 80% (to <⚀⚁⚂⚃⚃⚄). *There exists a 30% probability of immediate conflict* (<⚀⚀⚂⚃⚄⚅)

Probabilistic Approach

- model problem from **three different perspectives**.
- **collect** potentially disagreeing **information from multiple experts**.
- make the model able to understand disagreements;
  do not enforce a bad compromise.

View 1: The Mission (or a company)



- dissect mission into **smaller pieces**.

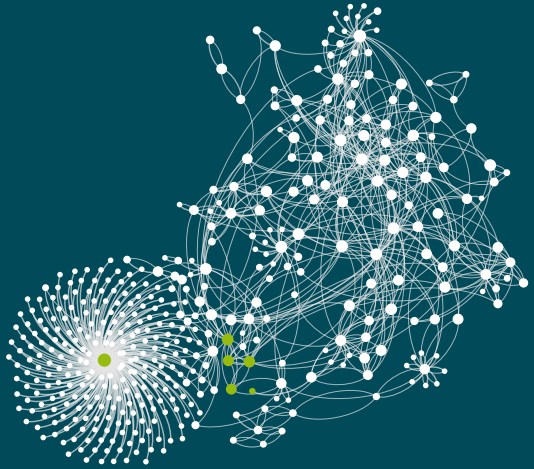
✓ collected **directly from** business and mission **experts**.

- conditional probabilities are understandable and validatable
  "probability of mission failing, given BP_1 fails is 80%" ⚀⚁⚂⚃⚄⚅

- *frontend or backend?*

→ **mission critical devices** (ABCD)
only scratch surface of infrastructure

View 2: The Infrastructure

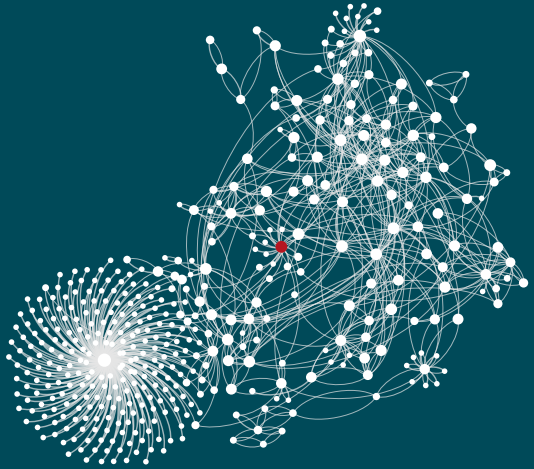


- MCDs are **only tip of the ice berg**
- huge **complex dependency structures**

✓ **automatically learnable**

- same **conditional probabilities** as before!

View 3: The Impact

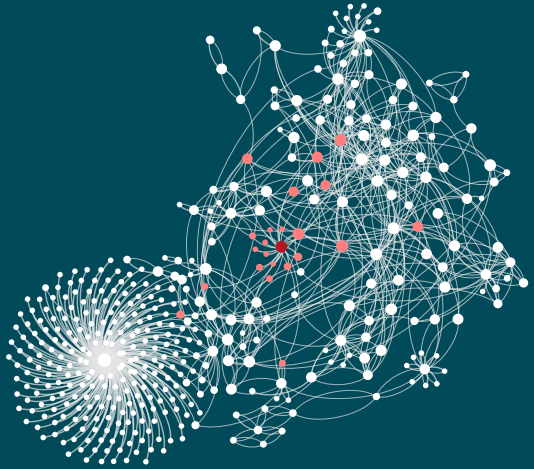


- something **fails** or is **attacked**.

→ probability of **local impact**.

- leads to **global impact**

View 3: The Impact

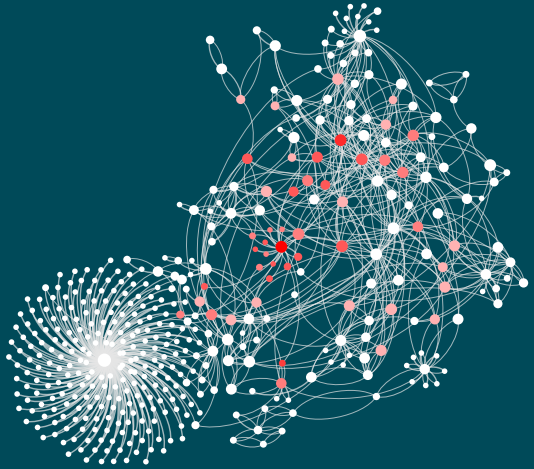


- something **fails** or is **attacked**.

→ probability of **local impact**.

- leads to **global impact**
- might even **spread**...

View 3: The Impact



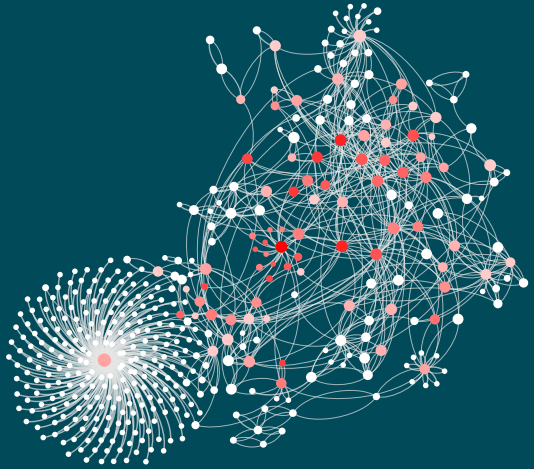
- something **fails** or is **attacked**.

→ probability of **local impact**.

- leads to **global impact**

- might even **spread**...
- ...to dependent nodes...

View 3: The Impact



- something **fails** or is **attacked**.

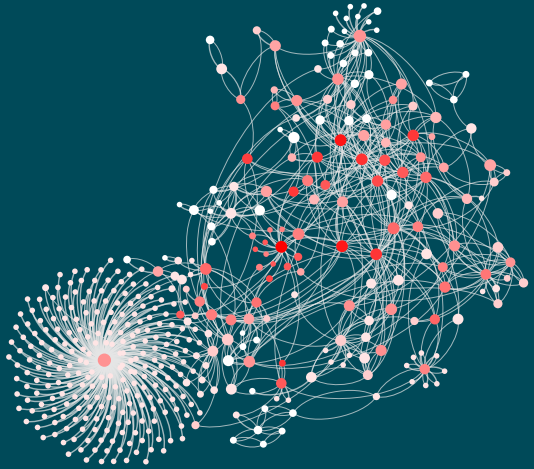
→ probability of **local impact**.

- leads to **global impact**

- might even **spread**...
- ...to dependent nodes...
- ...to dependent nodes...

MOTZEK ET AL. PROBABILISTIC MISSION DEFENSE AND ASSURANCE, NATO IST-148

View 3: The Impact



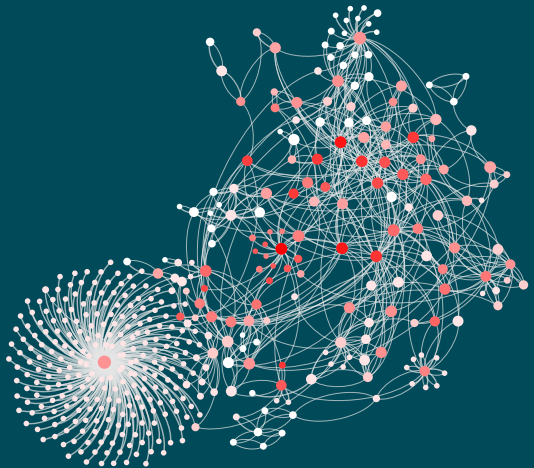
- something **fails** or is **attacked**.

→ probability of **local impact**.

- leads to **global impact**

- might even **spread**...
- ...to dependent nodes...
- ...to dependent nodes...
- until **everything** is impacted.
- how to assess?

Problems of "Spreading" Algorithms

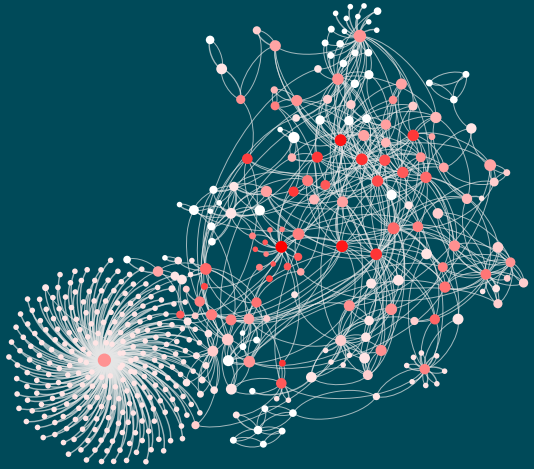


- various novel "spreading"-algorithms exist.
- novelly designed, hand-crafted.

✗ unclear behavior.
✗ sense for parameters missing.
✗ no clear definition for interpreting results.

→ only **deeply trained experts** can **parametrize** models and **understand** results.

Problems of "Spreading" Algorithms



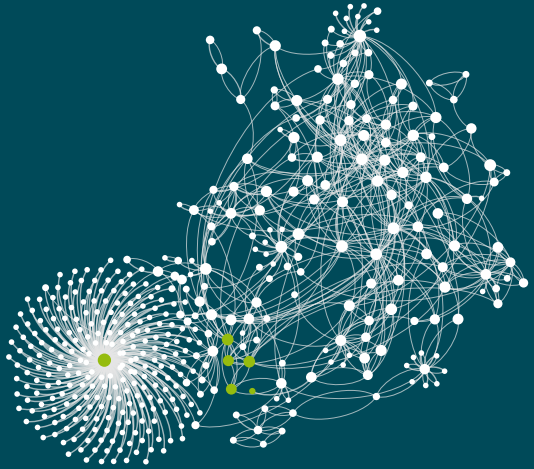
- various novel "spreading"-algorithms exist.
- novelly designed, hand-crafted.

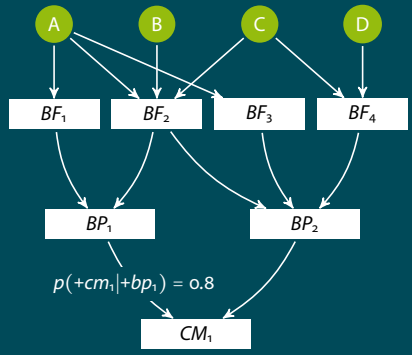
✗ unclear behavior.
✗ sense for parameters missing.
✗ no clear definition for interpreting results.

→ only **deeply trained experts** can **parametrize** models and **understand** results.

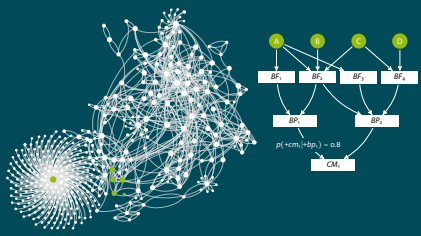
✓ reduce to mathematical problem!

Mission Impact Assessment is a Probabilistic Graphical Model





Mission Impact Assessment as a Probabilistic Inference Problem

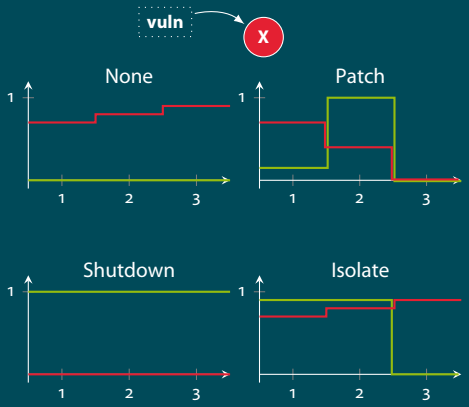


- probabilistic inference **projects local impacts globally on the mission.**
- ✓ well-defined mathematical problem.

- ✓ **validate the model**, not the algorithm.
- ✓ **parameters** define their own **semantic**.
- ✓ **results** are **directly understandable** by everyone.

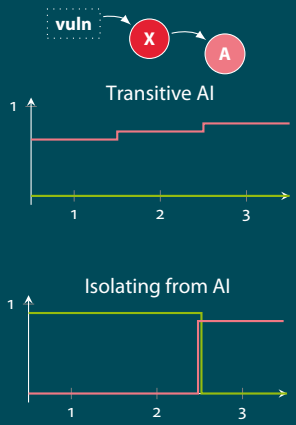
→ **model** adversarial **threats**, countermeasures **positive** & **negative intuitively and locally**.

Modeling Defense and Threats Locally: direct impact example



- **vulnerability** creates probability of **adverserial impact** **varying over time**: short-, mid-, long-term
- **shutdown** suffocates **AI**, but **nothing works**.
- **patching** causes prob. of conflict: **operational impact**
  short: **installation** conflict, mid: **reboot** required,
  long: vulnerability **removed**.
- **isolate**: no *local* "positive" effect. negative=shutdown.

Modeling Defense and Threats: transitive-effects example



- node A depends on affected node X. impact "**spreads**".

→ **transitive adverserial impact**
*(not modeled, **assessed automatically**)*

- **isolate X** for short- and mid-term
blocks adverserial impact for X *(assessed automatically)*

- but **blocks required information flow** towards A

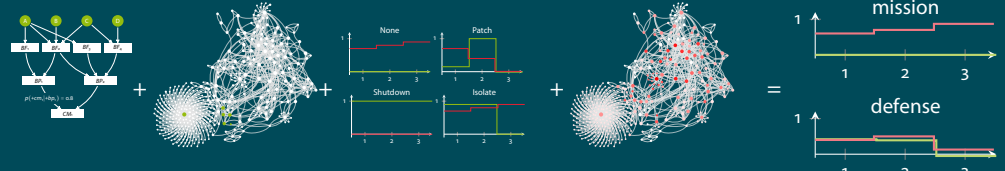
→ operational impact on A

Probabilistic Inference

- local impact models create **impact time-profiles**.
- ✓ considers **adversarial and self-inflicted impact** on the mission.

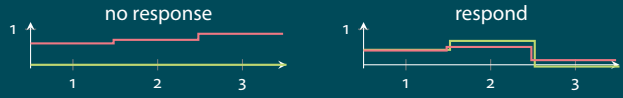
- **probabilistic inference projects local impacts** to the **global mission impact**
- ✓ directly **understandable**, interpretable and reportable.

- no novel spreading-algorithms, well defined mathematical problem
- ✓ **models can be validated** directly. **no holistic validation** required.



Probabilistic Inference

- assessment for the **current situation**, **benefits of our response** and its **negative side effects**.



- *probability of impact on the mission over the time.*

✓ based on **acquirable** and automatically **learnable data**.

✓ accept **disagreeing information sources** and **directly reflect expertise**.

✓ captures **unforeseen events and uncertainty** *"what all could happen"* through **transitive impacts**.

Experiments

- **experimented on live data** with artificially placed adversarial impacts in Acea ARETi.
- based on the placed impacts, **doing nothing was the best option** in short and mid term.
- **patching and isolating** first gains superiority in **long term perspective**.

- $\{\max_i(OI^i) = 0.8\} > \{\max_i(AI^i) = 0.75\}$
- delivered **non-trivial results** and precisely raised awareness for the **compromise between the good and the bad**.

Further Usage

- **no vendor lock in**: assessments are an **independent quality control**. no reference required.
  e.g., evaluate response plans from other applications, handbook approaches, intuition, guidelines, obliged responses
- **selecting "the best"** is = **find multi-dimensional semi-optimum** among all evaluated
  note: applicable on any subset. no holistic evaluation required
- use PGM to find POIs to **strategically block** communications
  min-cut graph problem *based on edge-contribution probability*

Conclusion

- **probabilistically** well-defined **mission impact defense** and assurance approach.
- encompasses uncertainty, missing links and disagreeing information sources.
- encompasses **the good and the bad** sides
- available and **easily acquirable data**.
- **validated results**, **understandable without context** and **without biased interpretations**.
- suitable for **reporting** along command chains and in documents for **justifying decisions**.
  e.g., understanding does not require vulnerabilities, attack paths, or algorithmic properties.
  probability of 83% remains 83% and is equivalent to tossing  .

Thank You.

... questions?

Independent Assessment

- every assessment can **stand on its own**.

✓ understandable knowing neither the algorithms nor the models.

✓ **no holistic reference set** required to "interpret" results. **no biased interpretation.**

*"Probability of impact onto mission is **83%**" instead of "Mission impact is **4546.345**".*

- therefore: **response-proposals may origin from anywhere.**
  e.g., other applications, handbook approaches, intuition, guidelines, obliged responses

- assessment is an **independent quality control**.

Decoupled Selection

- problem: given multiple assessments, **select a single response**.

- multiple dimensions might disagree.
- difficult to design a "cost function" among dimensions.

- well-defined problem: **unweighted multi-dimensional minimization** finding **best compromise**.

✓ **no bias** towards one dimension required.

✓ **does not require all possible responses** to be evaluated.

$$\mathring{RP} = \min_{\varepsilon} \left(\left\{ \bigcap_{d \in \vec{d}} \dot{RP}_{\varepsilon}^{d} \right\} \neq \varnothing \right). \tag{1}$$

Decoupled Generation

- problem: **how to obtain adequate responses**? use PGM for generation!

✓ no bad generation possible: **assessment is independent** judgment.

✓ "one does not have to find *the* best, only one whose assessment is independently acceptable."

- **randomly sample**: shutdown critical, directly affected, patch affected, isolate patched nodes.

- where to **strategically block communication**, i.e., firewall rules?
  mathematical problem in PGM: **find min-cut** in model based on minimal edge-contribution probability.