SARNET: Secure Autonomous Response Networks

Social Computational Trust Model (SCTM):
A Framework to Facilitate the Selection of Partners

Ameneh Deljoo[1], Tom van Engers[2], Leon Gommans[1,3] , and **Cees de Laat[1]**
[1]Systems and Networking Lab, University of Amsterdam
[2]Leibniz Center for Law, University of Amsterdam
[3]AirFrance-KLM, Amsterdam
a.deljoo@uva.nl

Supported by NWO and C2D grants
SARNET, DL4LD and NWA VWDATA.

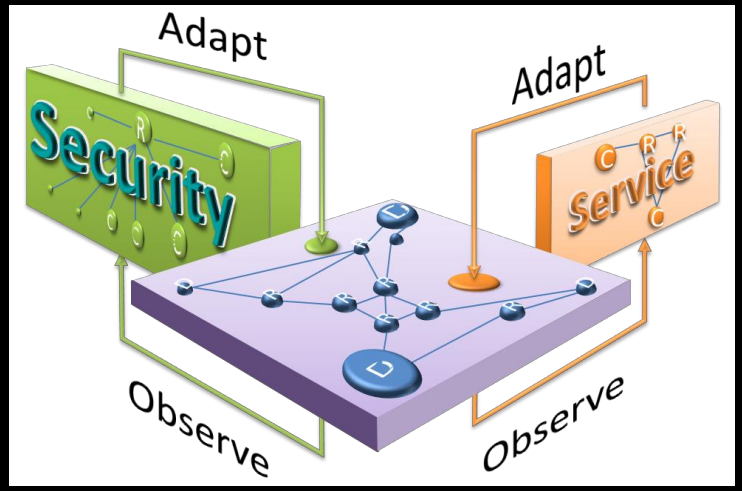
SARNET: Security Autonomous Response with programmable NETworks

Marc Lyonnais, Leon Gommans, Rodney Wilson, Rob Meijer,
Frank Fransen Tom van Engers, Paola Grosso, Gauravdeep Shami, Cees de Laat,
Ameneh Deljoo, Ralph Koning, Ben de Graaff, Gleb Polevoy, Stojan Travanovski.

Big Data: real time ICT for logistics
Data Logistics 4 Logistics Data (dl4ld)

Robert Meijer, TNO, PI, Cees de Laat, UvA, Co-PI, Leon Gommans, KLM

Cyber security program SARNET



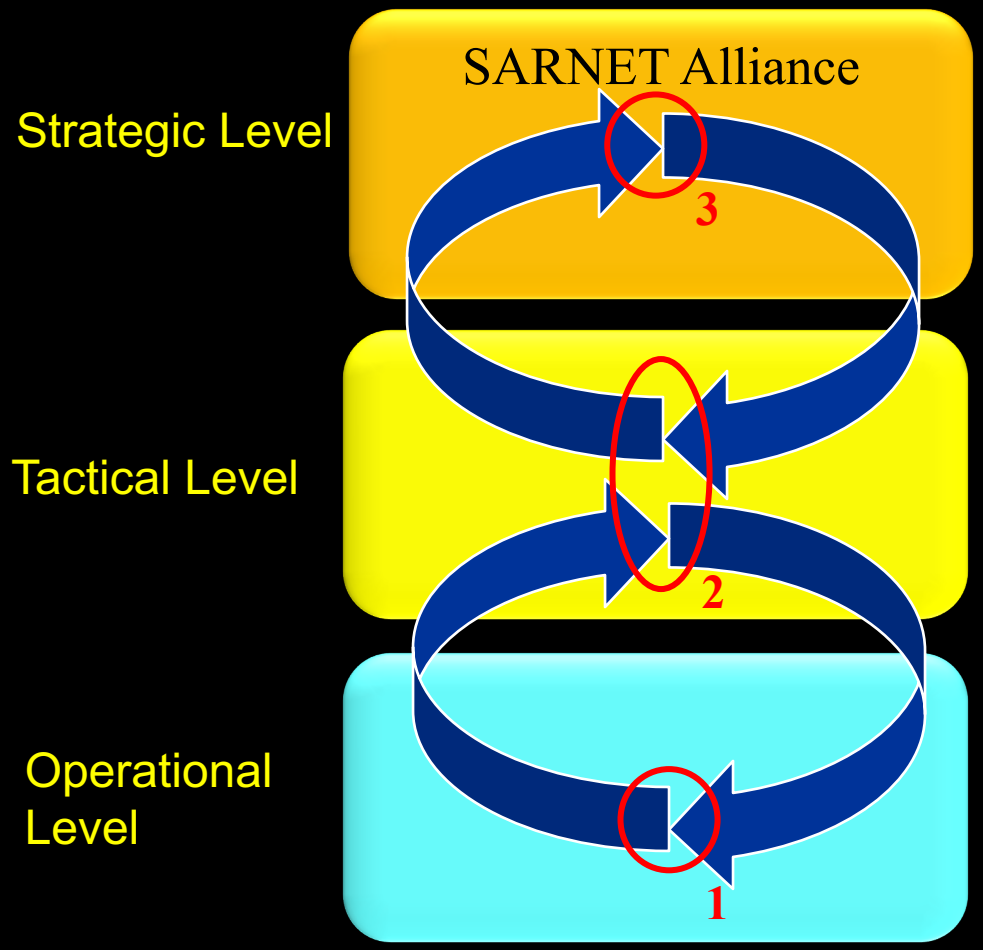
Research goal is to obtain the knowledge to create ICT systems that:

- model their state (situation)
- discover by observations and reasoning if and how an attack is developing and calculate the associated risks
- have the knowledge to calculate the effect of counter measures on states and their risks
- choose and execute one.

In short, we research the concept of networked computer infrastructures exhibiting SAR: Security Autonomous Response.

Context & Goal

Security Autonomous Response NETwork Research

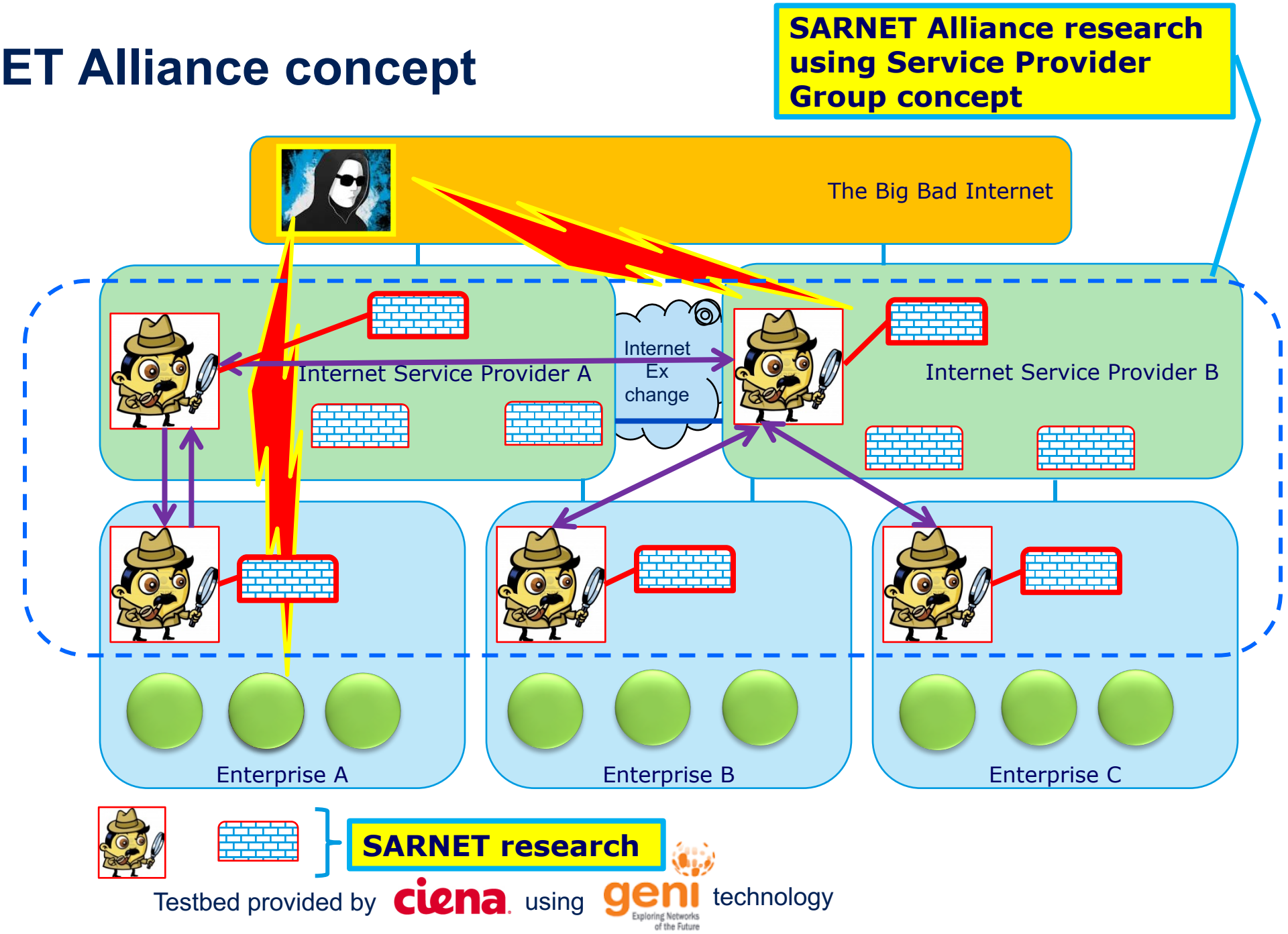


Ameneh Deljoo (PhD):
Why create SARNET Alliances?
Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders (3)

Gleb Polevoy (PD):
Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state, KPI information (2) keeping in mind strategic motifs (3).

Ralph Koning (PhD)
Ben de Graaff (SP):
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g cost)

SARNET Alliance concept

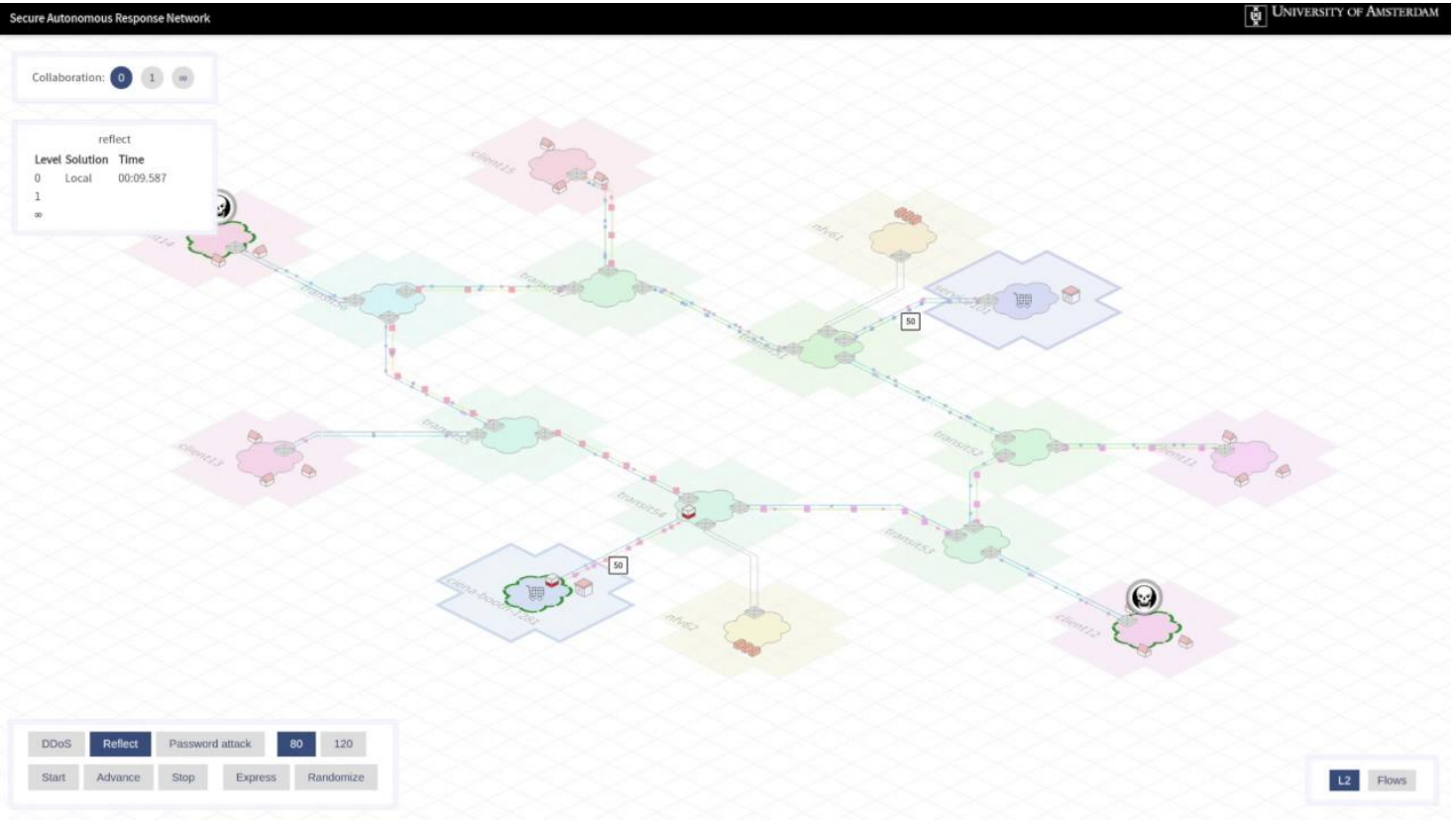


SARNET Alliance concept demos

See SC17 proof of concepts:

http://delaat.net/sc/sc17/

http://delaat.net/sc/sc17/demo01/index.html



Multi-Domain Autonomous mitigation of Cyber Attacks

Demonstration at Ciena booth #1281

Ralph Koning, Ben de Graaff, Paola Grosso, Robert Meijer, Cees de Laat

SARNET

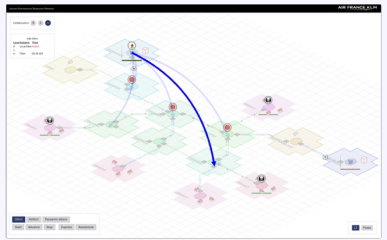
SARNET, Secure Autonomous Response NETworks, is a project funded by the Dutch Research Foundation. The University of Amsterdam, TNO, KLM, and Ciena conduct research on **automated methods against attacks** on computer **network infrastructure**.

Multi-Domain Autonomous Response

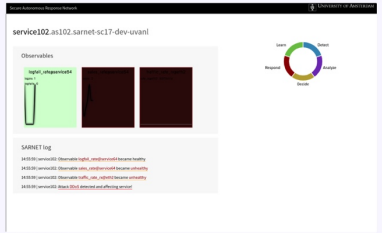
In this demonstration we let the viewers **initiate one of the pre-implemented attacks**. The touch interface shows a multi domain **network** and services. Each domain is **autonomous** and implements the SARNET **control loop** to that maintains is own **security** state. Additionally, domains can **collaborate** with each other by allowing certain **remote actions** that fellow collaborators can invoke.

By adjusting **levels of collaboration** we demonstrate the **effect on response capabilities** and **response** times.

Autonomy is achieved by **invoking** informational requests and defensive actions from the **victim**. This gives the **victim** the **autonomy** to make **decisions** over **its** destined **traffic** and it gives the **collaborators** the **autonomy** to decide on **how to handle** the requests.



Touch interface
The user can execute several attacks on the webservices who will try to defend the attack with the resources at their disposal. Increasing the collaboration level will increase the available resources and the defense capabilities.



Metrics screen
The graphs show the current state of a domain. When an observable becomes unhealthy the background of the graph becomes red. The log shows the defense actions that the domain applies, and whether they are successful.

Key takeaways:

- Domains can collaborate **and** maintain **autonomy**.
- Different **levels of collaboration** influence attack response times; more collaboration does not necessarily mean faster response times.
- **Collaborative defence strategies** are better in defending against heavy attacks.

Infrastructure

In this demo we use small scale but **realistic** attacks that are executed and contained inside **ExoGENI,** an international federated cloud testbed. A **Ciena 8700** switch is used at the UvA and Ciena sites to provide additional traffic isolation. We also implemented a SARNET on a **physical domain** that is part of the automation demo at **SURF booth #857**.

Ralph Koning <R.Koning@uva.nl>, Ben de Graaff <b.degraaff@uva.nl>, Paola Grosso <P.Grosso@uva.nl>, Cees de Laat <delaat@uva.nl>
http://sne.science.uva.nl | http://www.delaat.net/ | http://sarnet.uvalight.net

University of Amsterdam · SNE · NWO Netherlands Organisation for Scientific Research · COMMIT/ · TNO innovation for life · AIRFRANCE KLM · ciena

Creating Cyber Security Alliances Requires to:

- Define common benefits for the members,
- Organize and maintain Trust among the members, and
- Define a governance model to define common policies and standards for alliance's members.

Research objectives:

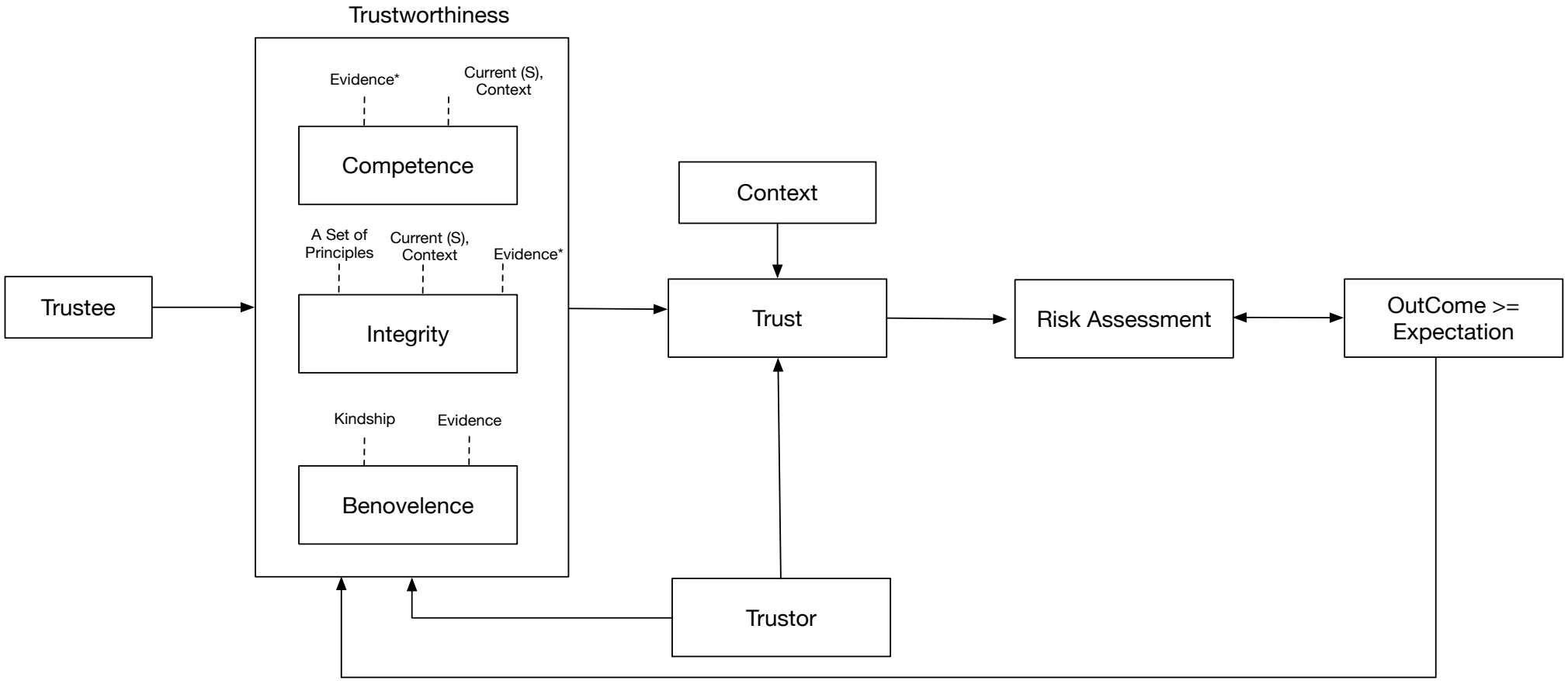
- Define Trust and its antecedents
- Present a Social Computational Trust Model (SCTM) and its Components.
- Present the Interaction Risk estimation through the SCTM Model.

Trust and its Antecedents

“x” expects “y” to do “t” and “y” will not exploit vulnerabilities of “x” when “y” is faced with the opportunity to do so. Therefore, ``y" has to exhibit:

- **Competence: Have the potential ability of a trustee to perform a given task**
- **Integrity: Adhere to the set of rules and act accordingly to fulfill the commitments, and**
- **Benevolence: Act and do good even if unexpected contingencies arise.**

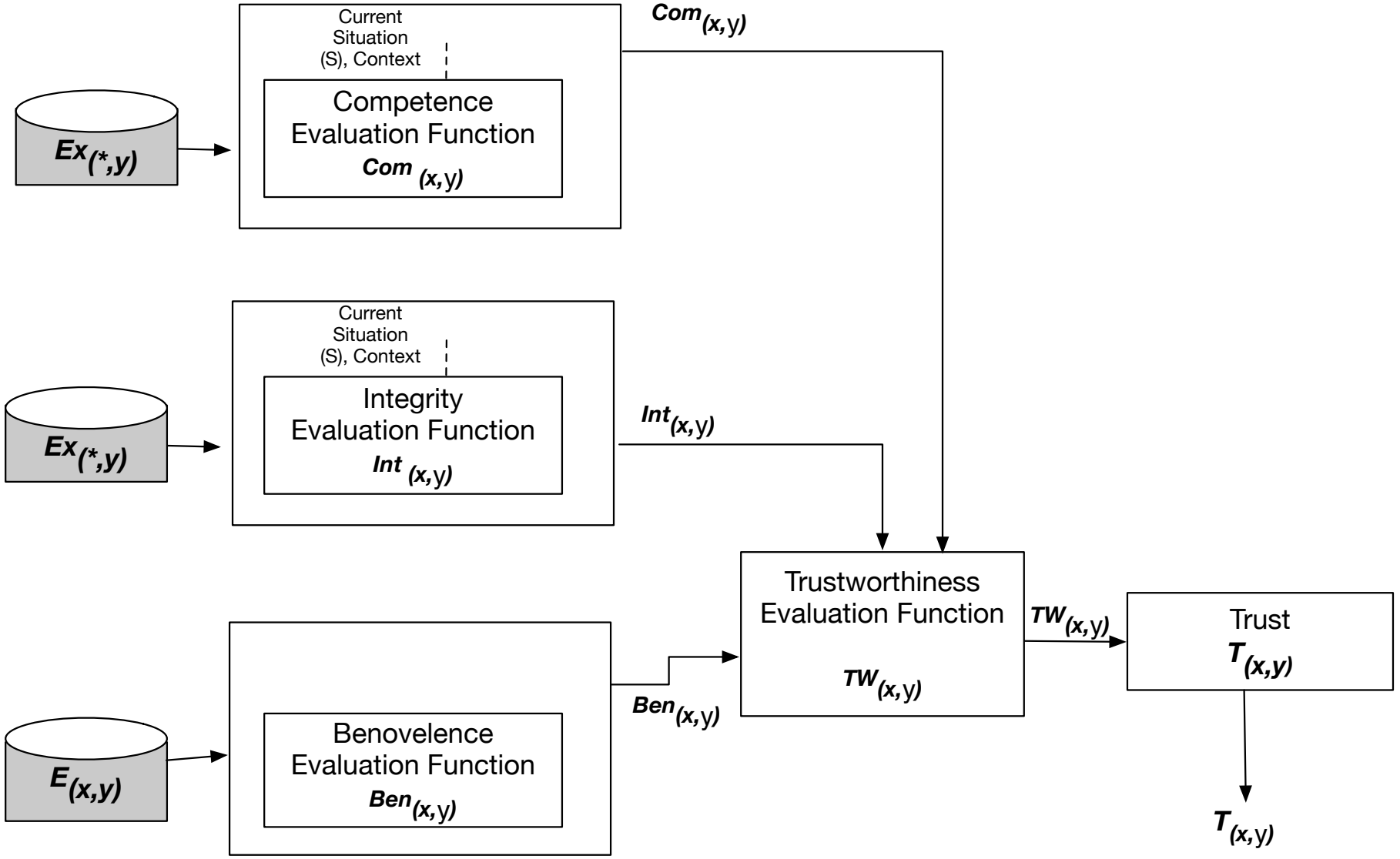
Trust Framework



Adopted from Mayer et al. (1995) ``An Integrative Model of Organizational Trust''

Social Computational Trust Model (SCTM)

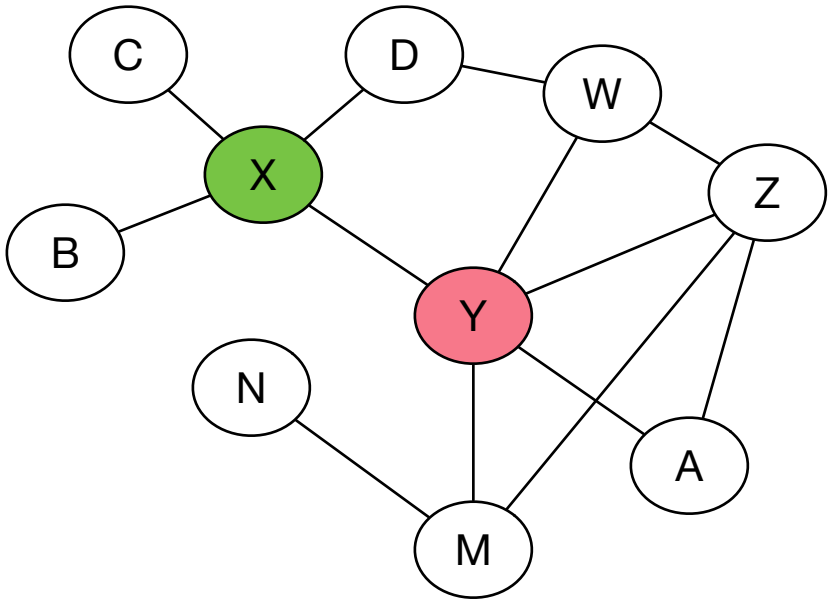
- Identify three distinctive trustworthiness factors (Benevolence Integrity and Competence)
- Evaluate Trust in a dynamic way
- Obtain the available evidence on the trustee
- Update Trust value



Benevolence Evaluation

- Based on the **Direct** interactions between X and Y (in the situation S).
- $Ben_x(y,S) \in [0,1]$

$$Ben_x(y,S) = \frac{1}{|N^1|}\sum(val(E_{(x,y)}))$$

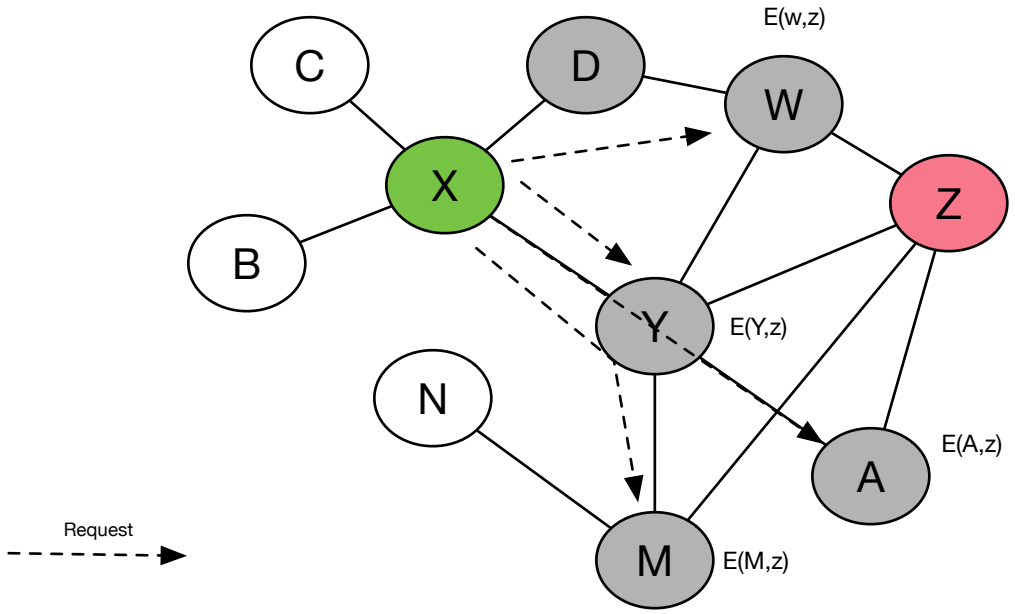


[1] Where N is the set of situations, in which “x” has interactions with “y”.

Competence Function

- Estimate based on the **all available** evidence on Trustee (e.g. y,z)
- $Com_x(y, S) \in [0,1]$

$$Com_x(y, S) = \frac{1}{|N|} \sum \text{val}\,(\text{E}_x(*,\text{y}))$$



Deljoo, Ameneh, et al. "The Impact of Competence and Benevolence in a Computational Model of Trust." IFIP International Conference on Trust Management. Springer, Cham, 2018.

Estimating Trust[1] based on Competence and Benevolence functions

$$T_x(y,S) = Com_x(y,S) + Ben_x(y,S)$$

[1] Integrity has been considered as a part of Benevolence function.

Risk Estimation

Interaction Risk (R_i) in the Alliance Consists of:

- Relational Risk (R_r): The **probability** and **consequence** of **not having** a successful cooperation.
- Performance Risk (R_p): The **probability** and **consequence** that alliance **objectives** are not **realized** despite **satisfactory cooperation** among the partners.

We can assume that Risk will be increased in the case of lack of Trust.

Propositions

Proposition1

Benevolent[1] behavior of partners **increases trust** and **reduces** former perceived **relational risk** in the alliance.

$$R_r(x,y) \propto \frac{1}{Ben_x(y,S)}$$

Proposition 2

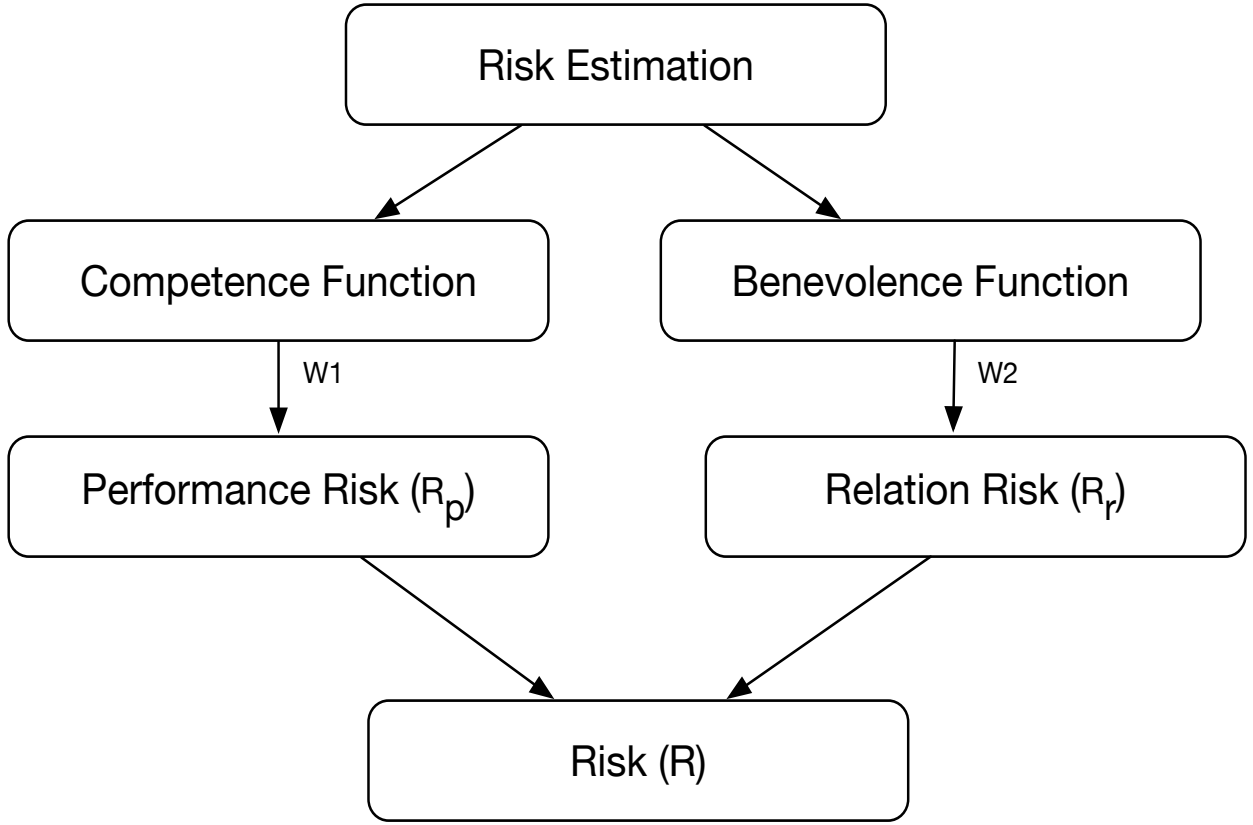
The **perceived performance risk** will be **reduced** if the competence of the given member is **high**.

$$R_p(x,y) \propto \frac{1}{Com_x(y,S)}$$

[1]Some of the scholars consider faith and good intentions instead of benevolence.

Perceived interaction risk

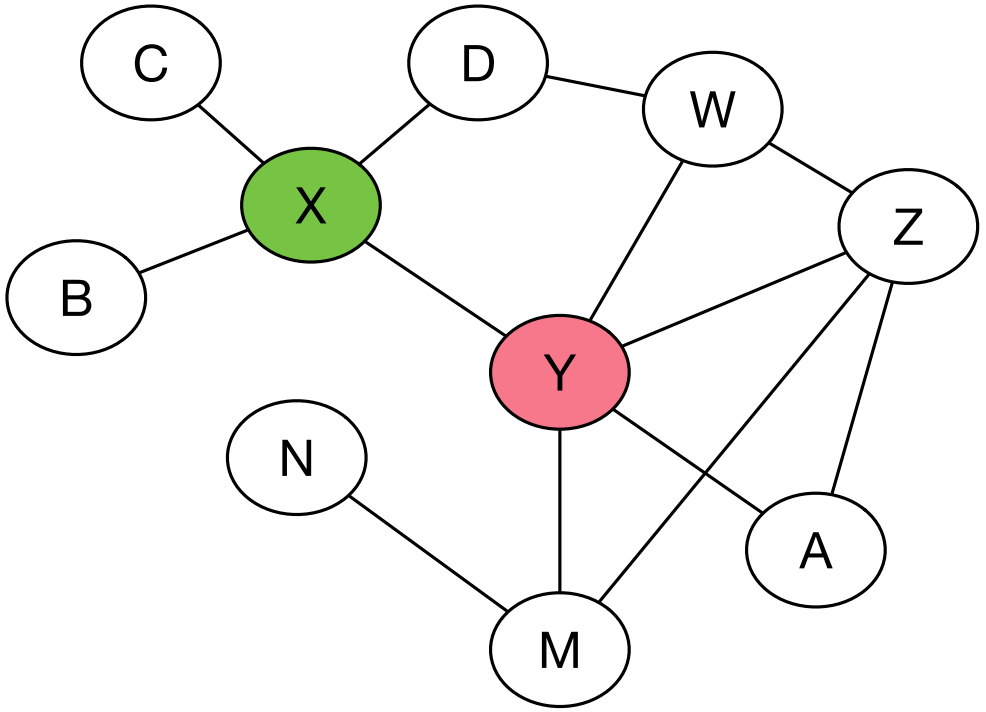
$$R_i(x,y) = \log_2\left(\frac{W_1^{*}}{1 + Ben_x(y,S)} + \frac{W_2}{1 + Com_x(y,S)}\right)$$



* *The value of* W_1 and W_2 have been considered equaly in this research.

$W_1, W_2 = 1$

Case Study



A Collaborative Network

Notation

Description	Representation	Value Range
Society of Agents	$x, y \in A$	
Situations	$S = \{s_1, s_2, s_3, s_4\}$	
Task	T	
Sub-tasks	$\alpha_1, \alpha_2, \alpha_3, \alpha_4$	
Context[1]	$d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8$	
Outcome	FD, FDD, V	1, 0.5, 0
Trust x on y in the situation S	$T_x(\mathrm{y}, \mathrm{S})$	[0,1]
All the available evidence on y	$\mathrm{E}_x(*,\mathrm{y})$	[0,1]
The direct evidence on y	E(x,y)	[0,1]

[1] d_1 = trustor, d_2 = trustee, d_3=time, d_4= location, d_5= task, d_6= complexity, d_7= deadline, d_7= outcome
[2] FD = Fulfill duty, FDD= Fulfill duty with delay, V=violation

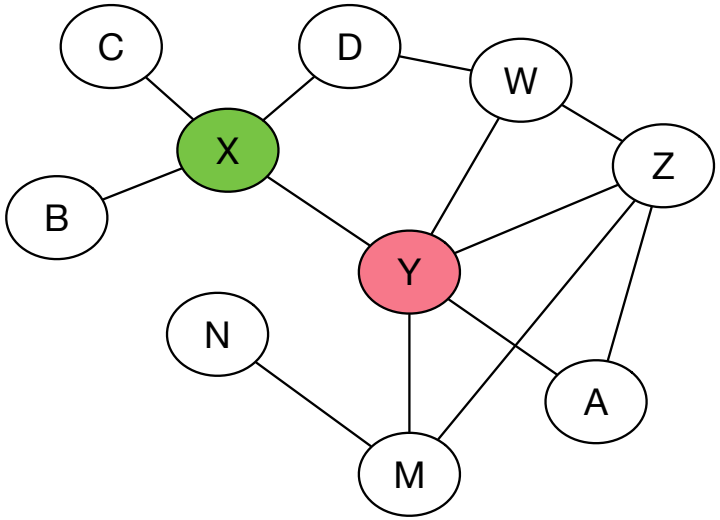
Algorithm 1 Calculate the Outcome Based on the Task's Deadline.

Require: $Time_w$: time window.
Require: Req_t: request time.
Require: Rep_t: report time.

$d_7 = Rep_t - Req_t$
if $d_7 <= Time_w$ **then**
  $d_8 = Fd$
else if $d_7 > Time_w$ **then**
  $d_8 = Fdd$
else if $d_7 = 0$ **then**
  $d_8 = V$
end if
return d_8

Scenario

Domain “N” wants to choose ideal domains for collaboration in order to **mitigate and defend against a certain attack.**

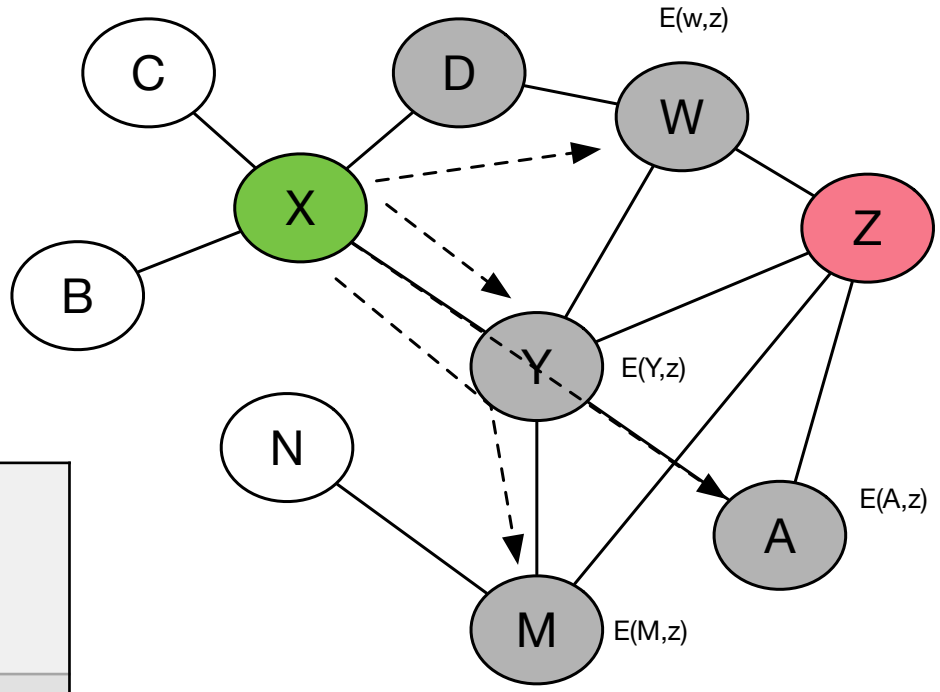


Task: Mitigate and defend against a certain attack.

Sub-tasks:

- α_1: provide resources within a certain time window,
- α_2: monitor a certain traffic,
- α_3: block a certain link,
- α_4: implement a certain counter measurement.

Gathering Evidence



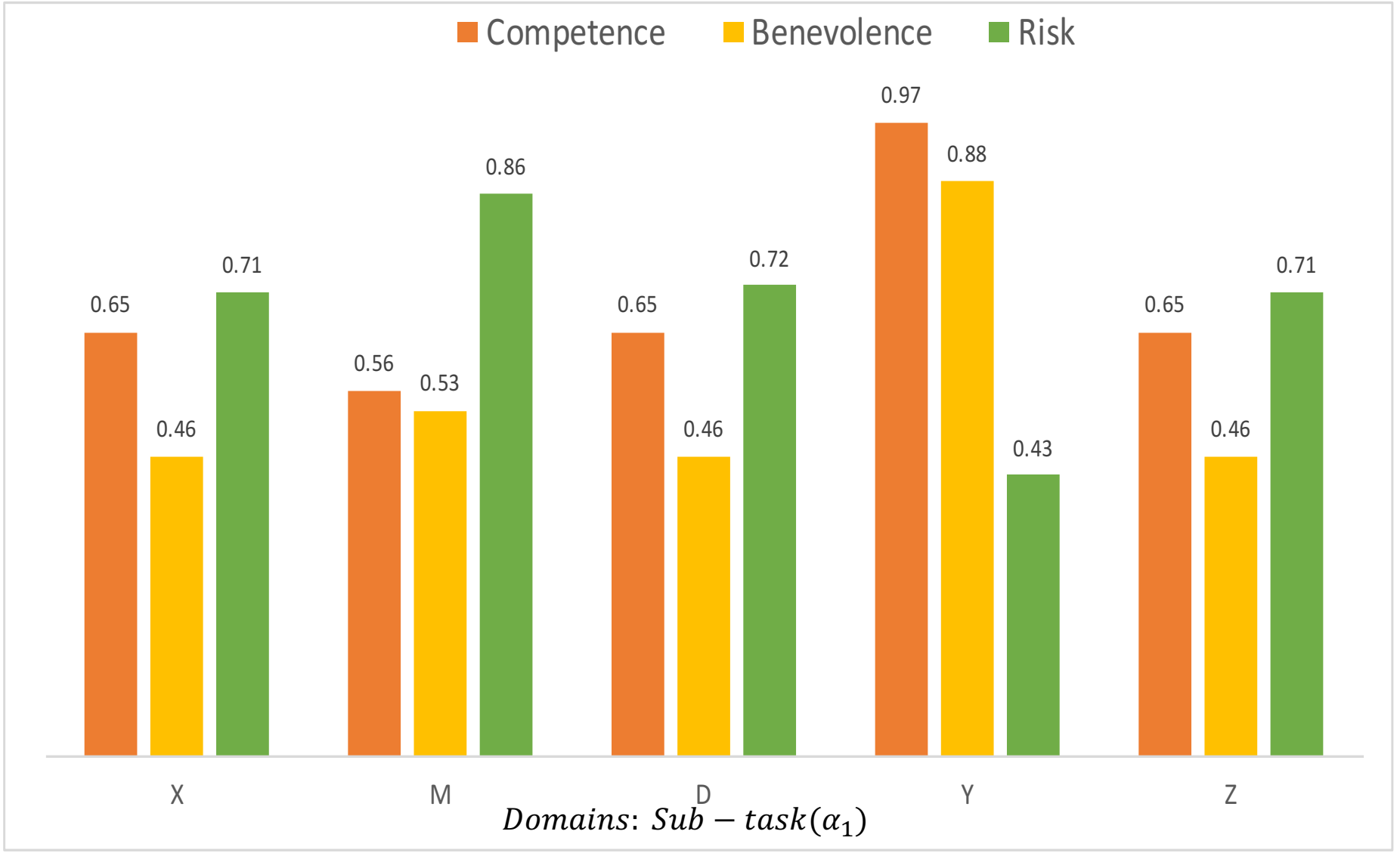
Sub-tasks / Agents	α_1	α_2	α_3	α_4
Y	FDD	FD	FD	FDD
M	FDD	FD	FD	FDD
W	FDD	FD	FD	FDD
A	FDD	FD	FD	FDD

Agent “X” asks different Agents’ (direct neighbors of ”Z”) opinion about agent ‘’Z” on the different (Sub-)tasks.

Result

❖α_1: provide resources within a certain time window.

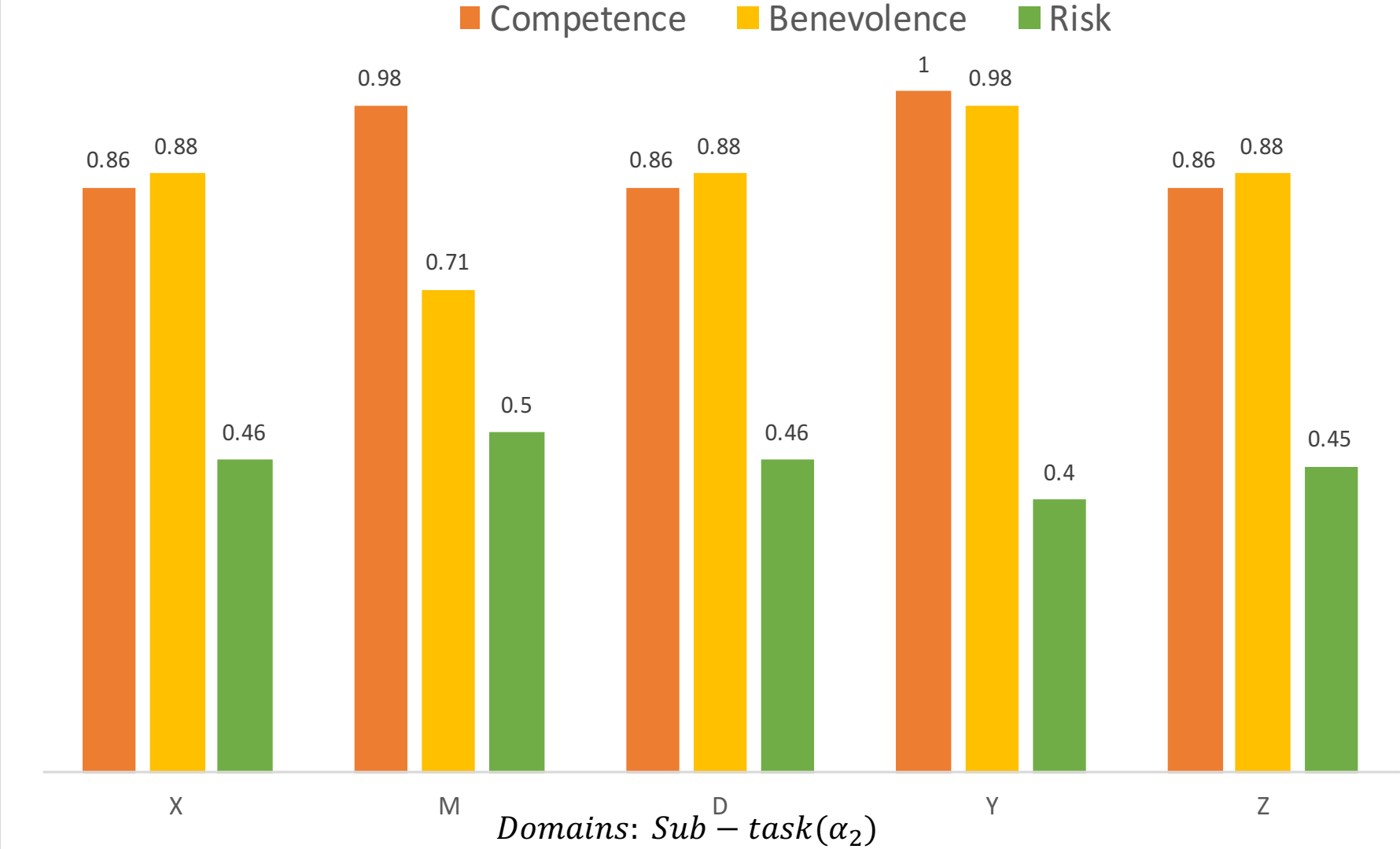
❖Domain “N” selects Domain “Y” to collaborate with.



Result Cont.

❖α_2: monitor certain traffic.

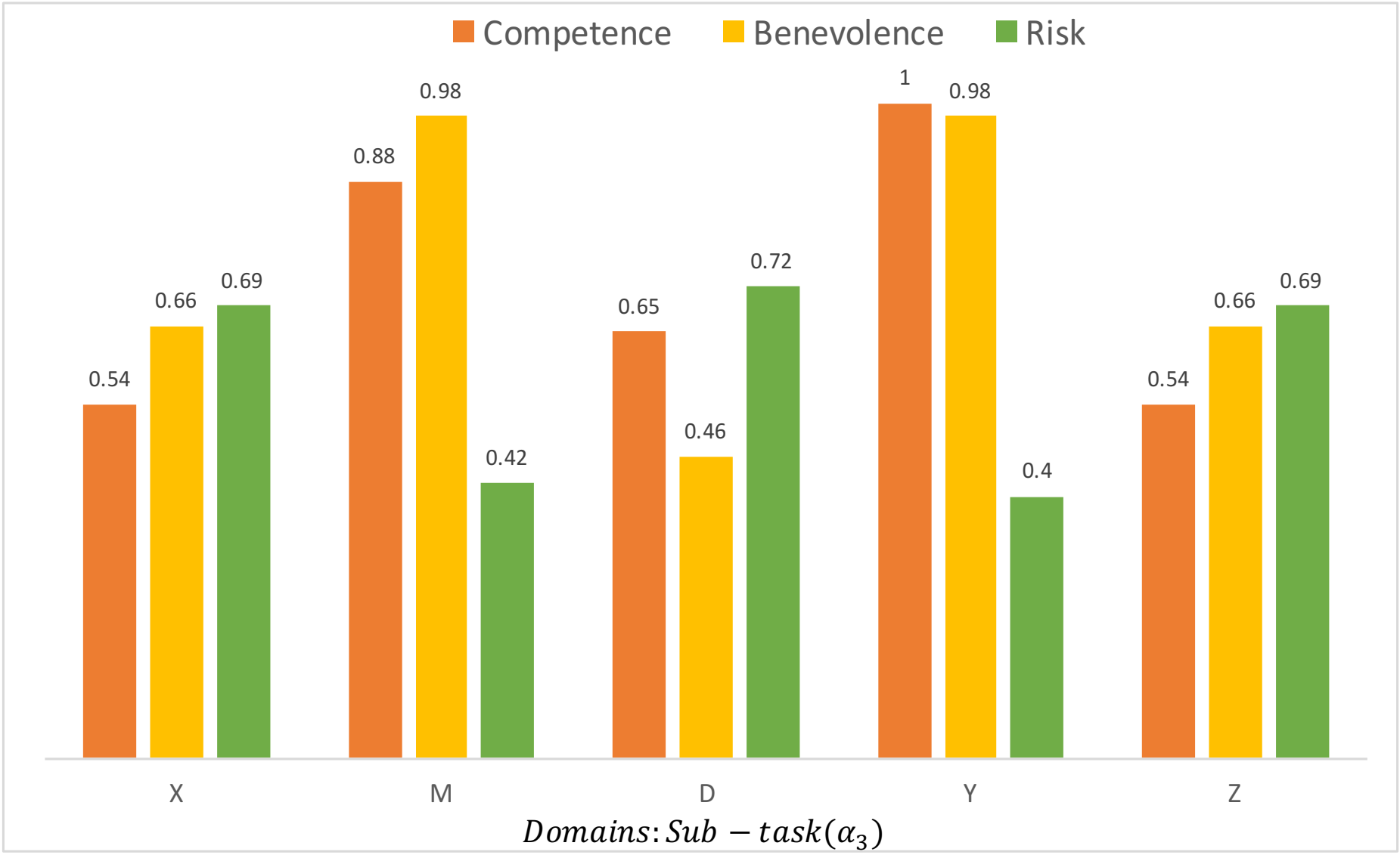
❖Domain “N” selects Domain “Y”, “X” and “Z” to collaborate with.



Result Cont.

❖α_3: block a certain link.

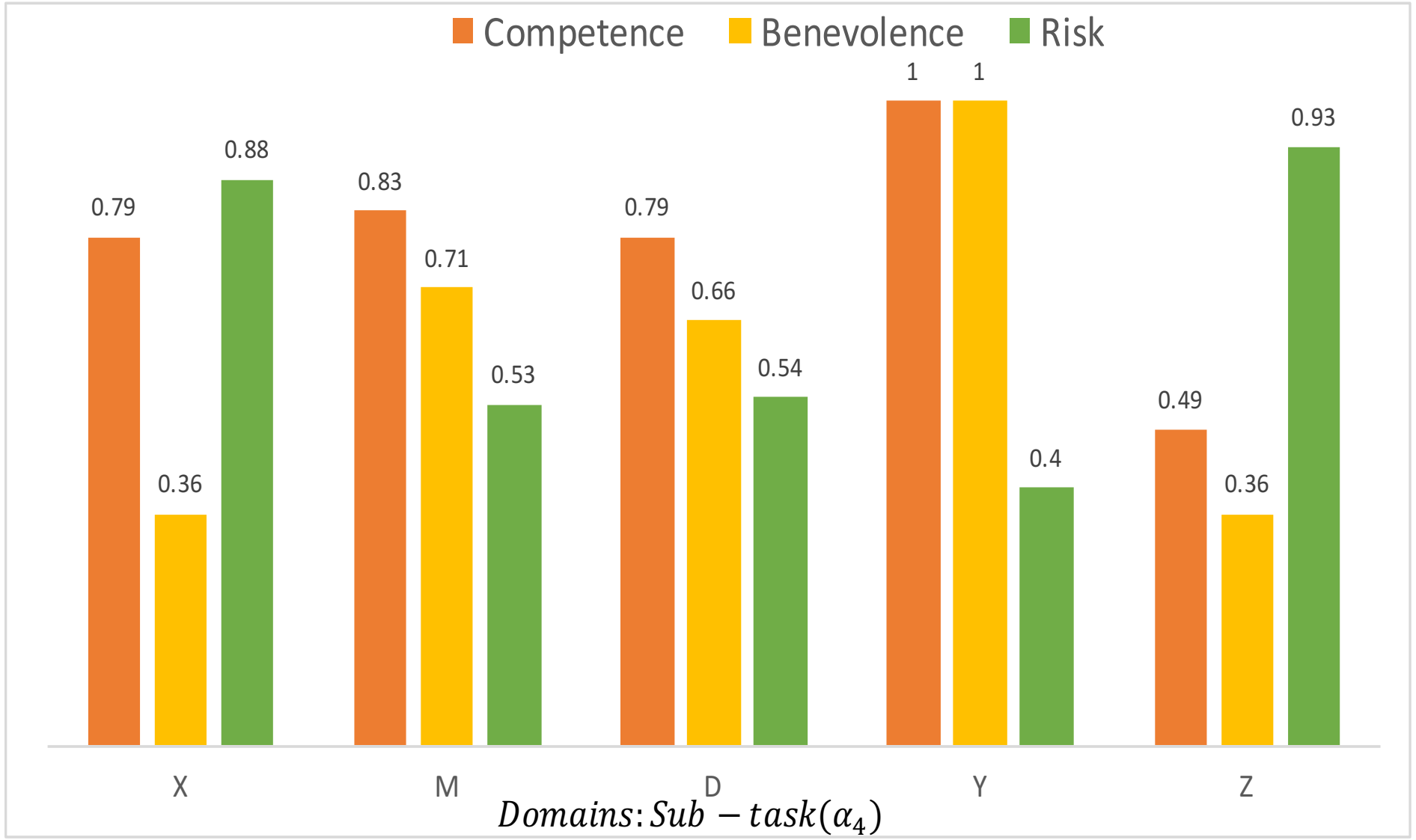
❖Domain “N” selects Domain “Y” and “M” to collaborate with.



Result Cont.

❖α_4: implement a certain counter measurement.

❖Domain “N” selects Domain “Y” to collaborate with.



Conclusion

SCTM allows us to:

- ❖ Identify and isolate untrustworthy members
- ❖ Evaluate an interaction's utility
- ❖ Estimate the interaction risk
- ❖ Estimate trust based on the direct and observed evidence
- ❖ Decide whether and with whom to interact

Q&A

- More information:
  - http://delaat.net/sarnet
  - http://delaat.net/dl4ld
- Contact:
  - a.deljoo@uva.nl