A Subjective Network Approach for Cybersecurity Risk Assessment

Nasser Al-Hadhrami
Department of Computing Science, University of Aberdeen, UK

Email: r01nama@abdn.ac.uk

Introduction

- Cybersecurity incidents (e.g., cyber-attacks) have been a main problem that faces organizations.
- Security analysts must properly respond to them, and take action to avoid their serious impacts.
- Responding to cybersecurity incidents requires *efficient evaluation* of their risks.

Limitations in Existing Approaches

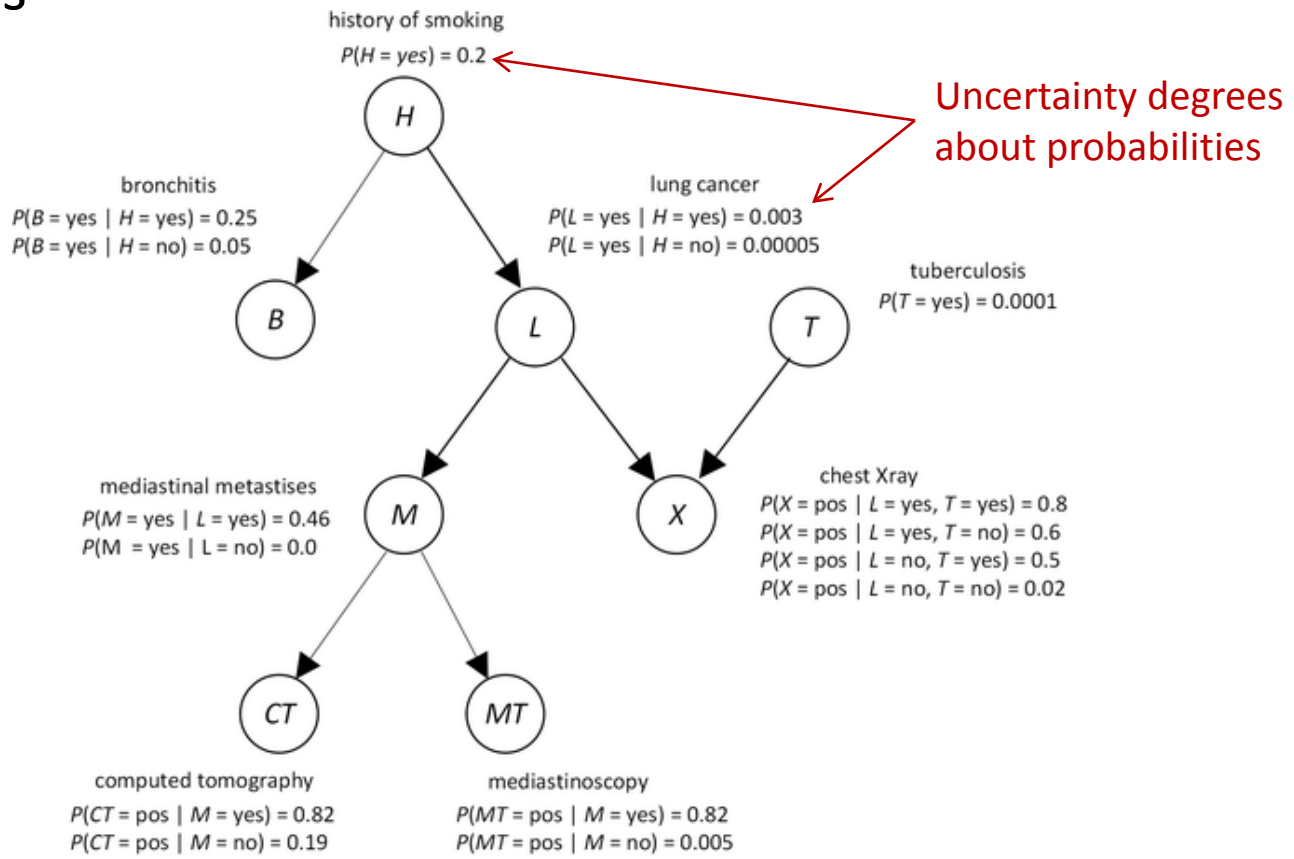
$$Risk = probability \times impact$$

- Difficult to elicit accurate probabilities
- Sources of evidence may not be trustworthy
- So, there is uncertainty about probability values

- Impact on what?
- No detailed analysis of the consequences
- No consideration of possible mitigating events

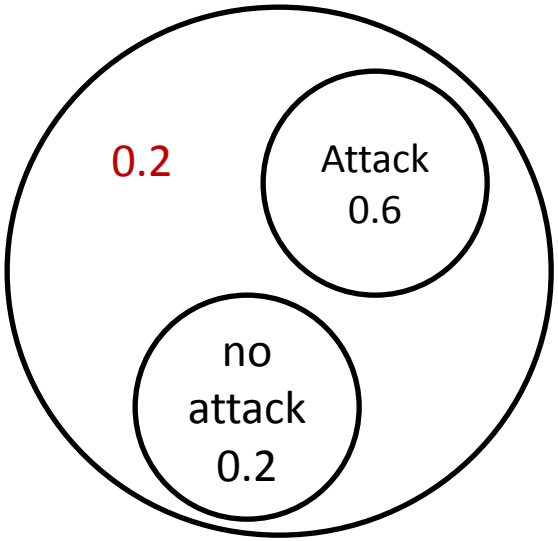
So, What We Need?

- A cause-effect model (e.g., Bayesian networks)
- Additionally, the model captures *uncertainty* about probabilities



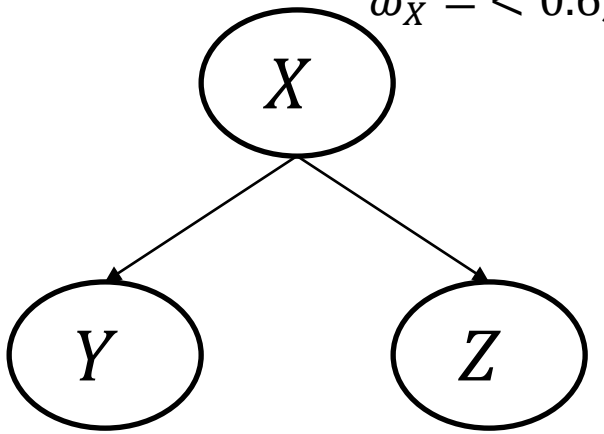
Subjective Bayesian Networks

- A generalisation of classical BNs.
- Probability distributions associated with the nodes are replaced with *subjective opinions* about them.
- An opinion is a tuple $\omega_x = < b_x, d_x, u_x, a_x >$.



$\omega_{attack} = < 0.6, 0.2, 0.2, 0.5 >$

$\omega_X = < 0.6, 0.2, 0.2, 0.5 >$

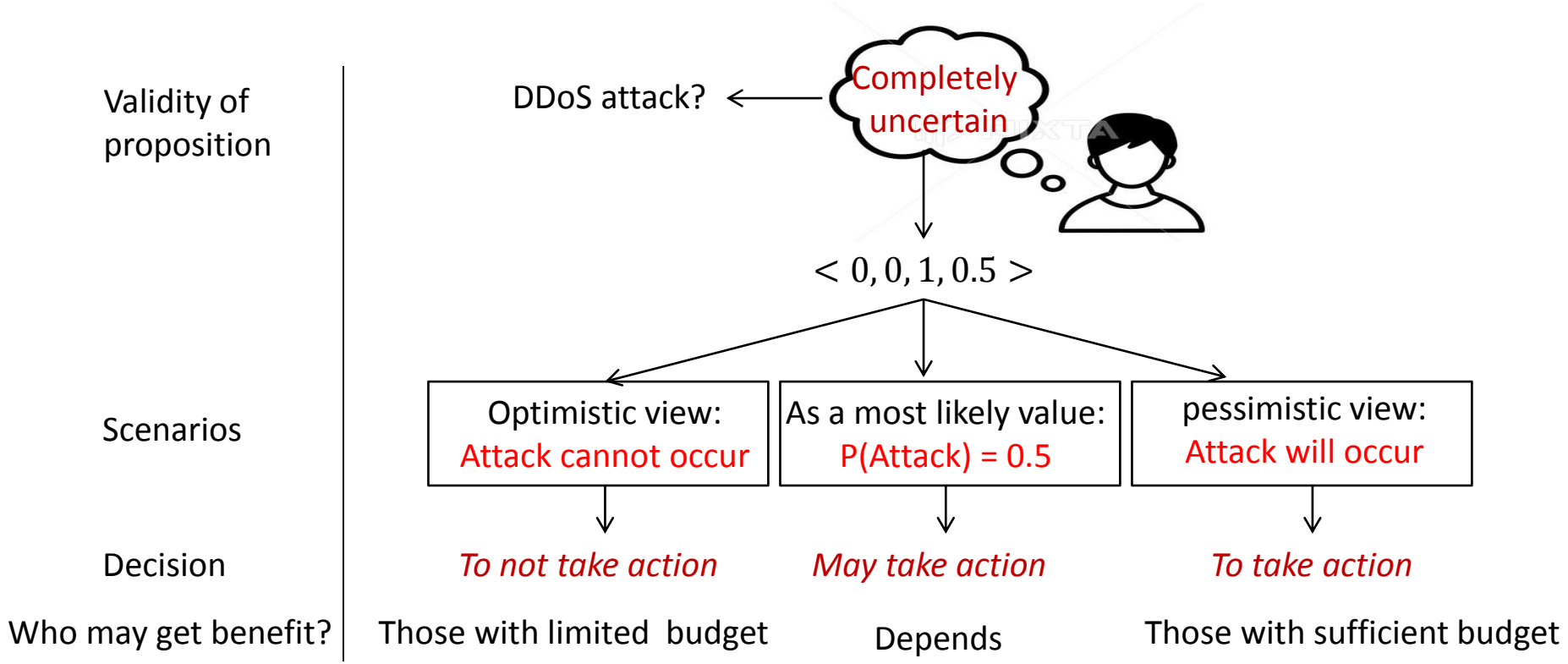


COT at node Y
$\omega_{Y\|x} = \langle 0.7, 0.15, 0.15 \rangle$
$\omega_{Y\|\dot{x}} = \langle 0.1, 0.85, 0.05 \rangle$

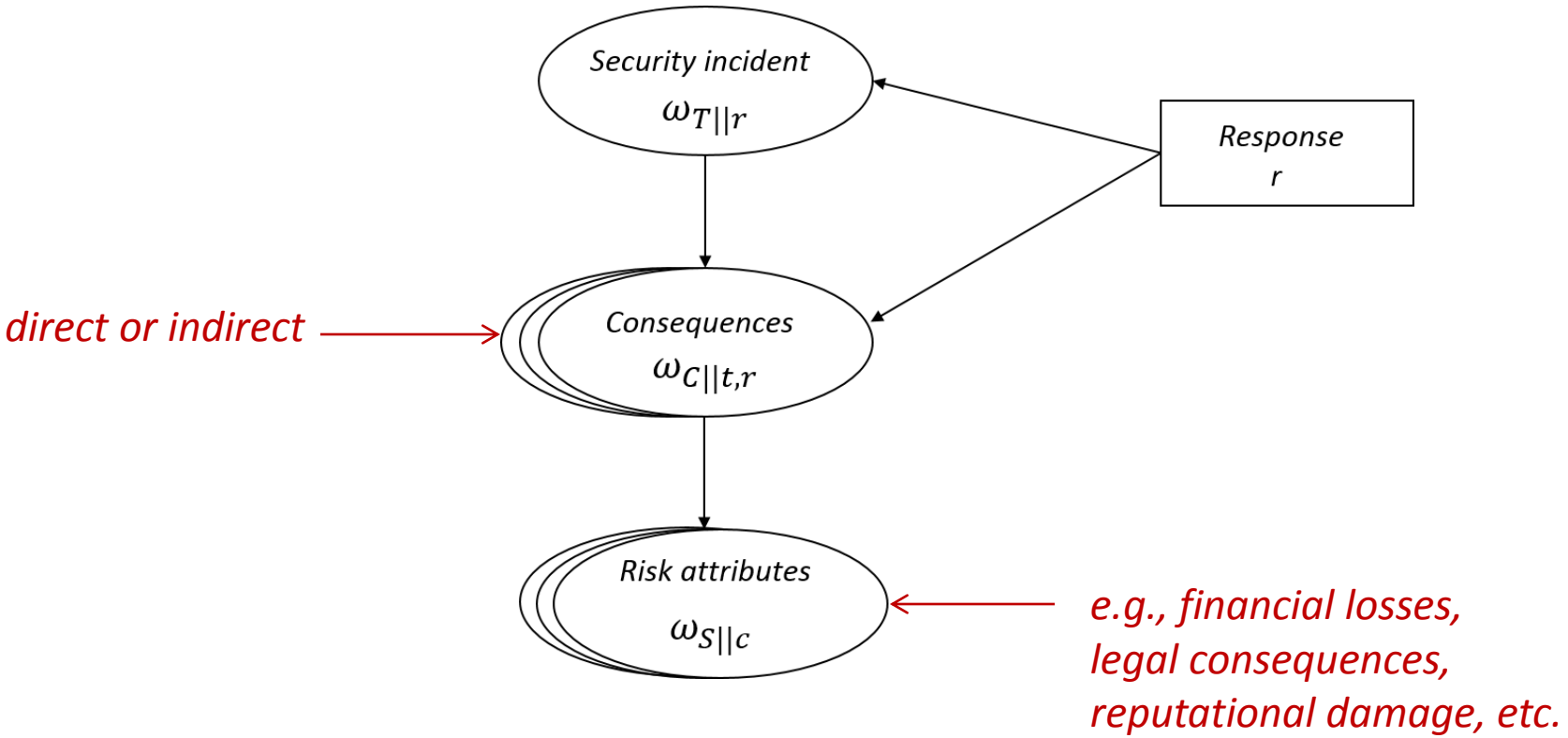
COT at node Z
$\omega_{Z\|x} = \langle 0.90, 0.00, 0.10 \rangle$
$\omega_{Z\|\bar{x}} = \langle 0.20, 0.60, 0.20 \rangle$

Why Should Uncertainty be Modelled?

- Different outcomes, and so different security decisions.
- Flexibility to decision-making process, especially when considering, e.g., risk attitudes or security investment budget.



SBN Model for Risk Assessment



Risk Evaluation

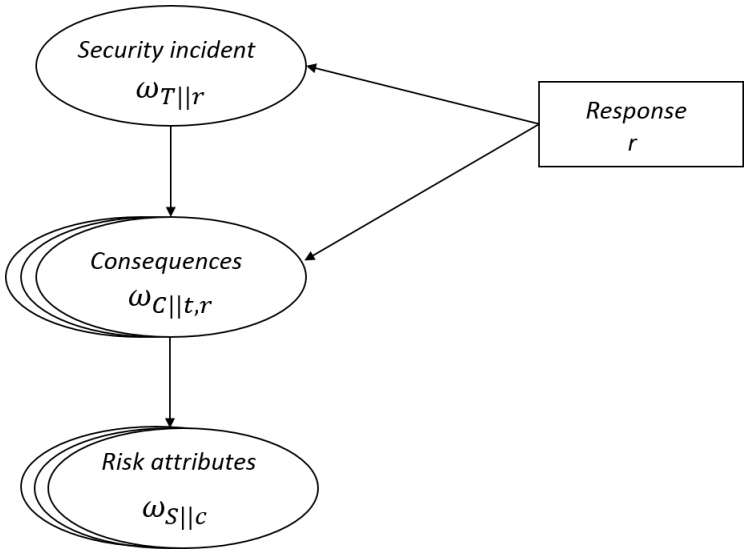
- Potential damage at an attribute node (S_j):

$$D_{S_j} = P(S_j) \cdot W_j \cdot V_i(S_j)$$

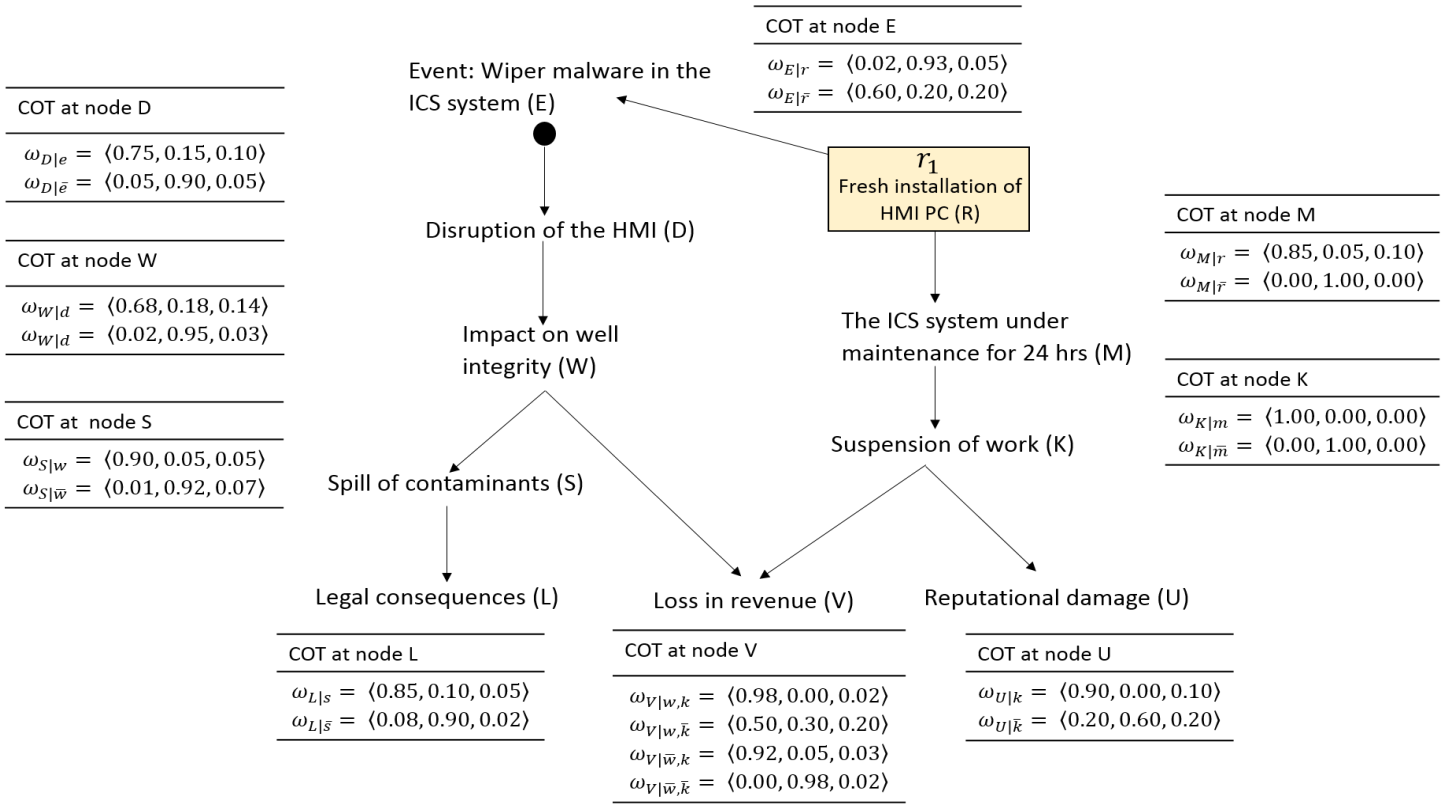
- Risk index: $RI_r = \sum_{j=1}^{n} D_{S_j}.$

- Security Response Effectiveness:

$$SRE(r_j) = \frac{RI_{r_0} - RI_{r_j}}{RI_{r_0}} \times 100,$$



Example



Risk index with no response	Risk index with r_1	Security decision
0.248	0.397	should not enforce r_1

Experimental Results

- We used the scenario of wiper malware.
- We generated three sets of probability values form the opinions (assuming they represent the truth values).
- We used these probabilities and inference approach in BNs to compute risk in the three experiments.
- We compared the results in the two approaches.
- Different outcomes… different decisions.

Approach		Risk index with r_0	Risk index with r_1	Security decision
SBN approach		0.248	0.397	enforce r_0
Probabilistic approach	Exp.1	0.185	0.175	enforce r_1
	Exp.2	0.116	0.105	enforce r_1
	Exp.3	0.137	0.144	enforce r_0

Conclusions

- A new risk assessment model that takes uncertainty about probabilities into account, using subjective Bayesian networks.
- The model formalises risk as multi-consequence.
- The model offers flexibility to decision-making process.
- The evaluation showed that taking uncertainty about probabilities into account may lead to different outcomes, and therefore different decisions.

References

- Jøsang, A. (2016). *Subjective logic*. Heidelberg: Springer.
- Jøsang, A., & Kaplan, L. (2016, July). Principles of subjective networks. In *2016 19th International Conference on Information Fusion (FUSION)* (pp. 1292-1299). IEEE.