UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR INFORMATIONSSYSTEME

INSTITUTE OF INFORMATION SYSTEMS

Probabilistic Mission Impact Assessment based on Widespread Local Events

IST-128 Workshop on Cyber Attack Detection,
Forensics and Attribution for Assessment of Mission Impact

Alexander Motzek[*] Ralf Möller[*] Mona Lange[*] Samuel Dubus[‡]

[*] Universität zu Lübeck
Institut für Informationssysteme
Ratzeburger Allee 160, 23562 Lübeck, Germany
{motzek,moeller}@ifis.uni-luebeck.de

[‡] Alcatel-Lucent, Bell Labs Research
Network Algorithm Routing and Security Program
Route de Villejust, 91625 Nozay, France
samuel.dubus@alcatel-lucent.com

June, 15th 2015

Mission Impact Assessment

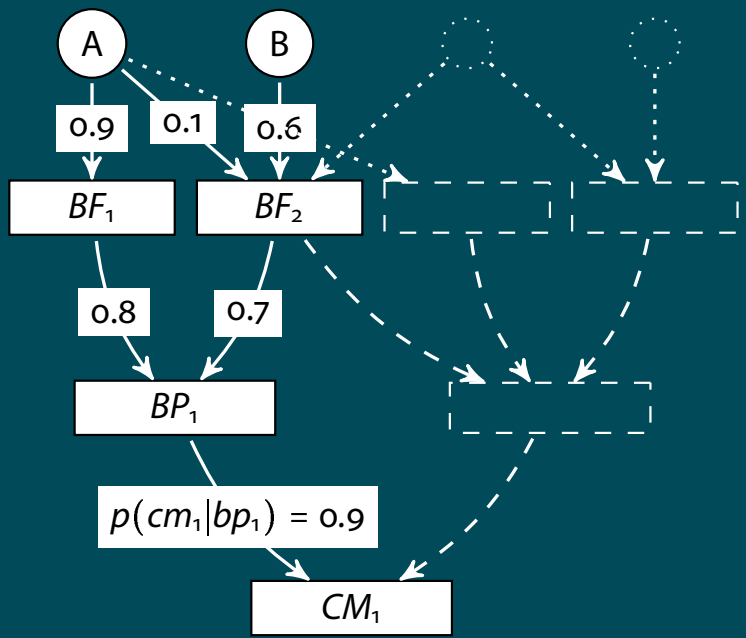
- Current approaches employ score-based algorithms
- "Number crunching"
- Data set validation mising
- Formalization missing
- We formalize MIA as a probabilistic well-defined problem
- with a well-defined solution

Dependency Models

- Three views
- Three Experts
- Three Expertises

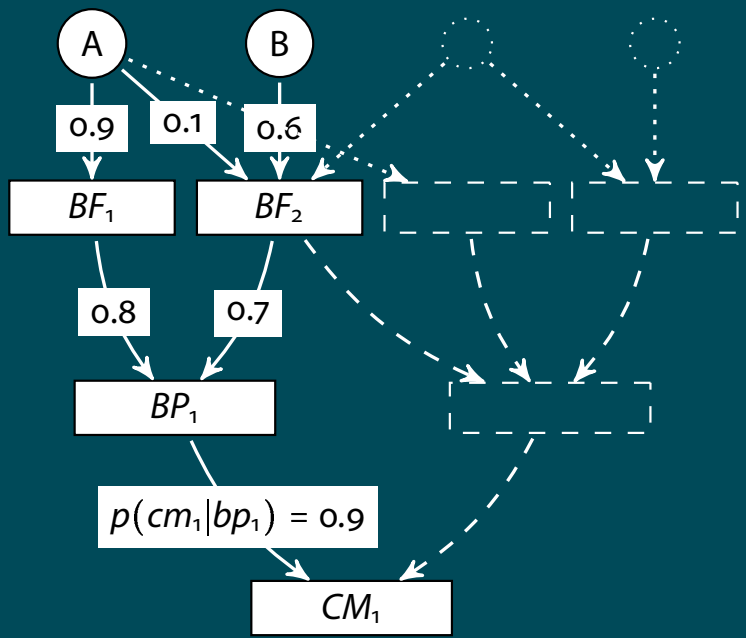
- We model MIA from three different perspectives
- Combined under the hood of probabilistic theory

View 1: Mission/Business Model



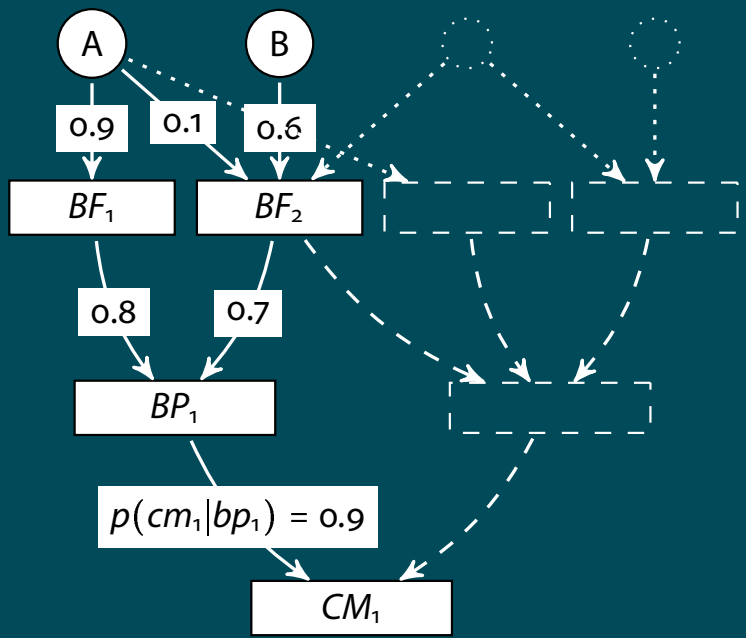
- Last 3 Layers: Expertise of Expert 1
- Extractable from BPMN
- Common, Feasible

View 1: Mission/Business Model



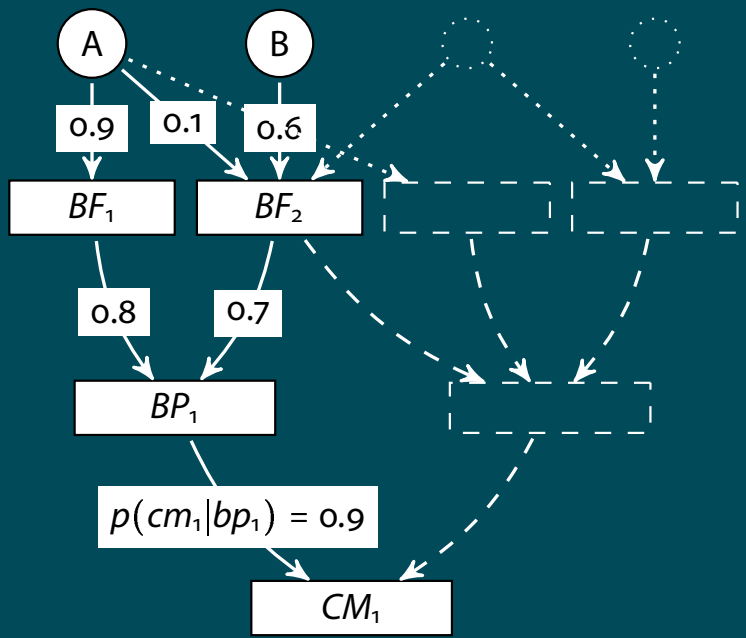
- Arcs represent dependencies as conditional probabilities
- "probability that a process fails, given that a business function fails"

View 1: Mission/Business Model



- A "company" consists of "business processes"
- "business processes" require "business functions/tasks"
- "business functions" are provided by "business devices"

View 1: Mission/Business Model



- Devices identified from operational view, e.g. identify a Frontend
- Crucial might be backend, supported by huge server clusters

→ Network View

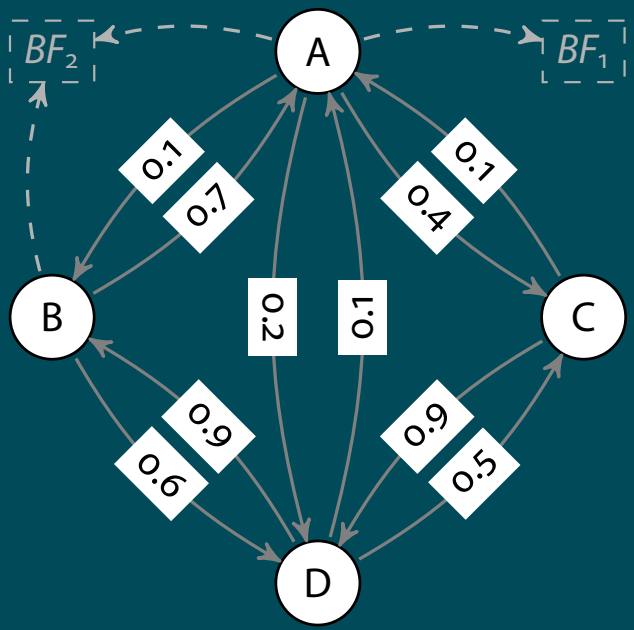
Probabilistic Preliminaries

Definition (Random Variables)

We represent every node inside our dependency models by a random variable, denoted as capital X, where every random variable is assignable to one of its possible values $x \in \mathrm{dom}(X)$. Let $P(X = x)$ denote the probability of random variable X having x as a value. For our case we consider $\mathrm{dom}(X) = \{true, false\}$ and we write x for the event $X = true$ and $\neg x$ for $X = false$.

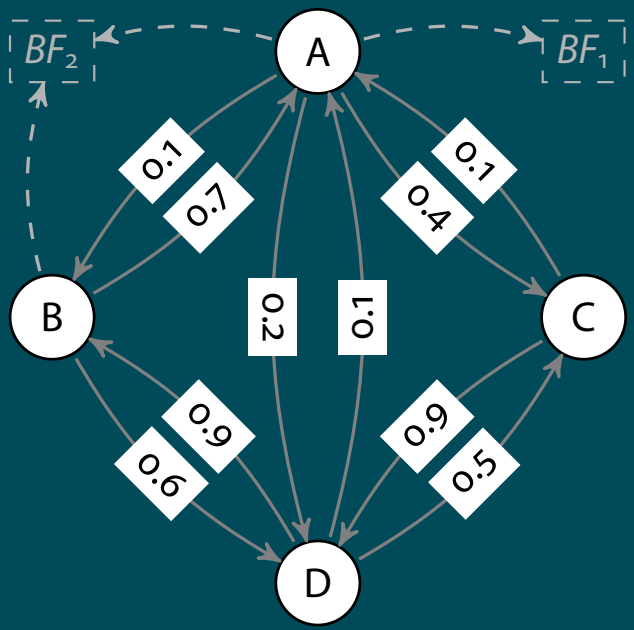
The event x represents the case that node X is operationally *impacted* and $\neg x$ that is is working at its fully operational capacity, i.e. no impact is present.

View 2: Network Model



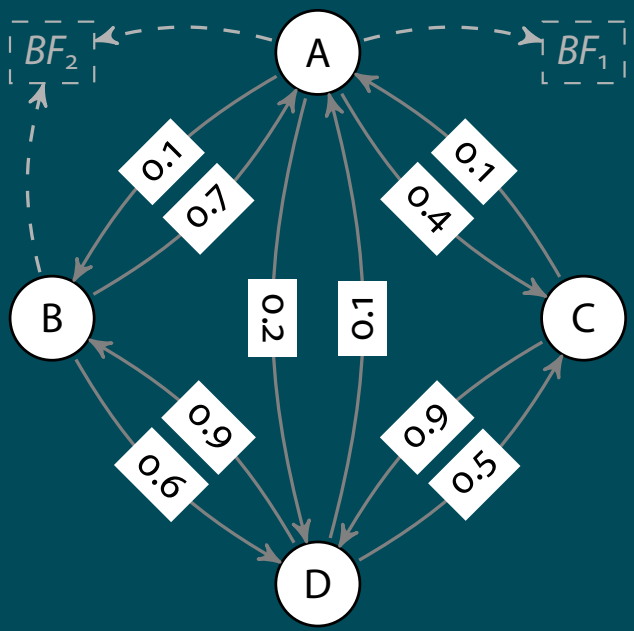
- Represents dependencies between nodes
- Nodes might be assets, buildings, computers, human resources
- Again, arcs represent dependencies as cond. probabilities.

View 2: Network Model



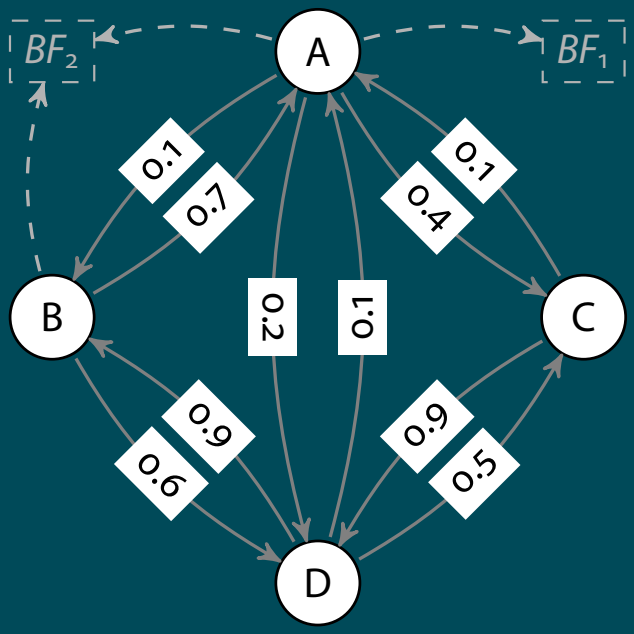
- Might not be feasible by hand
- Might not even be assessable by expert
- But verifiable for plausibility!

View 2: Network Model



- For usecase:
- Heuristic based on exchanged communication
- Reasonable assumption as long as single purpose nodes

View 2: Network Model



- Each of these nodes might become unavailable/compromised/stolen
- It might become impacted

→ Impacted due to an external event

View 3: External Shock Events

- Adapted from Reliability Analysis.
- Every node X might be affected by one or more external shock events $SE \in \vec{SE}$
- An external shock event $SE \in \vec{SE}$ might be present (se) or not be present ($\neg se$), for which a prior random distribution $P(SE)$ is defined.
- If se, there exists a probability of it affecting a node X, expressed as a local conditional probability fragment $p(x|se)$.
- If se and it is not inhibited, we speak of a *local impact* on x.

External Shock Events - Examples

- External Shock Events (ESEs) might be...

  Vulnerabilities, Attacks, Events, Conflicts, Observations, etc.
- *"Given that event, what is the probability of it locally affecting this device?"*

Example (Usecase - Response Plans)

A response to an attack might impact a node the same as the attack itself. The mitigation action "shutdown" of node *X* might heavily reduce the surface of an attack, but only completely inhibits this device. Therefore "shutdown" represents an external shock *se* event with $p(x|se) = 100\%$ local impact.

External Shock Events

Definition (Temporal Aspects)

We define a temporal aspect of an external shock event. We employ the idea of abstract timeslices in which the effect of an external shock event changes. Time-varying probabilities denoted as $\langle t_0 : p_0, \ldots, t_T : p_T \rangle$, where we have $T + 1$ abstract timeslices. In every abstract timeslice i, varying local impacts take their respective probability p_i defined for its time slice t_i.

Example (Usecase Excerpt - Patching)

Short term: Probability of immediate conflict, e.g. $p(x|se) = 10\%$
Midterm: Restart required, i.e. $p(x|se) = 100\%$.
Long term: Everything is running again, i.e. $p(x|se) = 0\%$.

$$\langle t_0 : 0.1, t_1 : 1.0, t_2 : 0.0 \rangle \tag{1}$$

Probabilistic Impact Assessment

- We have three views
- Some nodes "deep down" in the network might be impacted due to ESEs
- a node dependent on an impacted node *might* become impacted itself (network view)
- an identified business device might become impacted

→ might impact a function → might impact a process → might impact the complete company/mission (business view)

Definition (Mission Impact Assessment)

The probability of a mission node *MN* being impacted, is defined as the conditional probability of *MN* being impacted *mn* given all observed external shock events $se \in \vec{se}$, i.e. $P(mn|\vec{se})$, where the effects of local impacts due to $\vec{se}$ are mapped globally based on mission-dependency and network-dependency graphs.

Mathematical Problem

- Mission impact assessment is the task to calculate the probability $P(mn|\vec{se})$.
- With a noisy-or assumption, dependency networks form a probabilistic logic program determining the probability of connectivity between a MN and ESEs.
- This is a probabilistic path search.

Definition (Calculation)

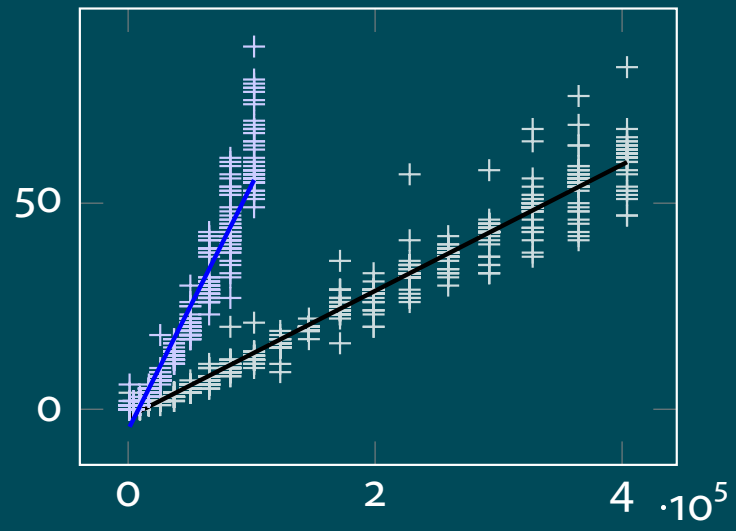
To calculate of $P(mn|\vec{se})$, every path w_i^{MN} from an external shock event $se \in \vec{se}$ to a mission node MN is a chain of probabilities and is sufficient to induce $\{MN = true\} = mn$. Every path exists with a probability $P(w_i^{MN})$, where $P(w_i^{MN})$ is the product of all probabilities in this path. Let $\mathbf{P}(w_i^{MN})$ denote the probability viewed as a set. $P(mn|\vec{se})$ is then the probability that at least one path exists. I.e.

$$P(mn|\vec{se}) = P(\bigvee_i w_i^{MN}) = \bigcup_i \mathbf{P}(w_i^{MN}), \quad (2)$$

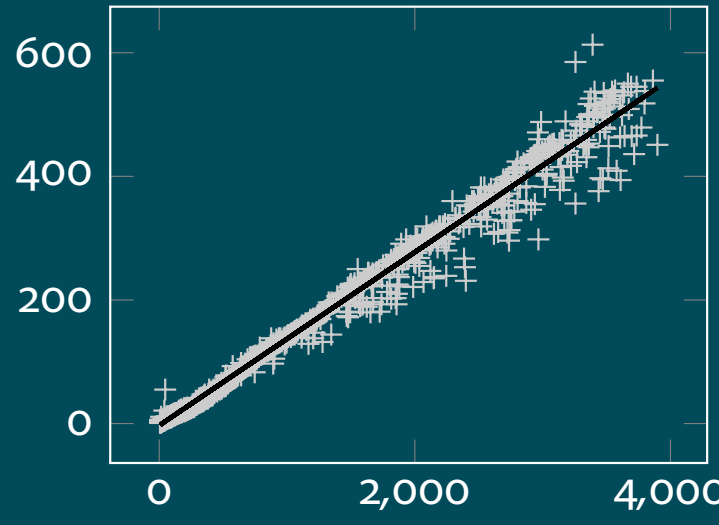
Monte Carlo Simulation

- Calculation of $\bigcup_i \mathbf{P}(w_i^{MN})$ is exponentially hard
- We use a Monte-Carlo simulation to approximate $P(\bigvee \vec{w}^{BD_i})$ for every business device $BD_i \in \vec{BD}$
- Has linear complexity with number of edges in network and number of shock events $\vec{SE}$.

$$t_{ps} = f(n_E)$$



$$t_{sim} = f(n_P)$$



Summary

- Three Views. Three experts.
- Focused on available and acquirable data.
- Tangible definitions of *local* conditional probabilities.
- Well formalized problem.
- Evaluation sound based on the probability axioms.
- Qualitative mission impact assessment.