International Institute for Applied Systems Analysis
IIASA www.iiasa.ac.at

Risk-based Selection of Mitigation Strategies for Cybersecurity of Electric Power Systems

Alessandro Mancuso[1,2], Piotr Żebrowski[3] and Aitor Couce Vieira[4]

[1]Politecnico di Milano (Italy),

[2]Aalto University (Finland),

[3]International Institute for Applied Systems Analysis,

[4]Institute of Mathematical sciences (Spain)

SRA-E 2019 conference

26 June 2019, Potsdam

Outline

- Introduction
- Standard practice and its deficiencies
- Probabilistic multi-dimensional risk assessment
- Portfolio optimization
- Summary

Introduction

Motivation:

- Extensive reliance on IT systems makes electric power grids vulnerable to cyber threats
- Impacts could be massive: cyber attack on Ukraininan power grids in 2015 resulted in power outage for 225 000 customers lasting up to six hours

Objective:

Selection of the **optimal portfolios of security measures** that reduce the susceptibility of power grids to cyber attacks.

Standard practice: a cyber threat scenario (Attack tree) as basic unit of analysis

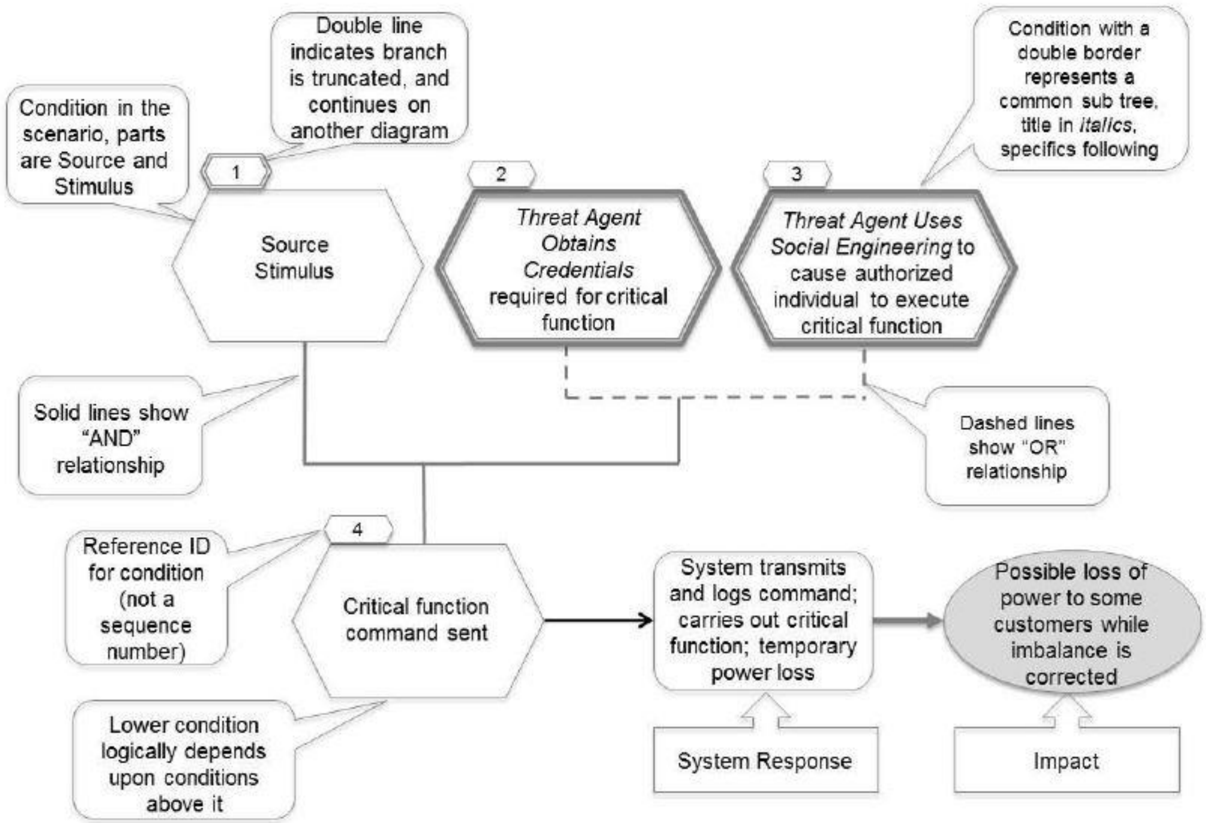


Figure 1
Graphical Notation for Annotated Attack Tree Format

Source: Lee, A., 2015. Analysis of selected electric sector high risk failure scenarios. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1.

Standard practice: impact assessment

- 14 impact criteria (dimensions)
- Score values in set {0, 1, 3, 9}
- Composite impact score $\sum_{k=1}^{14} IS_k$

Impact criterion	Scoring system
Public safety concern	0: none; 1: 10-20 injuries possible; 3: 100 injured possible; 9: one death possible.
Workforce safety concern	0: none; 3: any possible injury; 9: any possible death.
Ecological concern	0: none; 1: logical ecological damage such as localized fire or spill, repairable; 3: permanent local ecological damage; 9: widespread temporary or permanent damage to one or more ecosystems.
Financial impact of compromise on utility	0: petty cash or less; 1: up to 2% of utility revenue; 3: up to 5 %; 9: greater than 5 %.
Restoration costs	0: petty cash or less; 1: up to 1% of utility organization O&M budget; 3: up to 10%; 9: greater than 10%.
Negative impact on generation capacity	0: no effect; 1: small generation facility off-line or degraded operation of large facility; 3: more than 10% loss of generation capacity for 8 hours or less; 9: more than 10% loss of generation capacity for more than 8 hours.
Negative impact on the energy market	0: no effect; 1: localized price manipulation, lost transactions, loss of market participation; 3: price manipulation. lost transactions, loss of market participation impacting a large metro area; 9: market or key aspects of market non operational.
Negative impact on the bulk transmission system	0: no; 1: loss of transmission capability to meet peak demand or isolate problem areas; 3: major transmission system interruption; 9: complete operational failure or shut down of the transmission system.
Negative impact on customer service	0: no; 1: up to 4 hour delay in customer ability to contact utility and gain resolution, lasting one day; 3: up to 4 hour delay in customer ability to contact utility and gain resolution, lasting a week; 9: complete operational failure or shut-down of the transmission system.
Negative impact on billing functions	0: none; 1: isolated recoverable errors in customer bills; 3: widespread but correctible errors in bills; 9: widespread loss of accurate power usage data.
Damage to goodwill toward utility	0: no effect; 1: negative publicity but this does not cause financial loss to utility; 3: negative publicity causing up to 20% less interest in programs; 9: negative publicity causing more than 20% less interest in programs.
Immediate macro economic damage	0: none; 1: local businesses down for a week; 3: regional infrastructure damage; 9: widespread runs on banks.
Long term economic damage	0: none; 3: several years of local recession; 9: several years of national recession.
Loss of privacy	0: none; 1: 1000 or less individuals; 3: thousands of individuals; 9: millions of individuals.

Source:
Lee, A., 2015. Electric sector failure scenarios and impact analyses. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1.

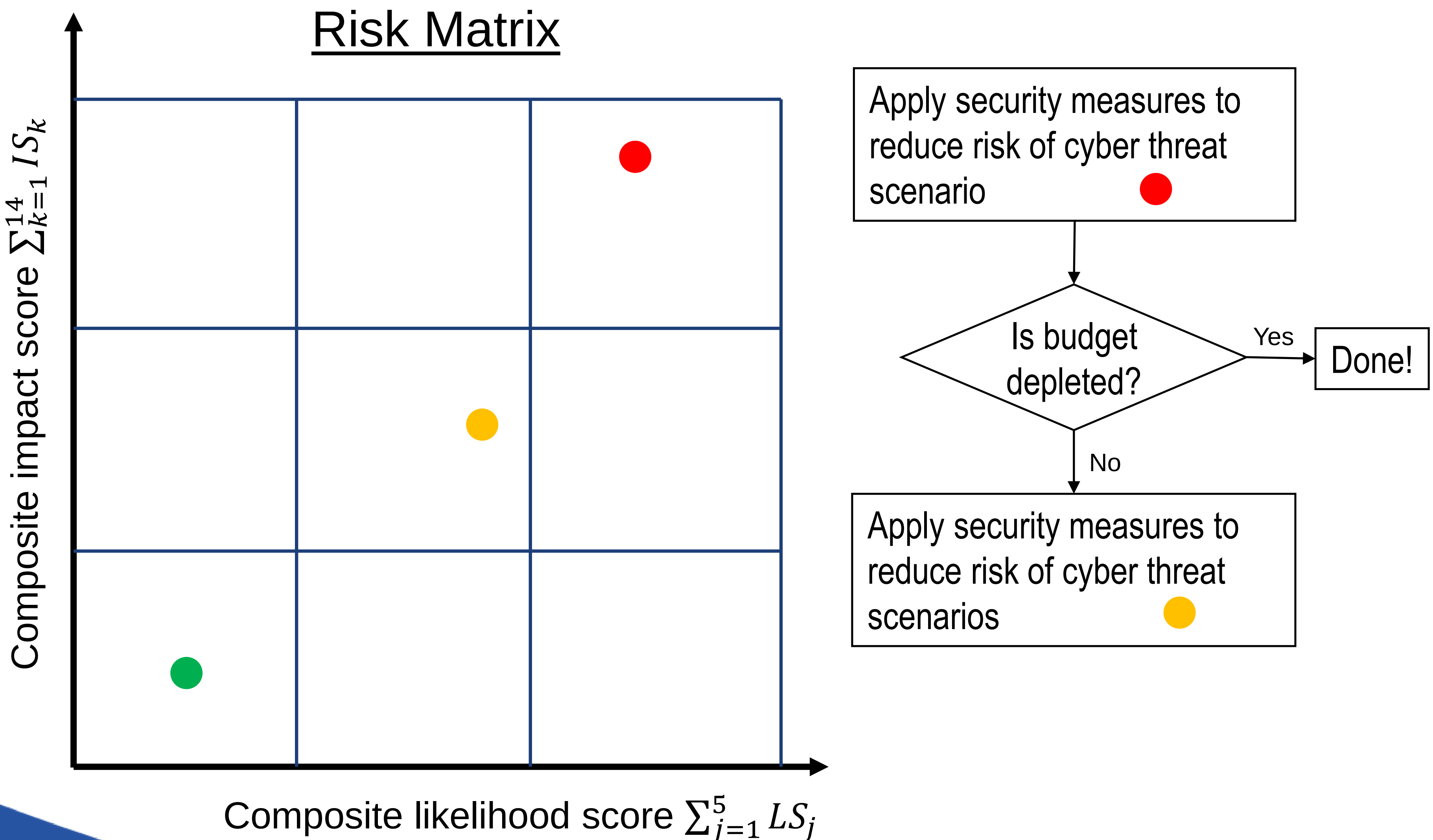
Standard practice: likelihood assessment

- 5 impact criteria
- Score values in set {0, 1, 3, 9}
- Composite likelihood score $\sum_{j=1}^{5} LS_j$

Likelihood criterion	Scoring system
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools; 1: Domain knowledge and cyber attack techniques; 3: Special insider knowledge needed; 9: Basic domain understanding and computer skills.
Accessibility (physical)	0: Inaccessible; 1: Guarded, monitored; Fence, standard locks; 9: Publicly accessible.
Accessibility (logical, assume have physical access)	0: High expertise to gain access; 1: Not readily accessible; 3: Publicly accessible but not common knowledge; 9: Common knowledge or none needed.
Attack vector (assume have physical and logical access)	0: Theoretical; 1: Similar attack has been described; 3: Similar attack has occurred; 9: Straightforward, for example script or tools available.
Common vulnerability among others	0: Isolated occurrence; 1: More than one utility; 3: Half or more of power infrastructure; 9: Nearly all utilities.

Source:
Lee, A., 2015. Electric sector failure scenarios and impact analyses. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1.

Standard practice: threats prioritization



Proposed improvements

Standard practice		Our framework
Analysis of individual threat scenarios	→	Integrated analysis of multiple threat scenarios
Aggregated composite impact score	→	Multiple impact dimensions
Likelihood score	→	Probabilisic model of cyber attacks

Case study: improving security of Advanced Metering Infrastructure (AMI)

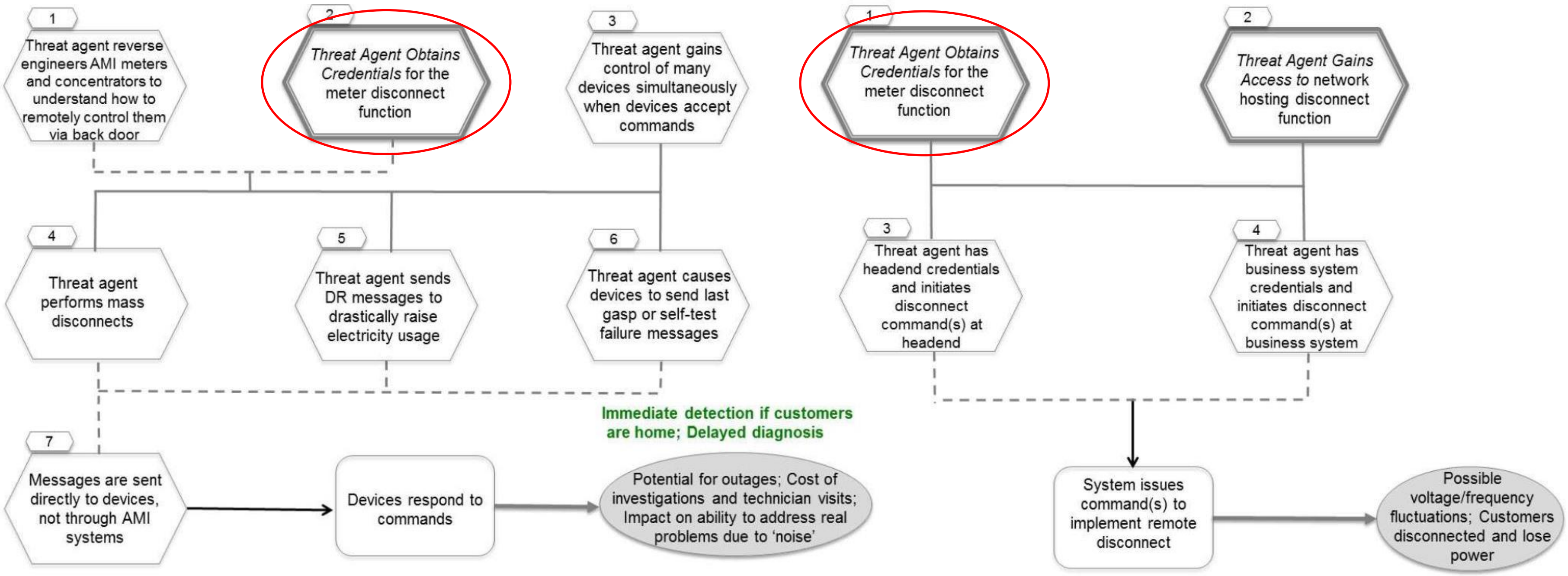
Security issues:

- AMI introduces large number of devices in widely dispersed and potentially insecure customers sites
- AMI allows for two-way communication with traditionally self-contained power systems.

Focus:

- 8 cyber threat scenarios with the highest priority for AMI systems
- 7 relevant impact dimensions considered (out of total 14 impact criteria considered in standard approach).

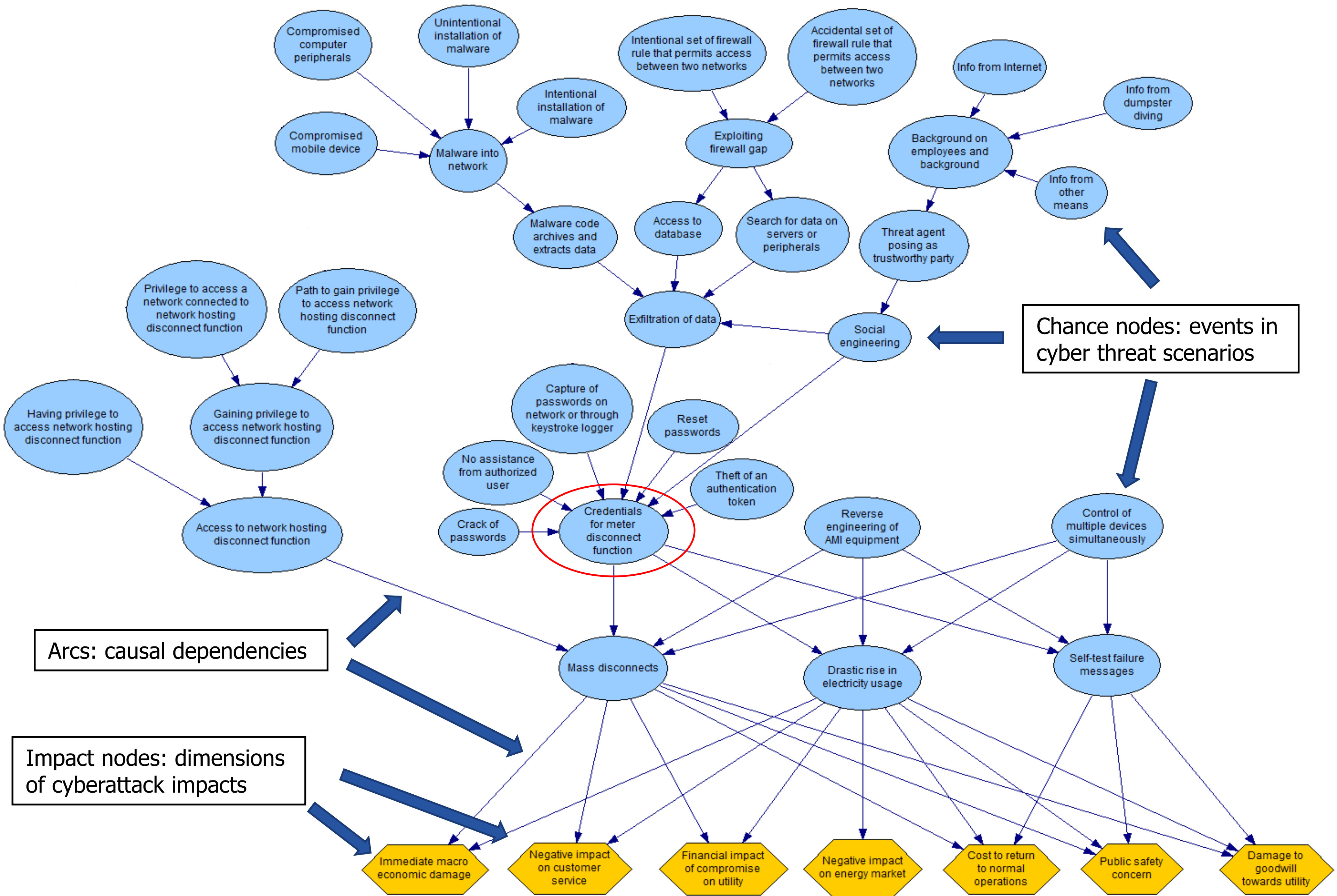
From individual attack graphs to integrated picture



”Reverse engineering of AMI equipment
allows unauthorized mass control”

”Invalid disconnect messages to meters impact customers and utility”

Graph of integrated attack scenarios



Probabilistic Risk Assessment with Bayesian Network

Turning integrated attack graph into a Bayesian Network:

- Attach a conditional probability table (CPT) to each node to represent occurance probabilities of corresponding event given the state of nodes on which it directly depends
- CPTs can be derived from: structure of attack graph (0-1 logical links), historical observations or expert judgements

For each impact dimension we define risk as:

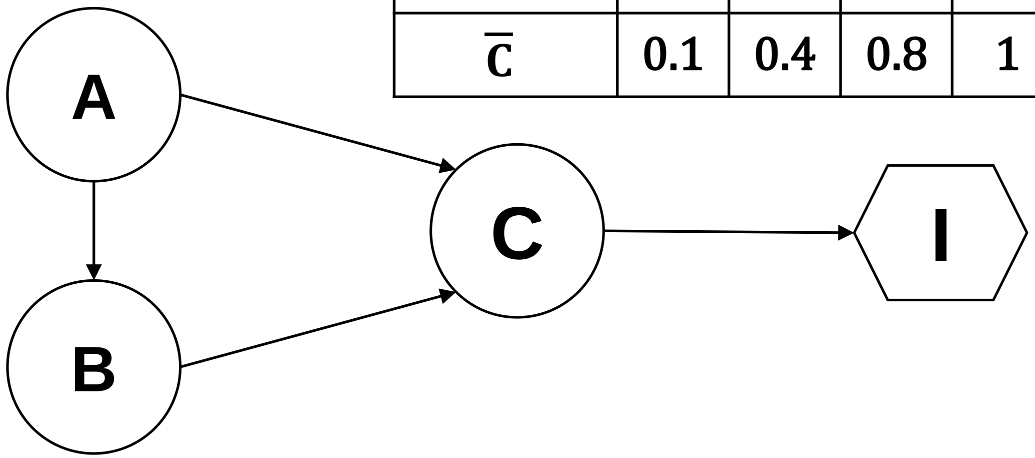
$$Risk_I = \textit{expected impact } I = \sum_{i \in IL} i \times P(I = i)$$

Where IL is the set of possible levels of impact I.

BN: a toy example

	A		$\bar{A}$	
	B	$\bar{B}$	B	$\bar{B}$
C	0.9	0.6	0.2	0
$\bar{C}$	0.1	0.4	0.8	1

A	0.4
$\bar{A}$	0.6



	I
C	9
$\bar{C}$	0

	A	$\bar{A}$
B	0.8	0.1
$\bar{B}$	0.2	0.9

$$\mathbb{P}(\mathbf{A}) = \mathbf{0.4}$$

$$\mathbb{P}(\mathbf{B}) = \mathbb{P}(\mathbf{B}|\mathbf{A}) \cdot \mathbb{P}(\mathbf{A}) + \mathbb{P}(\mathbf{B}|\bar{\mathbf{A}}) \cdot \mathbb{P}(\bar{\mathbf{A}}) = \mathbf{0.8} \cdot \mathbf{0.4} + \mathbf{0.1} \cdot \mathbf{0.6} = \mathbf{0.38}$$

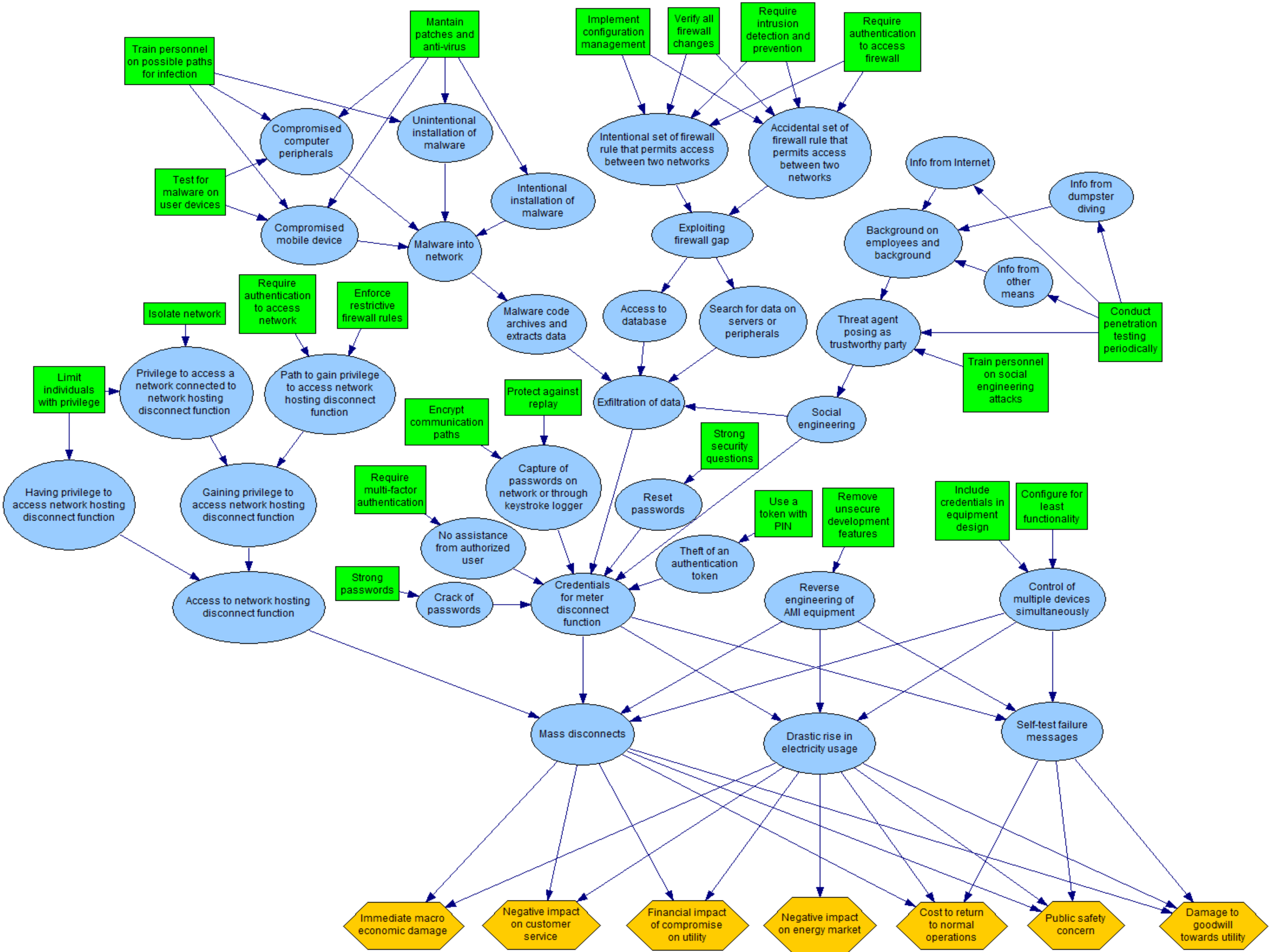
$$\begin{aligned} &\mathbb{P}(\mathbf{C}) \\ &= \mathbb{P}(\mathbf{C}|\mathbf{A},\mathbf{B}) \cdot \mathbb{P}(\mathbf{A}) \cdot \mathbb{P}(\mathbf{B}) + \mathbb{P}(\mathbf{C}|\bar{\mathbf{A}},\boldsymbol{B}) \cdot \mathbb{P}(\bar{\mathbf{A}}) \cdot \mathbb{P}(\mathbf{B}) + \mathbb{P}(\mathbf{C}|\mathbf{A},\bar{\boldsymbol{B}}) \cdot \mathbb{P}(\mathbf{A}) \cdot \mathbb{P}(\bar{\boldsymbol{B}}) \\ &+ \mathbb{P}(\mathbf{C}|\bar{\boldsymbol{A}},\bar{\boldsymbol{B}}) \cdot \mathbb{P}(\bar{\boldsymbol{A}}) \cdot \mathbb{P}(\bar{\boldsymbol{B}}) = \mathbf{0.348} \end{aligned}$$

$$\mathrm{E}[\mathbf{I}] = \mathbb{P}(\mathbf{C}) \cdot \boldsymbol{I}(\mathbf{C}) + \mathbb{P}(\bar{\mathbf{C}}) \cdot \boldsymbol{I}(\bar{\mathbf{C}}) = \mathbf{0.348} \cdot \mathbf{9} + \mathbf{0.652} \cdot \mathbf{0} = \mathbf{3.132}$$

Options for risk reduction

Index	Security measure	Index	Security measure
1	Train personnel on possible paths for infection	12	Protect against replay
2	Maintain patches and anti-virus	13	Strong security questions
3	Test for malware before connection	14	Require multi-factor authentication
4	Implement configuration management	15	Use a token with PIN
5	Verify all firewall changes	16	Limit individuals with privilege
6	Require intrusion detection and prevention	17	Isolate network
7	Require authentication to access firewall	18	Enforce restrictive firewall rules
8	Conduct penetration testing periodically	19	Require authentication to access network
9	Train personnel on social engineering attacks	20	Remove unsecure development features
10	Strong passwords	21	Include credentials in equipment design
11	Encrypt communication paths	22	Configure for least functionality

- Each security measure is applied to a specific chance node

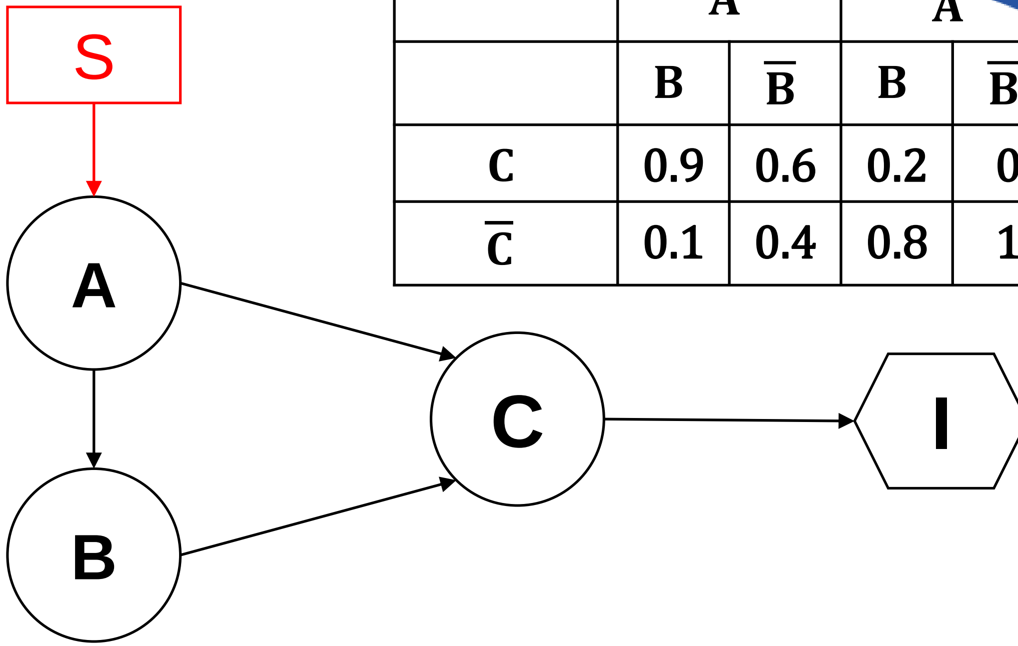


Train personnel on possible paths for infection
Mantain patches and anti-virus
Implement configuration management
Verify all firewall changes
Require intrusion detection and prevention
Require authentication to access firewall
Compromised computer peripherals
Unintentional installation of malware
Intentional set of firewall rule that permits access between two networks
Accidental set of firewall rule that permits access between two networks
Info from Internet
Info from dumpster diving
Test for malware on user devices
Intentional installation of malware
Compromised mobile device
Malware into network
Exploiting firewall gap
Background on employees and background
Info from other means
Require authentication to access network
Enforce restrictive firewall rules
Isolate network
Malware code archives and extracts data
Access to database
Search for data on servers or peripherals
Threat agent posing as trustworthy party
Conduct penetration testing periodically
Train personnel on social engineering attacks
Limit individuals with privilege
Privilege to access a network connected to network hosting disconnect function
Path to gain privilege to access network hosting disconnect function
Protect against replay
Encrypt communication paths
Exfiltration of data
Social engineering
Strong security questions
Capture of passwords on network or through keystroke logger
Reset passwords
Require multi-factor authentication
Having privilege to access network hosting disconnect function
Gaining privilege to access network hosting disconnect function
Use a token with PIN
Remove unsecure development features
Include credentials in equipment design
Configure for least functionality
No assistance from authorized user
Theft of an authentication token
Strong passwords
Crack of passwords
Credentials for meter disconnect function
Access to network hosting disconnect function
Reverse engineering of AMI equipment
Control of multiple devices simultaneously
Mass disconnects
Drastic rise in electricity usage
Self-test failure messages
Immediate macro economic damage
Negative impact on customer service
Financial impact of compromise on utility
Negative impact on energy market
Cost to return to normal operations
Public safety concern
Damage to goodwill towards utility

Options for risk reduction

Index	Security measure	Index	Security measure
1	Train personnel on possible paths for infection	12	Protect against replay
2	Maintain patches and anti-virus	13	Strong security questions
3	Test for malware before connection	14	Require multi-factor authentication
4	Implement configuration management	15	Use a token with PIN
5	Verify all firewall changes	16	Limit individuals with privilege
6	Require intrusion detection and prevention	17	Isolate network
7	Require authentication to access firewall	18	Enforce restrictive firewall rules
8	Conduct penetration testing periodically	19	Require authentication to access network
9	Train personnel on social engineering attacks	20	Remove unsecure development features
10	Strong passwords	21	Include credentials in equipment design
11	Encrypt communication paths	22	Configure for least functionality

- Each security measure is applied to a specific chance node
- It reduces the occurance probability of the event a node represents
- Bayesian Networks enable **probability update** on the cascading events of the cyber threat scenarios.



A	0.2
$\bar{A}$	0.8

	A	$\bar{A}$
B	0.8	0.1
$\bar{B}$	0.2	0.9

	A		$\bar{A}$	
	B	$\bar{B}$	B	$\bar{B}$
C	0.9	0.6	0.2	0
$\bar{C}$	0.1	0.4	0.8	1

	I
C	9
$\bar{C}$	0

$$\mathbb{P}(\mathbf{A}) = \mathbf{0.2}$$

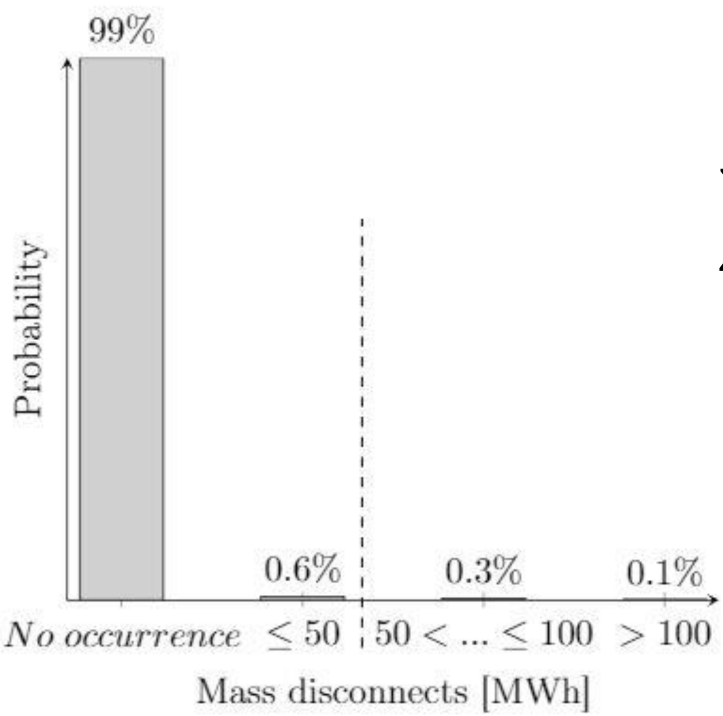
$$\mathbb{P}(\mathbf{B}) = \mathbb{P}(\mathbf{B}|\mathbf{A}) \cdot \mathbb{P}(\mathbf{A}) + \mathbb{P}(\mathbf{B}|\bar{\mathbf{A}}) \cdot \mathbb{P}(\bar{\mathbf{A}}) = \mathbf{0.8} \cdot \mathbf{0.2} + \mathbf{0.1} \cdot \mathbf{0.8} = \mathbf{0.24}$$

$$\mathbb{P}(\mathbf{C}) = \mathbb{P}(\mathbf{C}|\mathbf{A},\mathbf{B}) \cdot \mathbb{P}(\mathbf{A}) \cdot \mathbb{P}(\mathbf{B}) + \mathbb{P}(\mathbf{C}|\bar{\mathbf{A}},\boldsymbol{B}) \cdot \mathbb{P}(\bar{\mathbf{A}}) \cdot \mathbb{P}(\mathbf{B}) + \mathbb{P}(\mathbf{C}|\mathbf{A},\bar{\boldsymbol{B}}) \cdot \mathbb{P}(\mathbf{A}) \cdot \mathbb{P}(\bar{\boldsymbol{B}}) + \mathbb{P}(\mathbf{C}|\bar{\boldsymbol{A}},\bar{\boldsymbol{B}}) \cdot \mathbb{P}(\bar{\boldsymbol{A}}) \cdot \mathbb{P}(\bar{\boldsymbol{B}}) = \mathbf{0.184}$$

$$\mathrm{R}[\mathbf{I}] = \mathbb{P}(\mathbf{C}) \cdot \boldsymbol{I}(\mathbf{C}) + \mathbb{P}(\bar{\mathbf{C}}) \cdot \boldsymbol{I}(\bar{\mathbf{C}}) = \mathbf{0.184} \cdot \mathbf{9} + \mathbf{0.816} \cdot \mathbf{0} = \mathbf{1.656}$$

Portfolio of security measures

- A portfolio is a combintion of security measures, represented by a binary z such that $z_a = 1$ iff security measure a belongs to the portfolio.
- A portfolio must satisfy budget and technical constraints:



$$\sum_a \boldsymbol{z}_a \cdot \boldsymbol{c}_a \leq B$$ ⇨ Budget

$$\sum_s \mathbb{P}[X = s|\boldsymbol{z}] \leq \varepsilon$$ ⇨ Risk acceptability

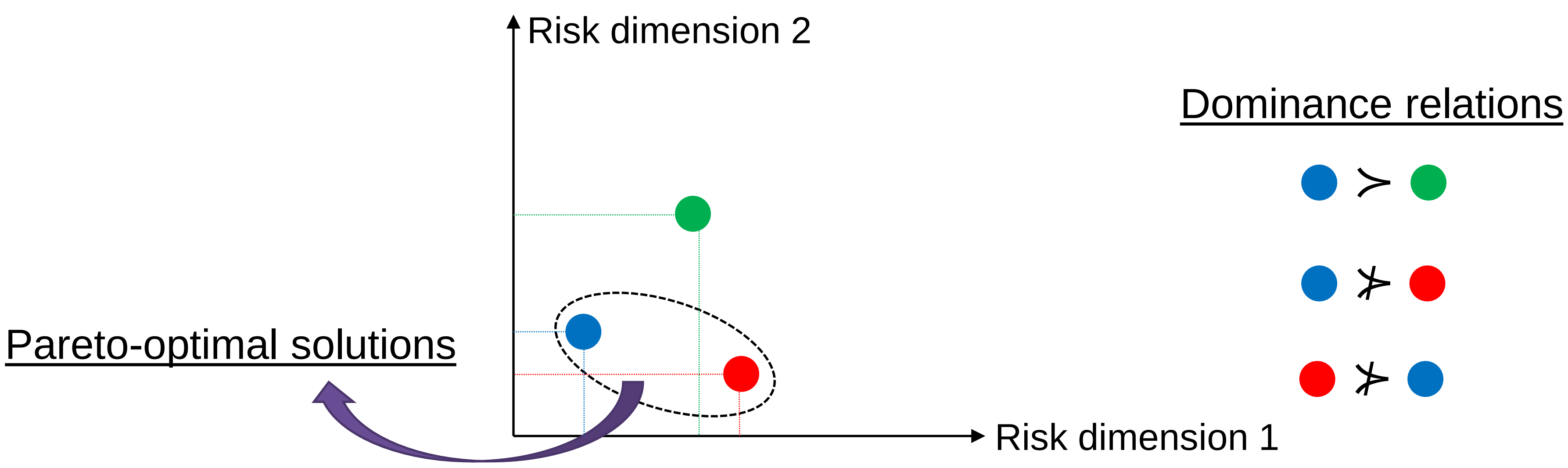
$$\boldsymbol{z}_{a'} + \boldsymbol{z}_{a''} \leq 1$$ ⇨ Mutually exclusive

$$\boldsymbol{z}_{a'} - \boldsymbol{z}_{a''} = 0$$ ⇨ Mutually inclusive

Goal: to find Pareto-optimal portfolios

A portfolio is Pareto-optimal if there is no other feasible portfolio that further reduces the risks in any of impact dimesnion I_k without increasing the risk in any other dimension

$$\boldsymbol{z}^* \succ \boldsymbol{z} \leftrightarrow \begin{cases} R[I_k](\boldsymbol{z}^*) \leq R[I_k](\boldsymbol{z}) & \text{for all } k \\ R[I_k](\boldsymbol{z}^*) < R[I_k](\boldsymbol{z}) & \text{for some } k \end{cases}$$



Computing the set of Pareto-optimal portfolios (Pareto front)

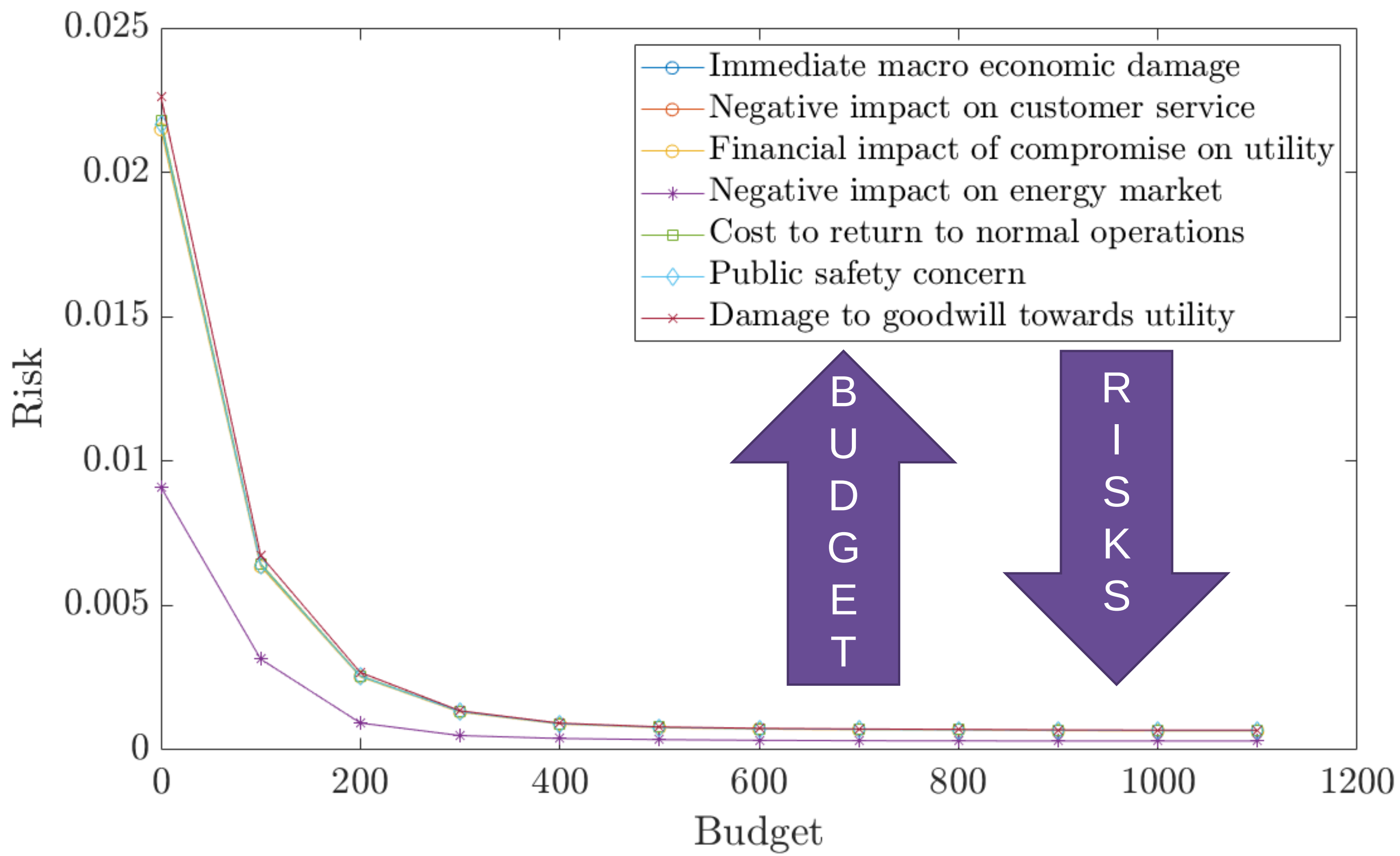
Input:

- Set of security measures
- Budget and technical constraints

Method: Implicit enumeration algorithm (Mancuso et al. 2019)

- Computationally efficient: intelligent search over 2^N portfolios, explores only subspace containing good candidates for Pareto-optimal portfolios
- Scalability: time consuming for large portfolios of security measures (>40)

Risk profiles (envelope of Pareto front)



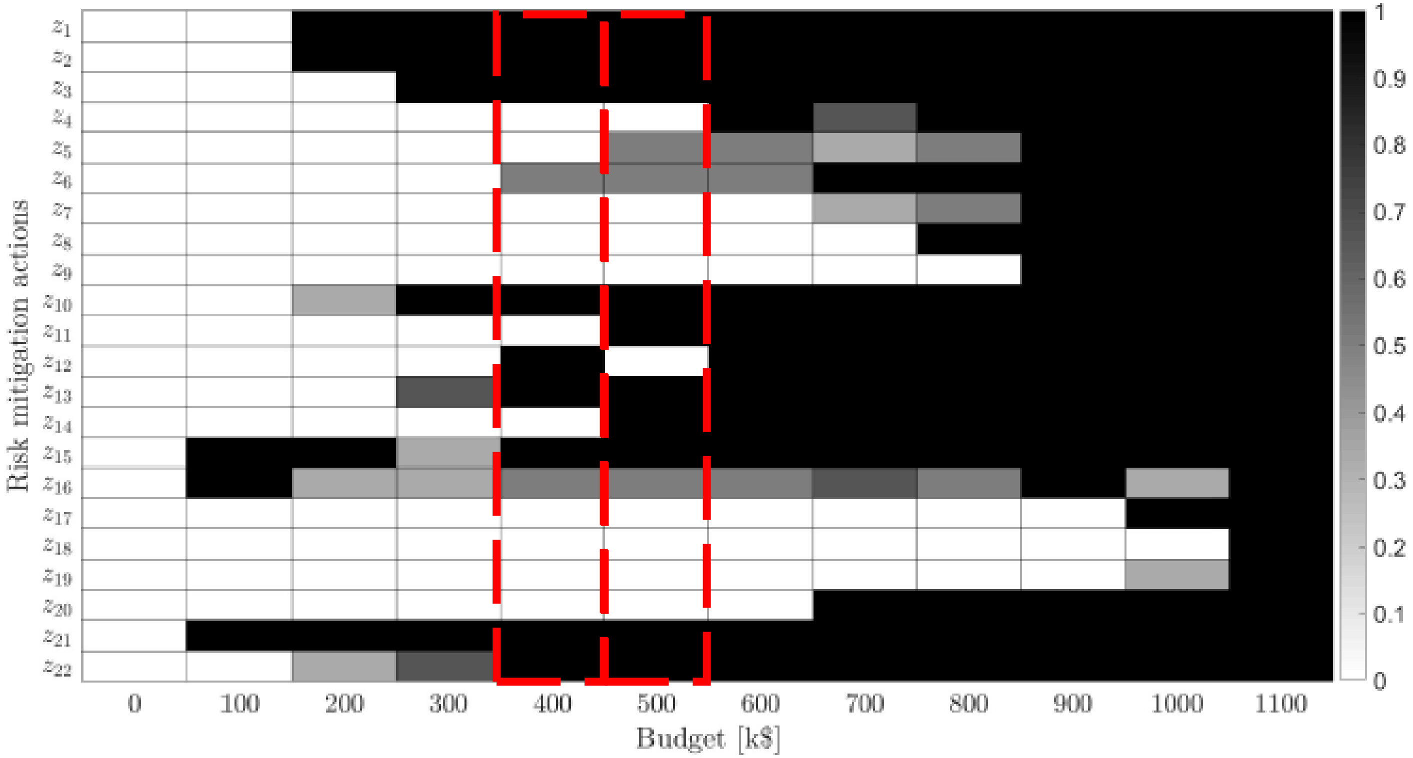
Picking a Pareto-optimal portfolio

- Set of Pareto optimal portfolios is large
- Possible guidance offered by the core index (Liesiö *et al.* 2008)

$$CI(a) = \frac{\text{No. of Pareto} - \text{optimal portfolios containing } a}{\text{No. of all Pareto} - \text{optimal portfolios}}$$

- Interpretation: high $CI(a)$ implies that a belongs to the core i.e., subset of measures shared by all Pareto-optimal portfolios (for given constraints).

Core index map for selection of security measures



Summary

- Quantitative extension of qualitative standard practice
- Systemic perspective:
  - Different threat scenarios analysed jointly
  - Different risk dimensions represented explicitly
  - Taking advantage of synergies between mitigation actions
- Probabilistic approach:
  - Natural representation of likelihoods, framework for rigorous likelihood calculus
  - Bayesian Network:
    - Probabilistic model of cascading events leading to successful cyber attacks
    - Conditional probabilities: tractable and (relatively) easy to estimate
    - Allow to calculate contribution of portfolios of security measures to reduction of risks
- Risks understood as expected impacts
- Optimization
  - Multi-objective
  - Representation of budget and technical constraints
  - Efficient algorithm of computing the set of Pareto-optimal portfolios of mitigation actions

Thank you for your attention!

Questions?

Piotr Żebrowski
IIASA, Advanced Systems Analysis program
zebrowsk@iiasa.ac.at

Optimization algorithm

The selection of Pareto optimal portfolios is performed through an **implicit enumeration algorithm**.

Cost vector

30	40	30	20	50	20	60	40	30	50

Budget=100

1	1/0	1/0	0	0	0	0	0	0	0

Saving 2^7 portfolio evaluations!

1	1	0	1/0	0	1/0	0	0	0	0

Saving 2^4 portfolio evaluations!