SARNET Alliance

Ameneh Deljoo

Cees de Laat, Tom van Engers and Leon Gommans

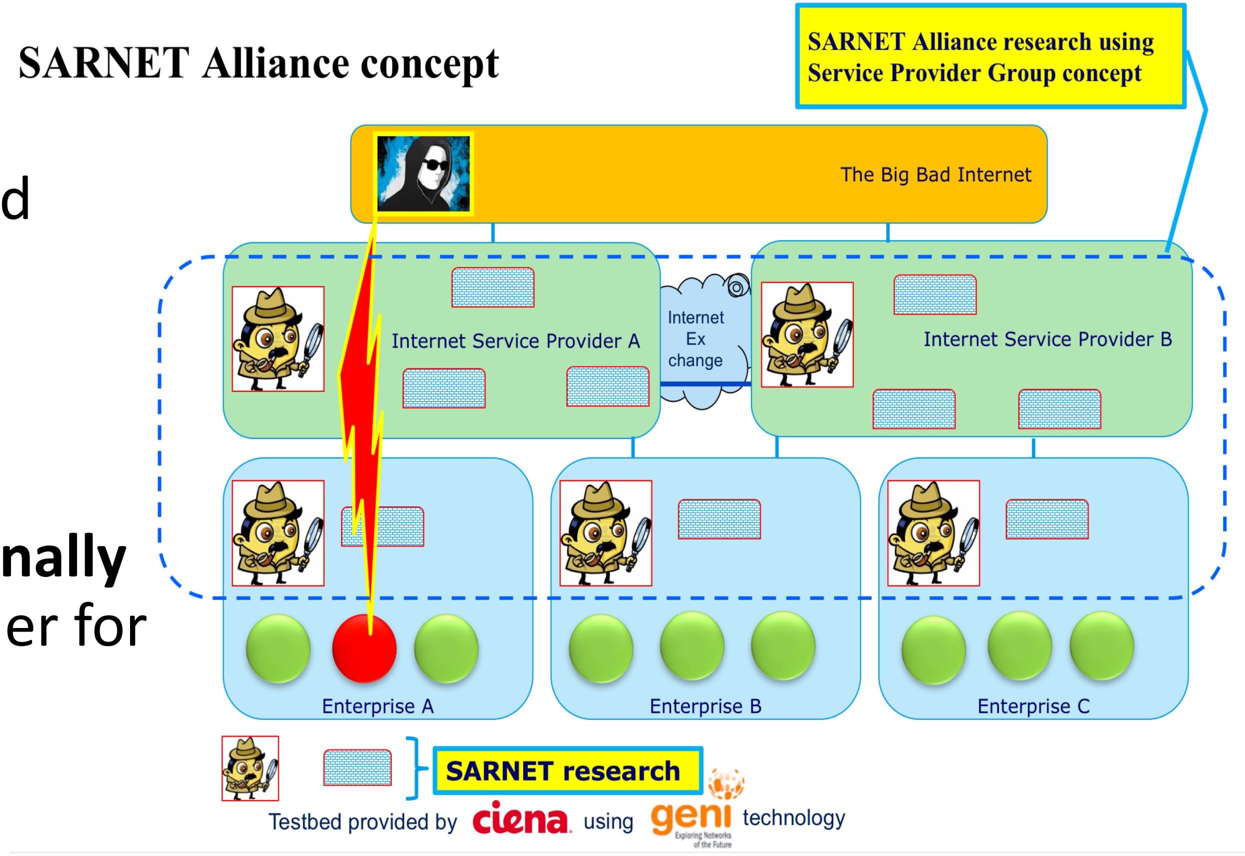
Systems and Networking Lab
University of Amsterdam
a.deljoo@uva.nl

Motivation

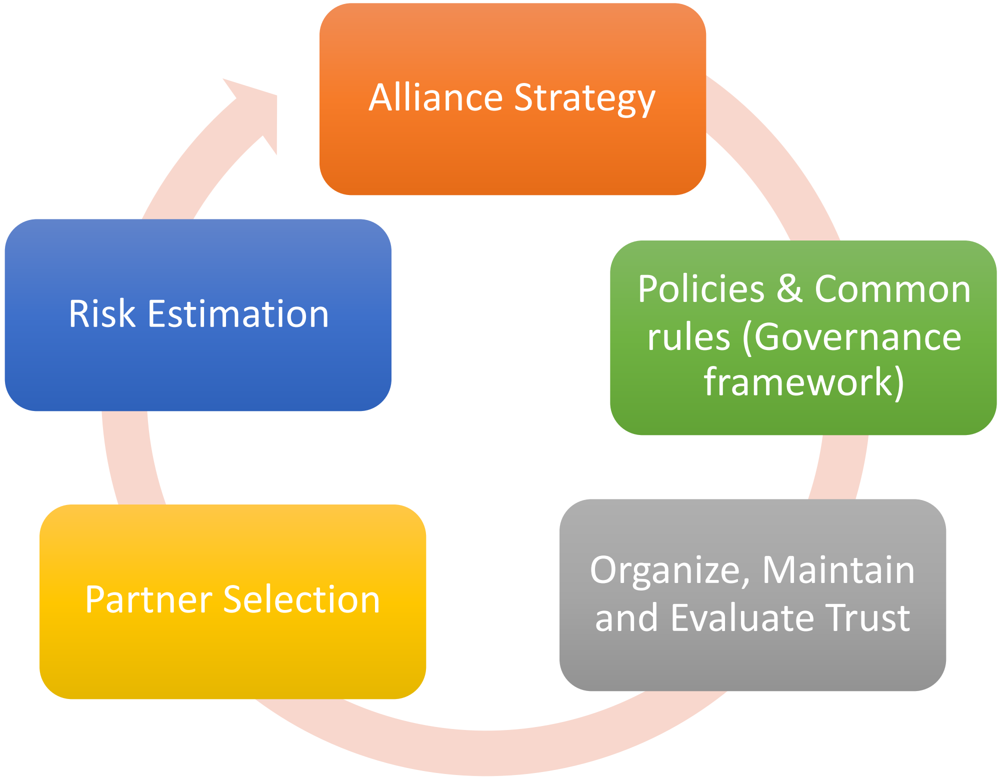
- Defence against **organized attacks** requires collaboration amongst service providers
- Protection of the network can often only be **guaranteed** and **financed** as a **shared effort**
- Network of organizations **evolve** over time and become more complex
- Find a “**right**” partner is a challenging task.

We need to:

- Define a more **sophisticated** and **computationally executable** method to select the “**right**" partner for **sharing data** and **intelligence**.


SARNET Alliance concept
SARNET Alliance research using Service Provider Group concept
The Big Bad Internet
Internet Service Provider A
Internet Ex change
Internet Service Provider B
Enterprise A
Enterprise B
Enterprise C
SARNET research
Testbed provided by ciena. using geni technology
Exploring Networks of the Future

Requirements To Create An Alliance



Alliance Strategy

Policies & Common rules (Governance framework)

Organize, Maintain and Evaluate Trust

Partner Selection

Risk Estimation

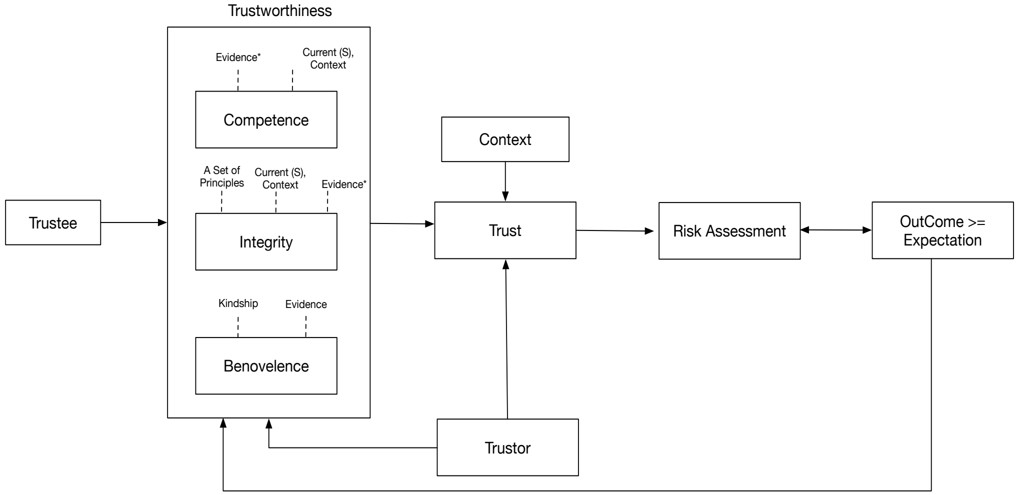
Contributions

- **Evaluate, measure and maintain trust among the alliance members.**
- **Present and implement the computational trust model (SCTM).**
- **Risk estimation** through the SCTM model. The SCTM facilitates risk-based partner selection to select the **“right"** partner to collaborate in joint tasks.
- A **governance model** to define a set of policies and rules.

Trust and its Antecedents

Organize, Maintain and Evaluate Trust

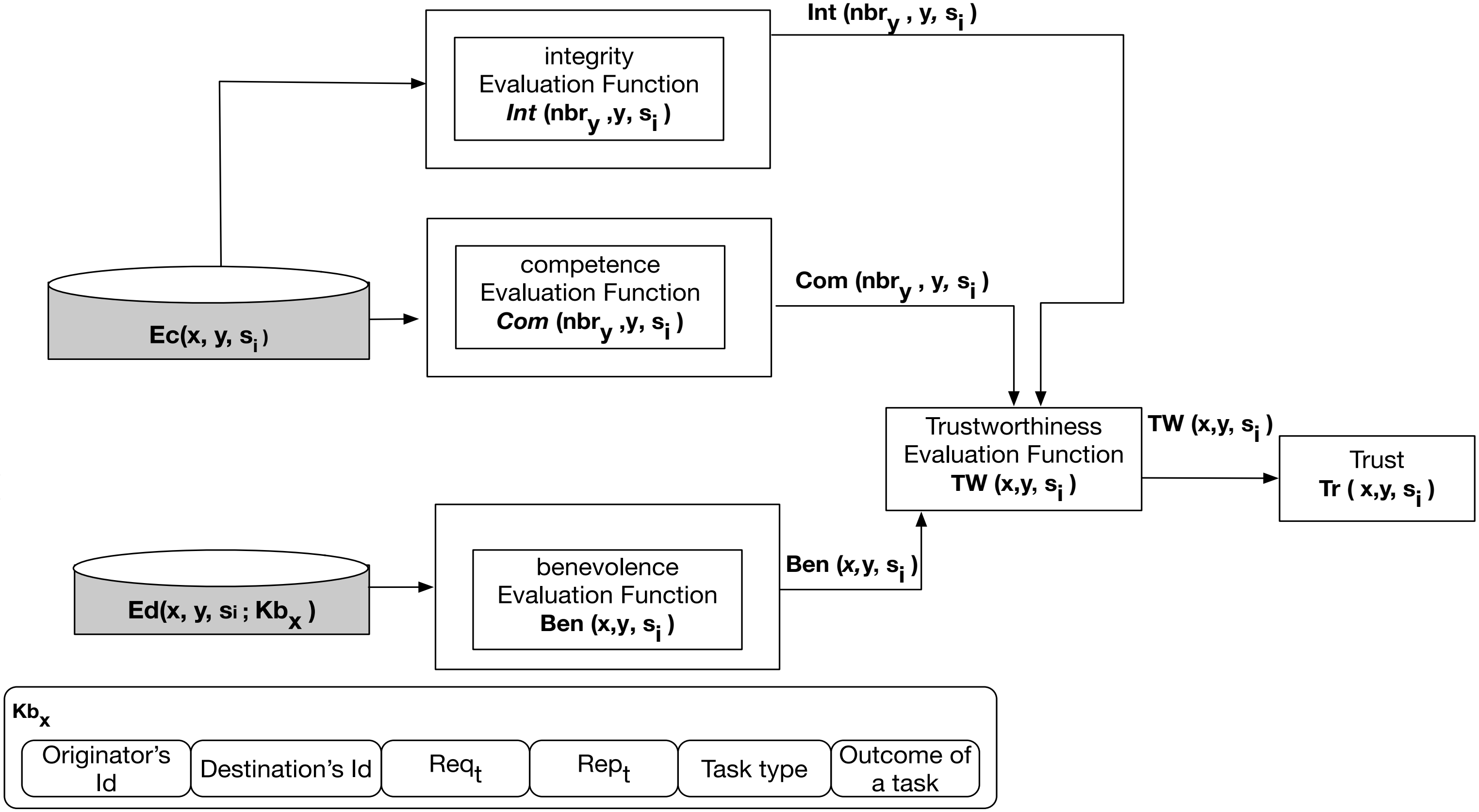
- “x” expects “y” to do task (τ) and “y” will not exploit vulnerabilities of “x” when “y” faced with the opportunity to do so. Therefore, “y”:
  - Has the **potential ability** to perform a given task (competence),
  - **Adheres** to a set of **rules** agreed upon and acts accordingly to **fulfill the commitments** (integrity), and
  - **Acts** and does **good** even if unexpected contingencies arise (benevolence).



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

Computational Trust Model (SCTM)

- Identify three distinctive trustworthiness factors (**Benevolence, Integrity and Competence**)
- Evaluate Trust in a dynamic way
- Gather the direct and indirect evidence on a trustee
- Update Trust value



integrity Evaluation Function *Int* (nbr$_y$,y, s$_i$)
Int (nbr$_y$, y, s$_i$)
competence Evaluation Function *Com* (nbr$_y$,y, s$_i$)
Com (nbr$_y$, y, s$_i$)
Ec(x, y, s$_i$)
Trustworthiness Evaluation Function TW (x,y, s$_i$)
TW (x,y, s$_i$)
Trust Tr (x,y, s$_i$)
Ed(x, y, si ; Kb$_x$)
benevolence Evaluation Function Ben (x,y, s$_i$)
Ben (*x*,y, s$_i$)
Kb$_x$
Originator's Id
Destination's Id
Req$_t$
Rep$_t$
Task type
Outcome of a task

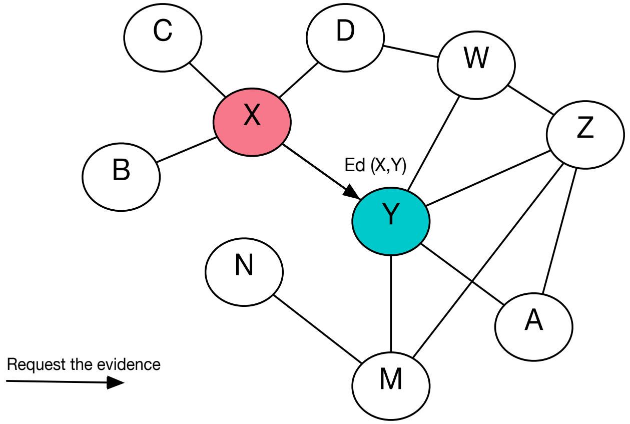
Context Definition

In order to define the situations that lead to an agreement between a trustor and a trustee:

- d_1 = trustor,
- d_2= trustee,
- d_3 = time,
- d_4= location,
- d_5= task,
- d_6= complexity,
- d_7= deadline,
- d_8= Outcome
- Three different outcome of tasks

$$\text{val}\,(d_8) = \begin{cases} 1\,, & if\ d_8 = Fd \\ 0.5\,, & if\ d_8 = Fdd \\ 0\,, & if\ d_8 = V \end{cases}$$

Evidence Gathering: Direct evidence



- A trustor looks at its Kb to collect the evidence on a trustee based on past interactions.

$$val_d(.) \longrightarrow [0,1]$$

$$Ed(x, y, s_i; kb_x) = \{d_8(\text{x, y}, s_i) \in kb_x\}$$

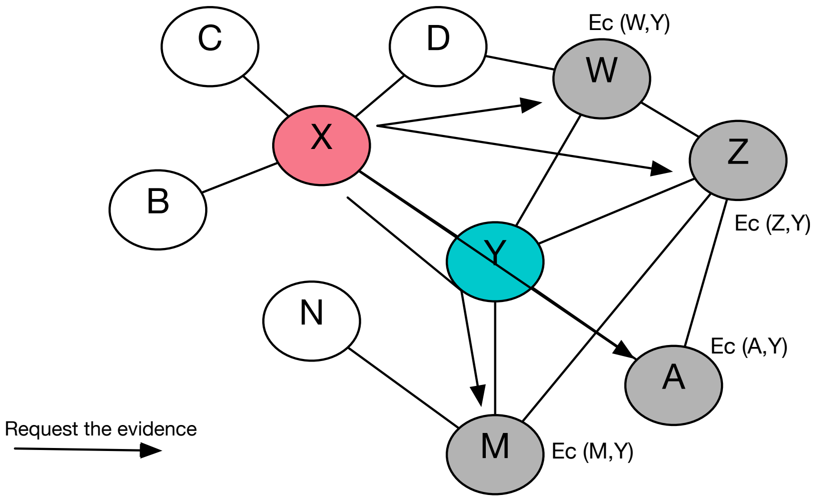
$$val_d(Ed(x, y, s_i; kb_x)) = \frac{1}{N_x} \sum_{d_8(x,y,s_i) \in Ed(x,y,s_i;\, kb_x)} val(d_8(\text{x, y}, s_i))$$

$$\text{val } (d_8) = \begin{cases} 1\,, & if\ d_8 = Fd \\ 0.5\,, & if\ d_8 = Fdd \\ 0\,, & if\ d_8 = V \end{cases} \qquad , N_x = number\ of\ enrties\ in\ the\ Kb's$$

Kb$_x$

Originator's Id	Destination's Id	Req$_t$	Rep$_t$	Task type	Outcome of a task

Evidence Gathering: Indirect evidence



- A trustor asks a trustee’s direct neighbors to send him their evidence on a given trustee.

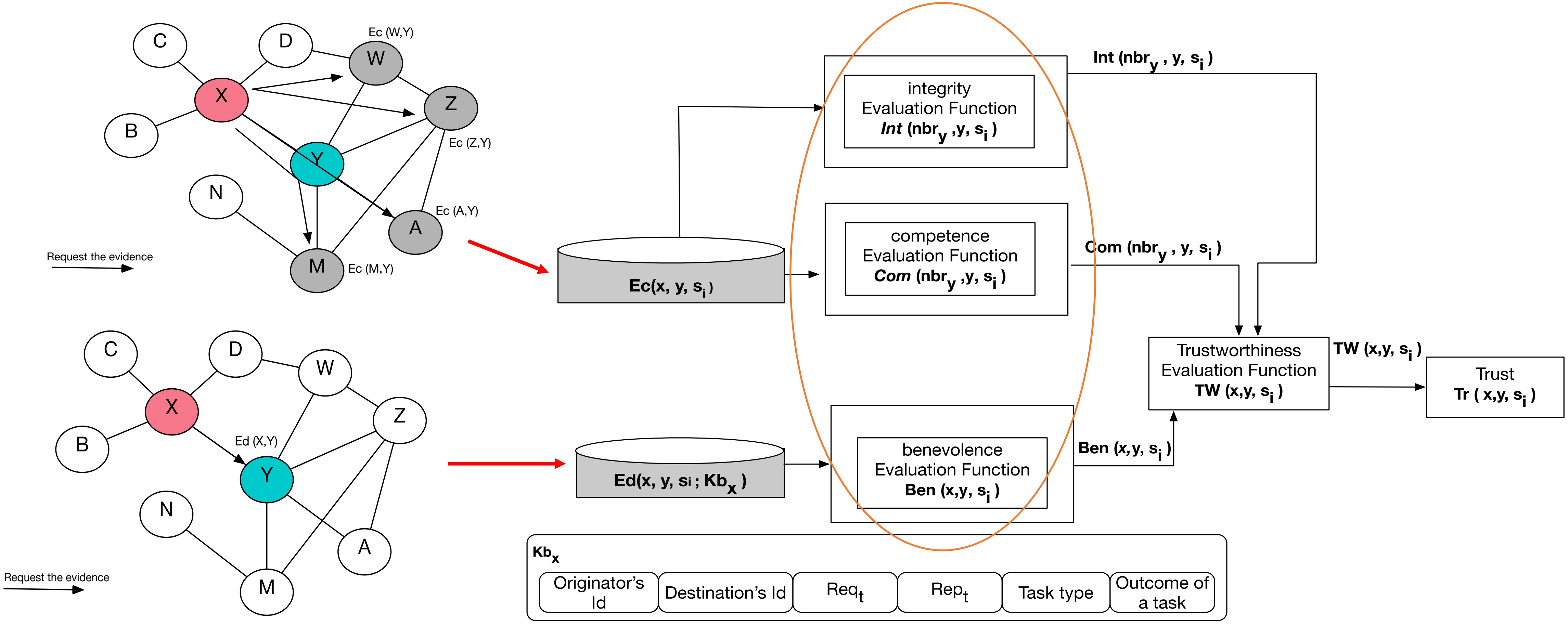
$$val_c(.) \longrightarrow [0,1]$$

$$Ec\,(nbr_y, y, s_i) = \{\, Ed(u, y, s_i; kb_u) \mid u \in nbr_y \}$$

$$val_c(Ec(x, y, s_i)) = \frac{1}{N_{nbr}} \sum_{Ed(u,y,s_i;\, kb_x) \in Ec(nbr_y, y,\, s_i)} val_d(Ed(u, y, s_i; kb_u))$$

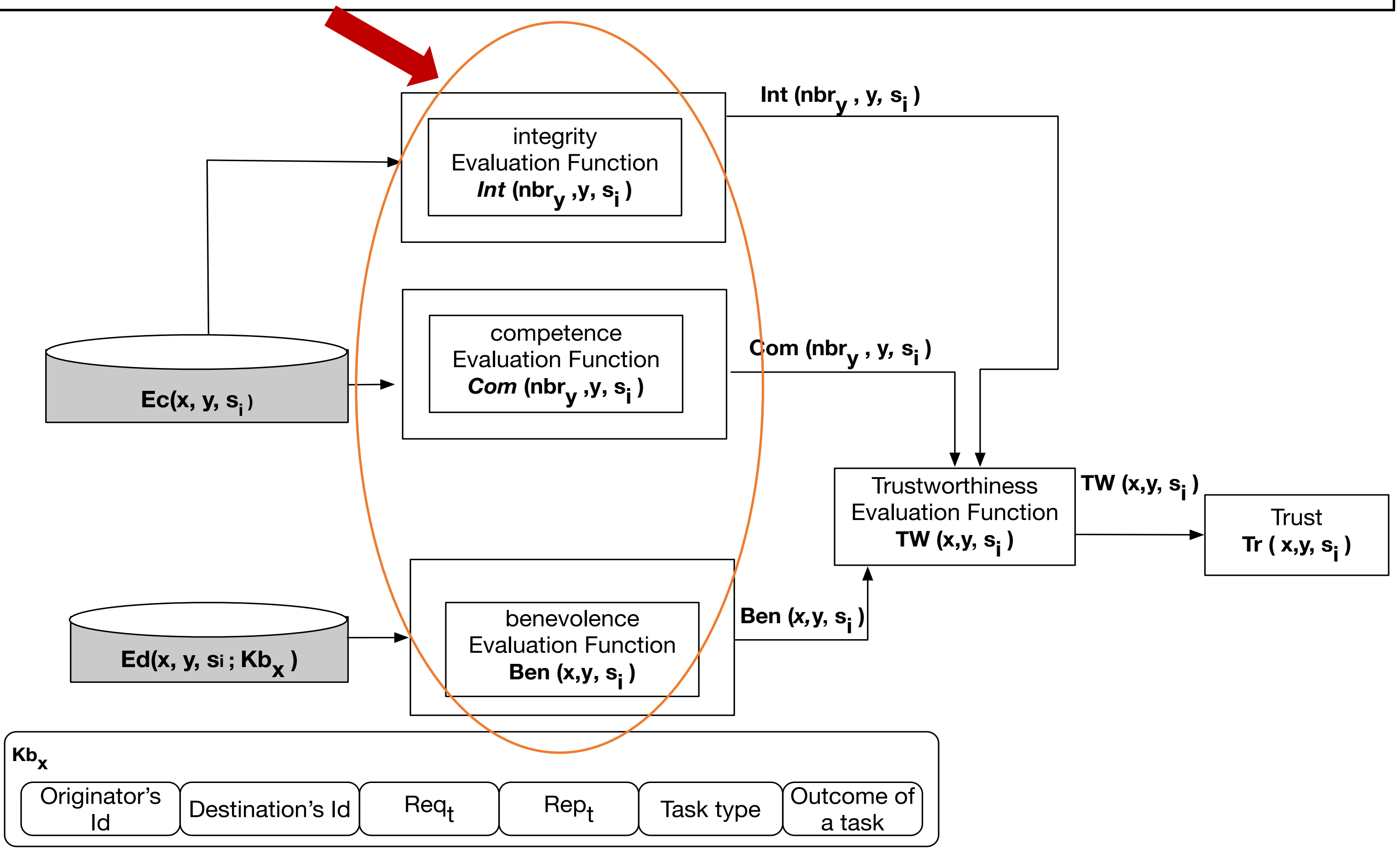
$N_{nbr} = number\ of\ neighbors\ that\ contribute\ to\ the\ val_c$

SCTM



Originator's Id	Destination's Id	Req_t	Rep_t	Task type	Outcome of a task

SCTM



integrity Evaluation Function *Int* (nbr$_y$,y, s$_i$)

competence Evaluation Function *Com* (nbr$_y$,y, s$_i$)

benevolence Evaluation Function Ben (x,y, s$_i$)

Ec(x, y, s$_i$)

Ed(x, y, si ; Kb$_x$)

Int (nbr$_y$, y, s$_i$)

Com (nbr$_y$, y, s$_i$)

Ben (*x*,y, s$_i$)

Trustworthiness Evaluation Function TW (x,y, s$_i$)

TW (x,y, s$_i$)

Trust Tr (x,y, s$_i$)

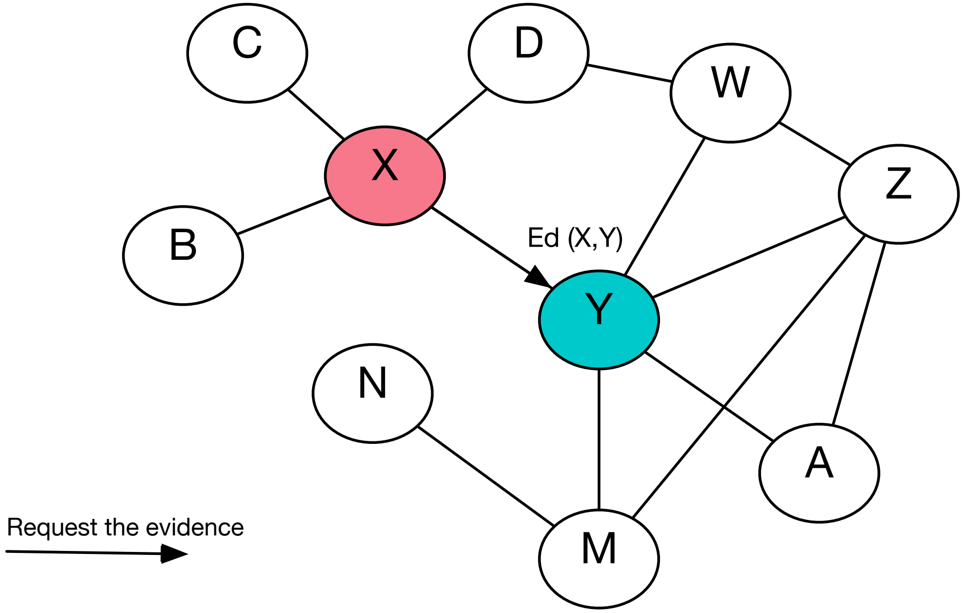
Kb$_x$

Originator's Id	Destination's Id	Req$_t$	Rep$_t$	Task type	Outcome of a task

Benevolence Function

- Based on the **direct** interactions between $trustor\ x\ and\ trustee\ y$ in the situation s_i.

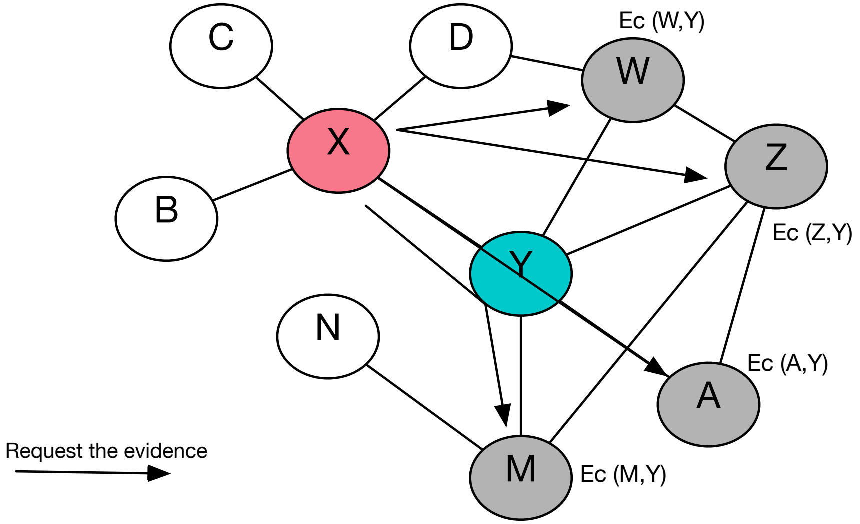
$$Ben(x, y, s_i) = val_d(Ed(x, y, s_i, kb_x))$$



Competence Function

- Evaluate based on the **all available** evidence on Trustee (e.g. y,z)

$$Com(nbr_y, y, s_i) = val_c(Ec(nbr'_y, y, s_i)), nbr'_y = nbr_y \backslash \{x\}$$



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.

Integrity Function

- The given trustee's integrity is computed by:

$$Int\left(nbr_y, y, s_i\right) = \frac{\sum_{Kb_{u\in}nbr_y} N_{Fd}\,(Kb_u, y)}{N_{Ec}}$$

where

$$N_{Fd}(Kb_u, y) = |\left(Ed(u, y, s_i, kb_u)\right)|u \in nbr_y \,\&\, val(d_8(u, y, s_i)) = \ Fd\ |$$

Estimating Trust based on Competence and Benevolence functions

$$Tw(x,y,s_i) = \frac{1}{3}(Com(nbr_y,y,s_i) + Int(nbr_y,y,s_i) + Ben(x,y,s_i))$$

$$\Downarrow$$

$$Tr(x,y,s_i) = Tw(x,y,s_i)$$

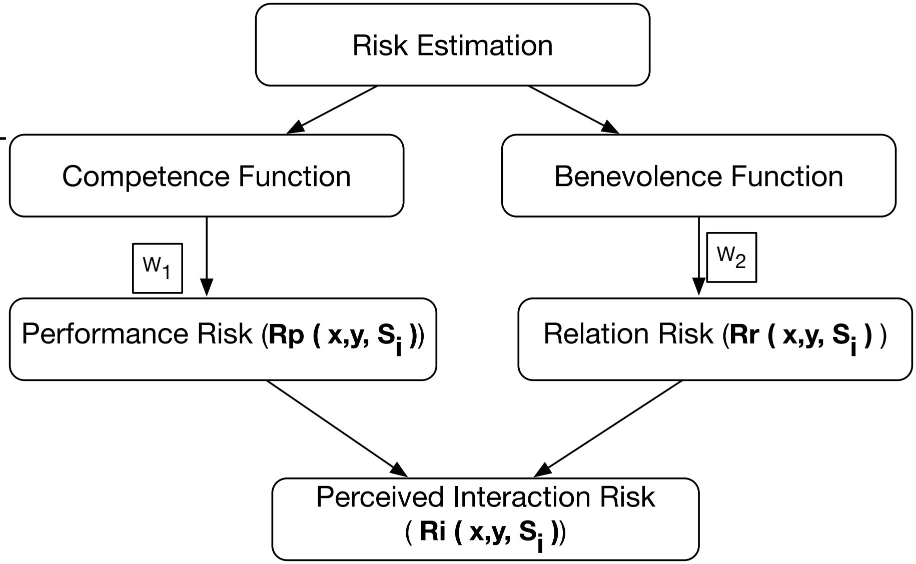
Risk Estimation

Risk Estimation

Interaction Risk $(R_i(x, y, s_i))$ in the Alliance Consists of:

- Relational Risk $\left(R_r(x, y, s_i)\right)$: The **probability** and **consequence** of **not having** a successful cooperation (Benevolent behavior) .
- Performance Risk $(R_p(x, y, s_i))$: The **probability** and **consequences** that alliance **objectives** are not **realized** despite **satisfactory cooperation** among the partner (the competence of the given member).

Interaction risk


Risk Estimation
Competence Function
Benevolence Function
W1
W2
Performance Risk (Rp (x,y, Si))
Relation Risk (Rr (x,y, Si))
Perceived Interaction Risk
(Ri (x,y, Si))

Interaction Risk is given by:

$$R_i(x, y, s_i) = \; R_r(x, y, s_i) + R_p(x, y, s_i)$$

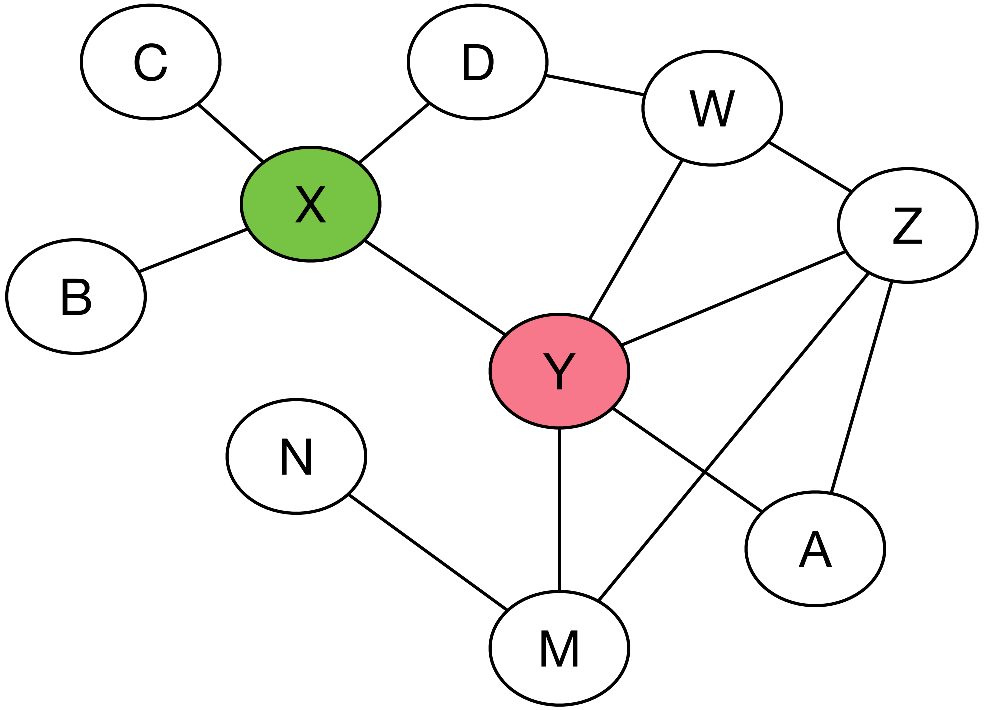
$$R_i(x, y, s_i) = w_1(1 - Com(x, y; s_i)) + \; w_2\big(\; 1 - Ben(x, y; s_i)\big)$$

$$R_i(x, y, s_i) = \; \alpha\left(1 - Com\big(nbr_y, y, s_i\big)\right) \; + \; (1 - \alpha)\big(\; 1 - Ben(x, y, s_i)\big), \qquad 0 \leq \alpha \leq 1$$

$w_1 = \alpha$, $w_2 = 1 - \alpha$

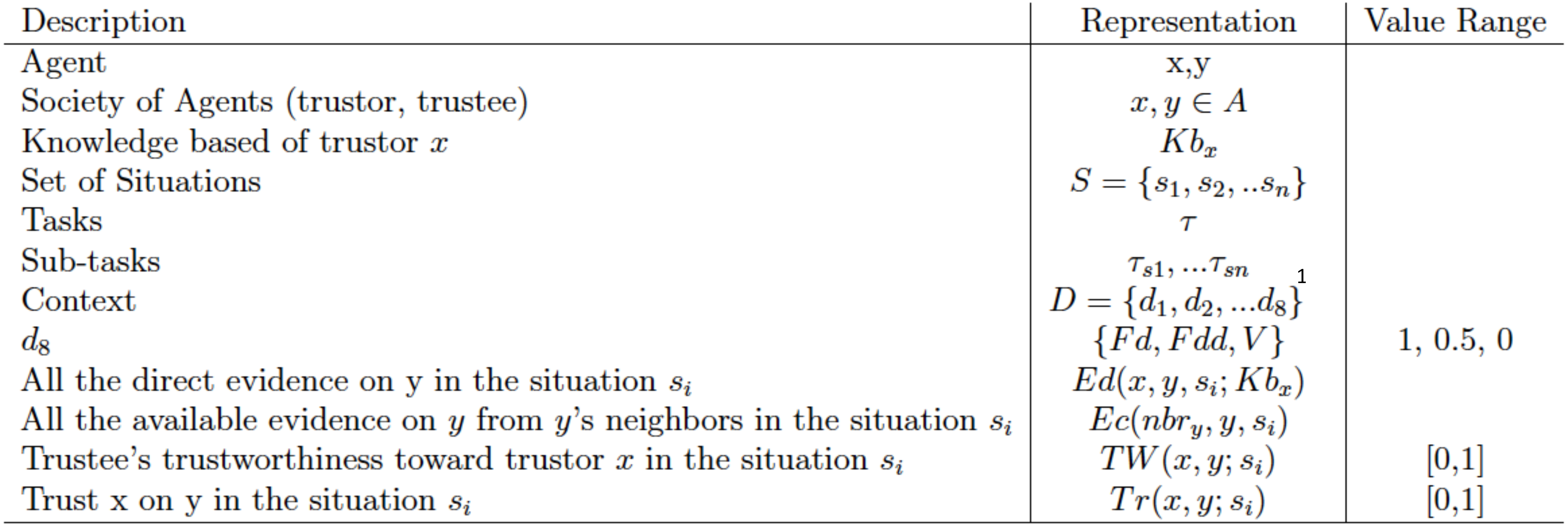
T. Das, B.-S. Teng, Risk types and inter-frim alliance structures, Journal of management studies 33 (6) (1996) 827{843.

Case Study



A Collaborative Network

Notation



Description	Representation	Value Range
Agent	x,y	
Society of Agents (trustor, trustee)	$x, y \in A$	
Knowledge based of trustor x	Kb_x	
Set of Situations	$S = \{s_1, s_2, ..s_n\}$	
Tasks	τ	
Sub-tasks	$\tau_{s1}, ...\tau_{sn}$	
Context	$D = \{d_1, d_2, ...d_8\}$[1]	
d_8	$\{Fd, Fdd, V\}$	1, 0.5, 0
All the direct evidence on y in the situation s_i	$Ed(x, y, s_i; Kb_x)$	
All the available evidence on y from y's neighbors in the situation s_i	$Ec(nbr_y, y, s_i)$	
Trustee's trustworthiness toward trustor x in the situation s_i	$TW(x, y; s_i)$	[0,1]
Trust x on y in the situation s_i	$Tr(x, y; s_i)$	[0,1]

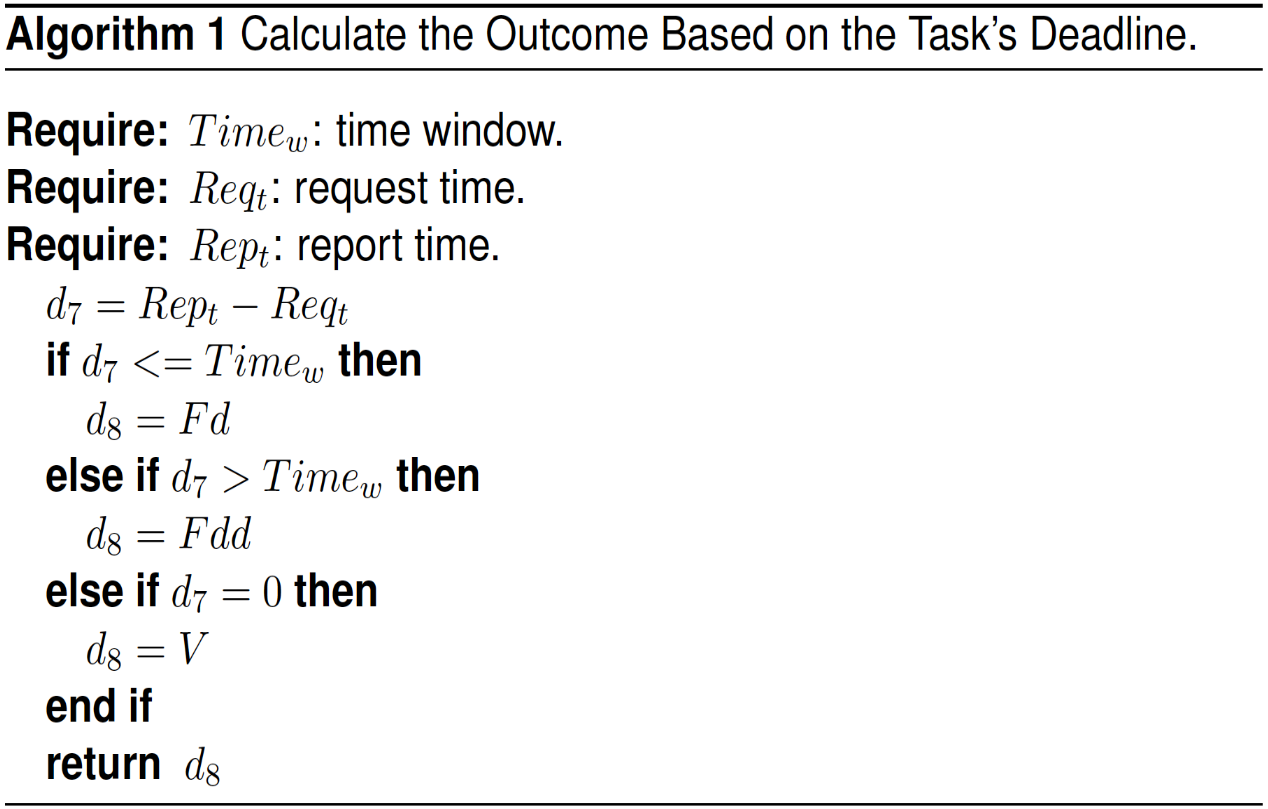
[1] Dimensions are: d1 = trustor, d2= trustee , d3 = time, d4= location, d5= task, d6=complexity, d7= deadline, d8= Outcome

Calculate the Outcome

- ❖ d_8= Outcome
- ❖ Three different outcome of tasks

$$Fd(Fullfil\ duty)$$
$$Fdd(Fullfil\ duty\ with\ delay)$$
$$V(Violate)$$

$$\text{val}\ (d_8) = \begin{cases} 1\ , & if\ d_8 = Fd \\ 0.5\ , & if\ d_8 = Fdd \\ 0\ , & if\ d_8 = V \end{cases}$$



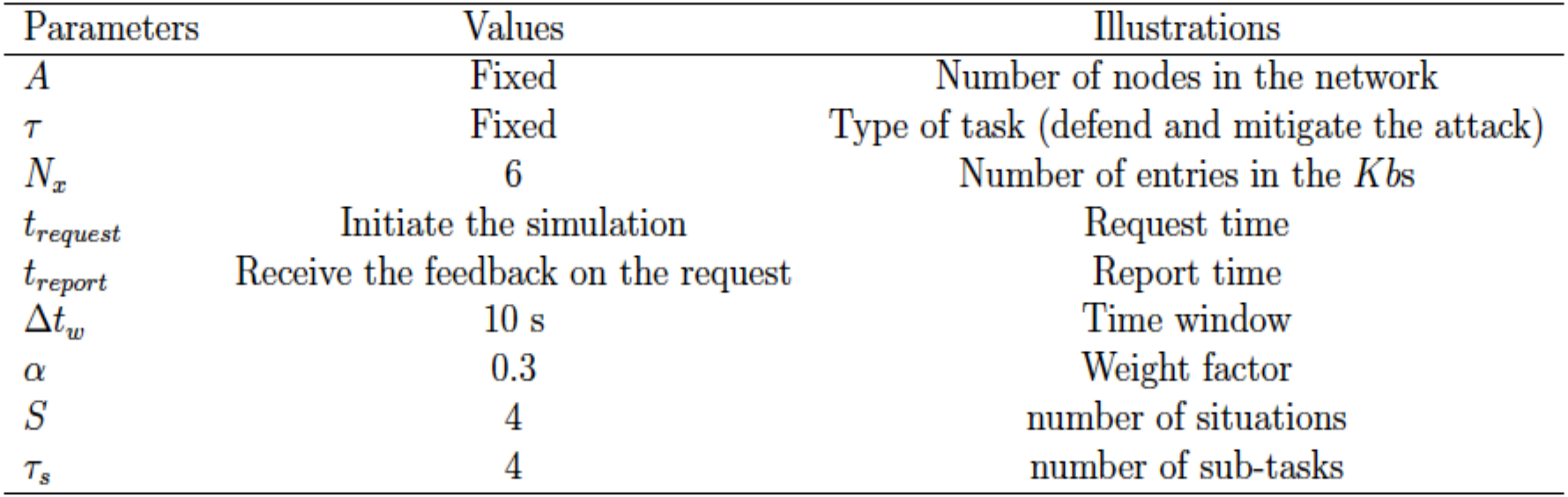
Algorithm 1 Calculate the Outcome Based on the Task's Deadline.

```
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 $d_8$
```

Kb_x

Originator's Id	Destination's Id	Req_t	Rep_t	Task type	Outcome of a task

Simulation settings and their illustrations



Parameters	Values	Illustrations
A	Fixed	Number of nodes in the network
τ	Fixed	Type of task (defend and mitigate the attack)
N_x	6	Number of entries in the Kbs
$t_{request}$	Initiate the simulation	Request time
t_{report}	Receive the feedback on the request	Report time
Δt_w	10 s	Time window
α	0.3	Weight factor
S	4	number of situations
τ_s	4	number of sub-tasks

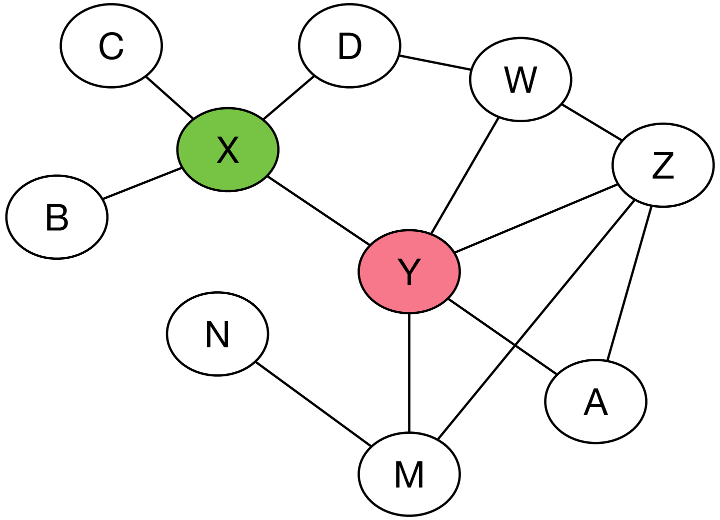
Scenario

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

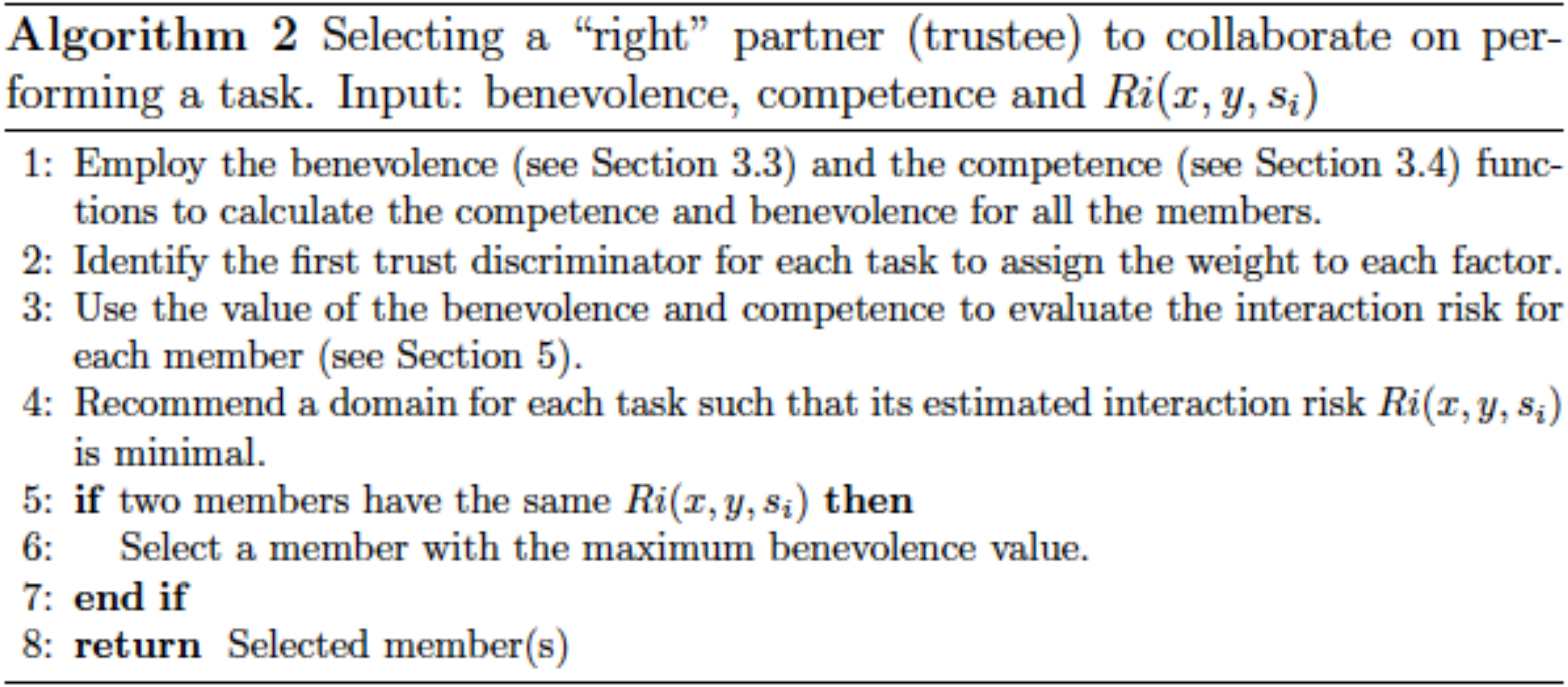
Task (τ): Mitigate and defend against a certain attack.

Sub-tasks:

- τ_{s1}: provide resources within a certain time window,
- τ_{s2}: monitor a certain traffic,
- τ_{s3}: block a certain link,
- τ_{s4}: implement a certain counter measurement.



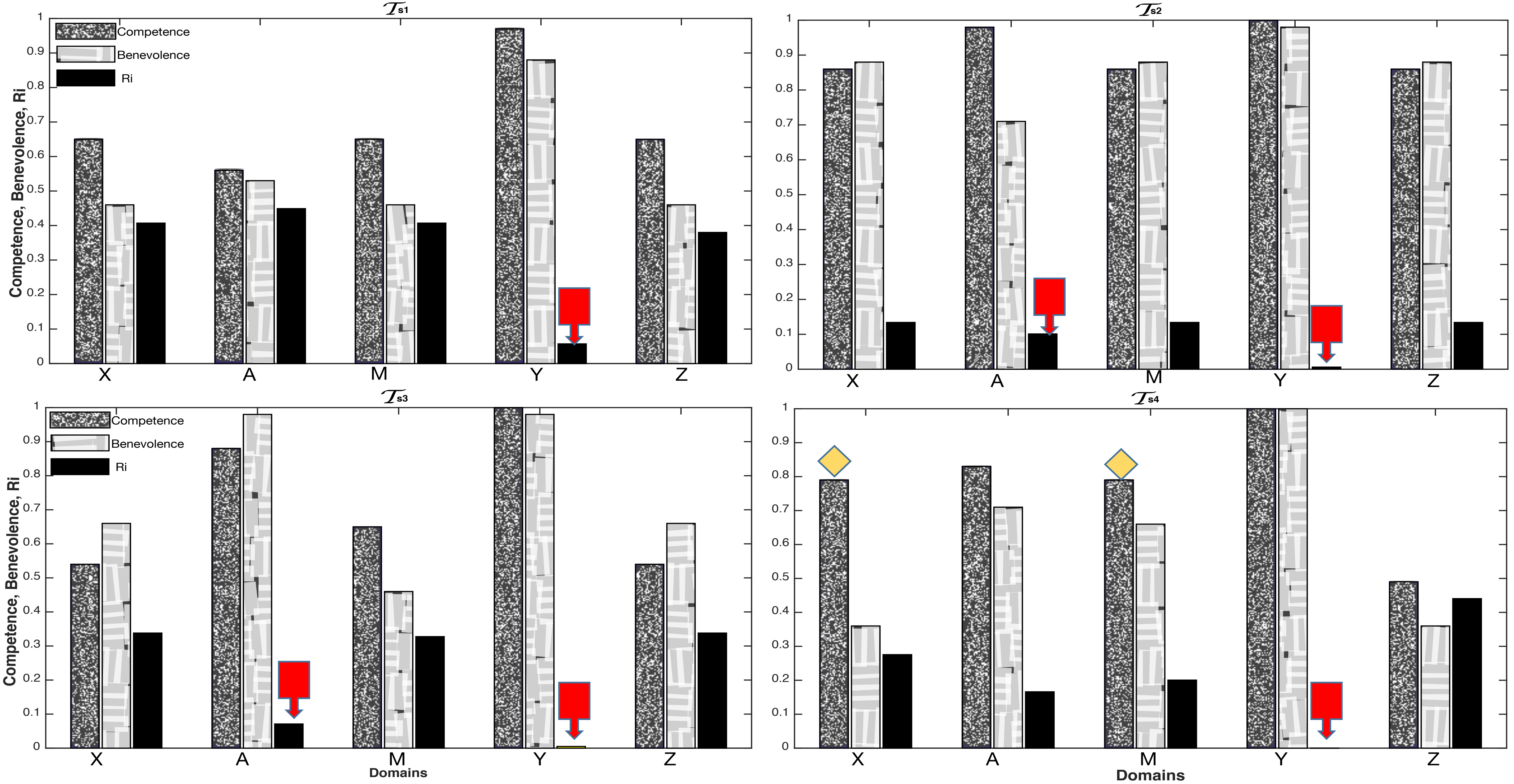
Selecting a “right” partner algorithm



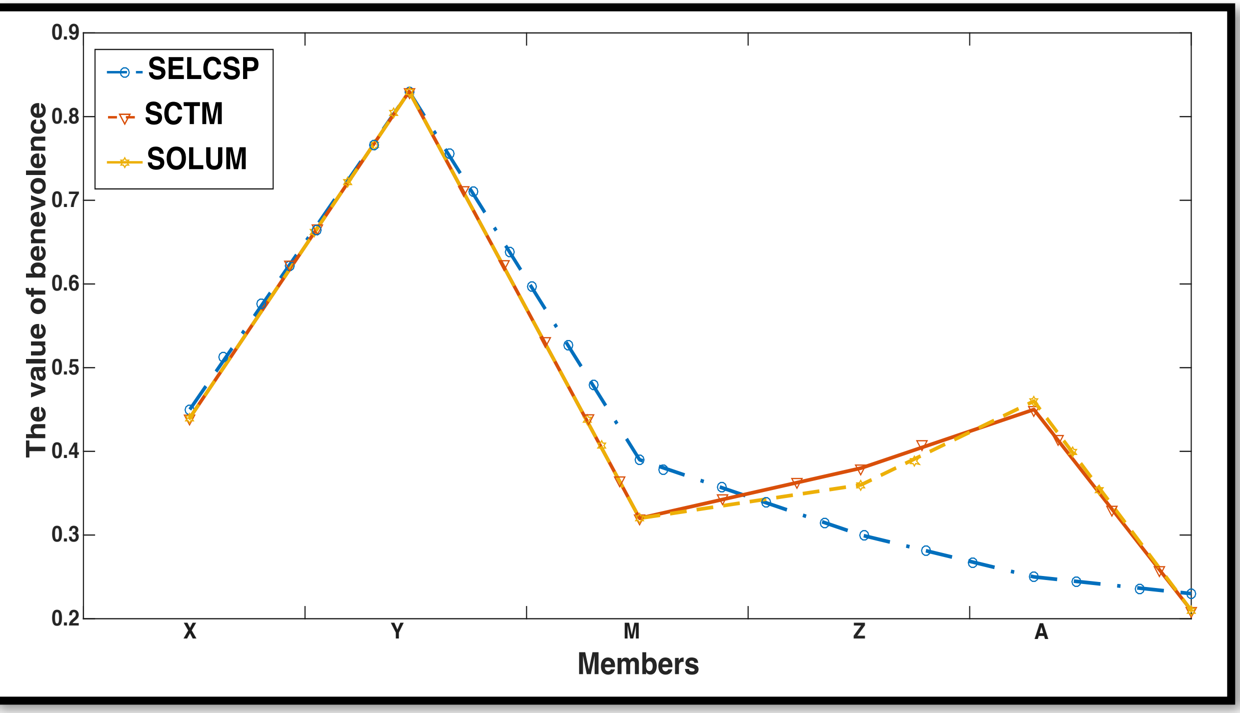
Algorithm 2 Selecting a “right” partner (trustee) to collaborate on performing a task. Input: benevolence, competence and $Ri(x, y, s_i)$

```
Employ the benevolence (see Section 3.3) and the competence (see Section 3.4) functions to calculate the competence and benevolence for all the members.
Identify the first trust discriminator for each task to assign the weight to each factor.
Use the value of the benevolence and competence to evaluate the interaction risk for each member (see Section 5).
Recommend a domain for each task such that its estimated interaction risk $Ri(x, y, s_i)$ is minimal.
if two members have the same $Ri(x, y, s_i)$ then
    Select a member with the maximum benevolence value.
end if
return Selected member(s)
```

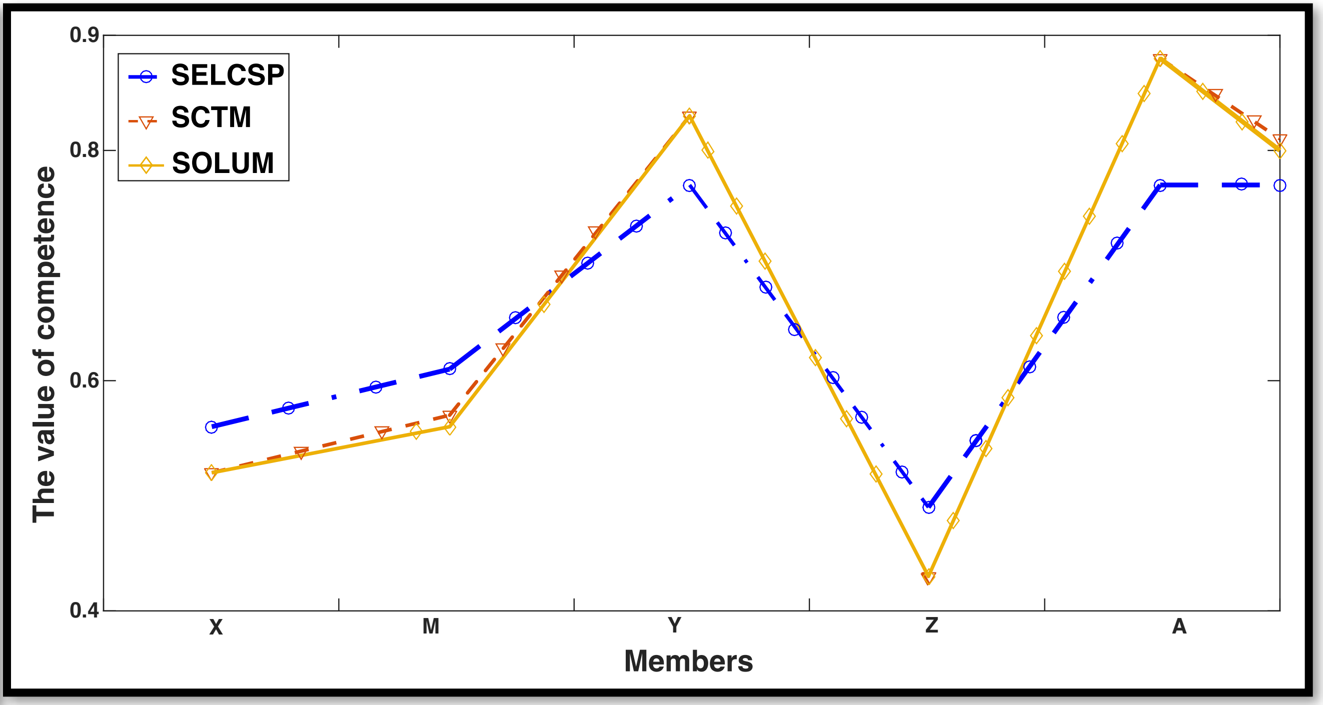
Result


$\mathcal{T}_{s1}$
$\mathcal{T}_{s2}$
$\mathcal{T}_{s3}$
$\mathcal{T}_{s4}$
Competence
Benevolence
Ri
Competence, Benevolence, Ri
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
X
A
M
Y
Z
Domains

Evaluation Result



The value of benevolence for three different algorithms

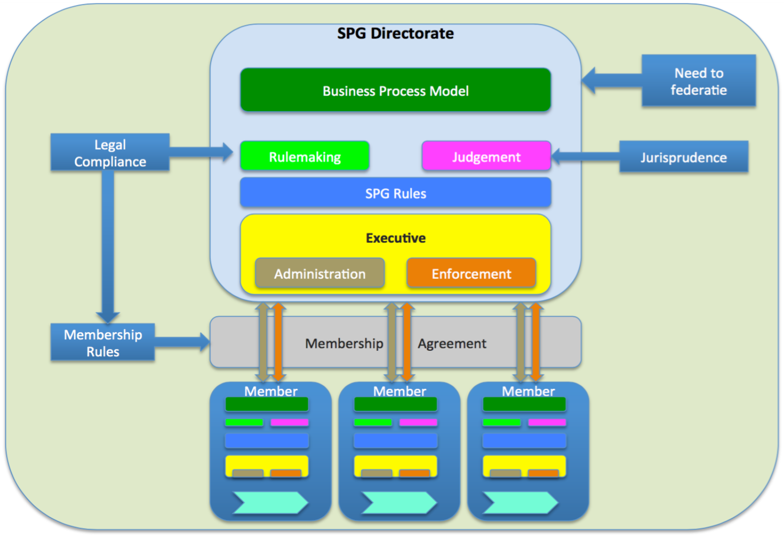


The value of competence for three different algorithms

Governance framework

Policies & Common rules (Governance framework)

- We use the **Service Provider Group (SPG)** framework to define a set of common rules and Policies
- **A normative Agent Based Model (N-BDI*)** to monitor the members' behavior
- Eduroam, Cyber threat Alliance
- Digital Data Market Place https://klm-4tlas.herokuapp.com/
  - Employ the block chain and smart contract to implement the rules.
  - Stability of the Digital Data Marketplace.



Conclusion

- To **evaluate** the **trustworthiness** of a trustee the **direct** and **indirect** evidence on the given trustee were taken into account.
- The **trust** value is computed by **three** trust factors, namely **competence, integrity** and **benevolence**.
- **Benevolence** is computed from **direct** evidence between a trustee and a trustor
- **Competence and integrity** are assessed on the base of the **received feedback** from the other alliance members (a trustee's direct neighbors).
- We are able to collect a **variety of evidence** on a trustee by introducing **eight dimensions** for each context.

Conclusion

- The **interaction risk** estimated through the **SCTM** by combining **benevolence** and **competence**.
- The **weighting factors** used to determine different weights to select the partners based on the task.
- We evaluated the SCTM framework with **SARNET Emulation** developed by Ralph.
- The **N-BDI* framework** defined to monitor the member’s behavior.

Thank you.

Ameneh Deljoo

a.deljoo@uva.nl