

Seventh International Crisis Management Workshop (CrIM'13)
University of Oulu (Finland), 25-26 November 2013

Trust and Reputation for Critical Infrastructure Protection

Filipe Caldeira^{1,2}

¹CISUC - DEI, University of Coimbra, Coimbra, Portugal

²Polytechnic Institute of Viseu, Viseu, Portugal

caldeira@estgv.ipv.pt

Outline

- Motivation / Introduction
- MICIE FP7 Project
- Trust and Reputation Model
 - The Trust and Reputation System
 - Validation
- Integrating Trust and the CI Security Model
 - Trust Based Dependency Weighting
 - Validation – Grid'5000
- Conclusions

Motivation

- "Critical infrastructures (CI) are those physical and cyber-based systems essential to the minimum operations of the economy and government.
 - Those systems are so vital, that their incapacity or destruction would have a debilitating impact on the defence or economic security” [1].
- CI sectors include, amongst others:
 - Electricity, telecommunication, air traffic and transport sectors.
- CIs can be **mutually dependent**
 - A failure in one CI can **cascade** to another (inter)dependent CI and cause service disruptions.

[1] Clinton, W.J.: Executive order 13010 - critical infrastructure protection. Federal Register 61(138) (July 1996) 37347

Motivation

- Governments and citizens are becoming aware.
- The media is also contributing to public awareness:
 - TV series “24” season 7
 - Government is worried about CI protection and protected every CI with a “CIP firewall”
 - One device + its programmer
 - (Michael Latham - kidnapped)...
 - ...terrorists make an intrusion in the air traffic control system and prove that they can control all (inter)dependent CIs in the country.



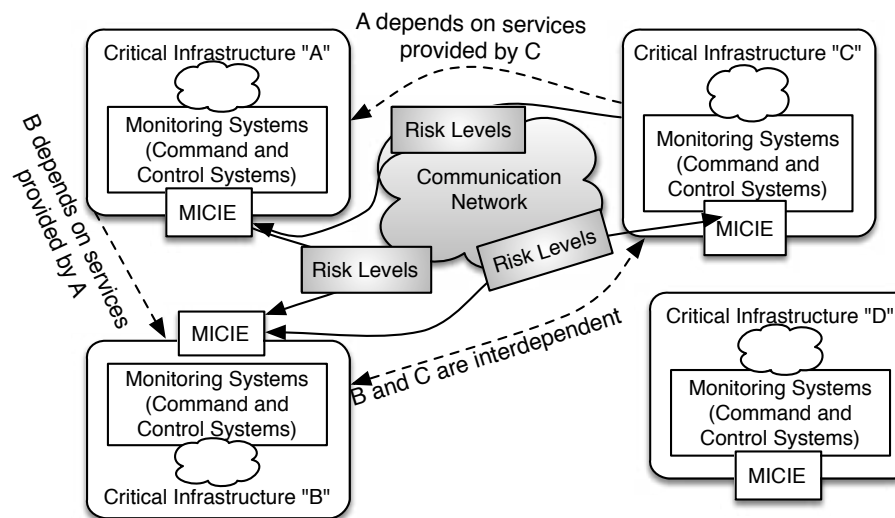
Now Jack Bauer has to
find the device...
We clearly need better

Introduction

- Critical infrastructures (CIs) are complex interacting systems providing services to customers.
- CIs may depend on services of other CIs
 - (Inter)Dependencies.
- CIs differ among each other, mainly regarding
 - The services they provide;
 - The components they are composed of;
 - Their organisational structure.
- In an attempt to model CIs and dependencies and share CI information
 - What is a “common ground” to model CIs?
 - How can information be presented?
 - Easy to exchange and interpret.

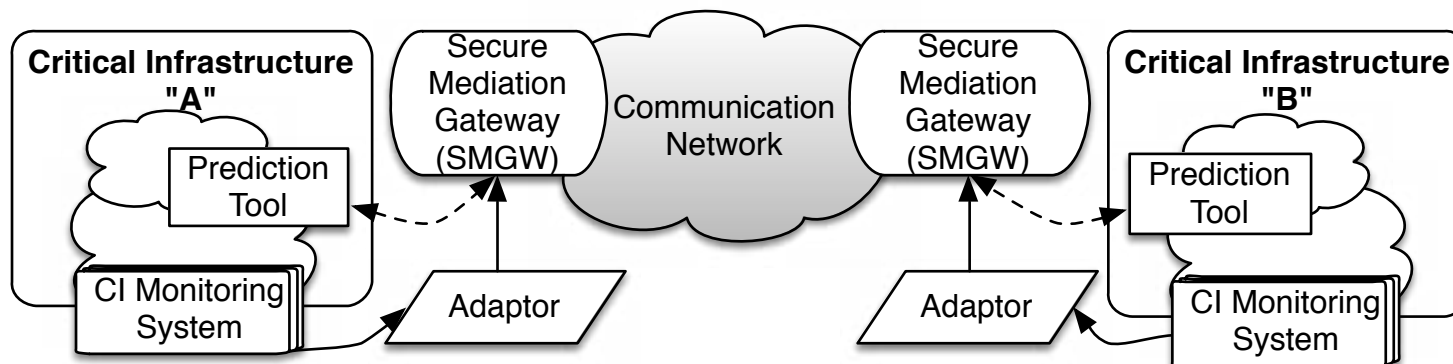
MICIE FP7 Project - MICIE Alerting System

- MICIE project (www.micie.eu) contributes in three main areas:
 - Identification and modelling of interdependencies among CIs;
 - Development of risk models and risk prediction tools;
 - A framework enabling secure and trustfully information sharing among CI.
- MICIE main goal:
 - To provide, in “real time”, each CI Operator with a CI risk level measuring the probability that, in the future, he will loose the capacity of provide some services or receive some service.



MICIE overall system architecture

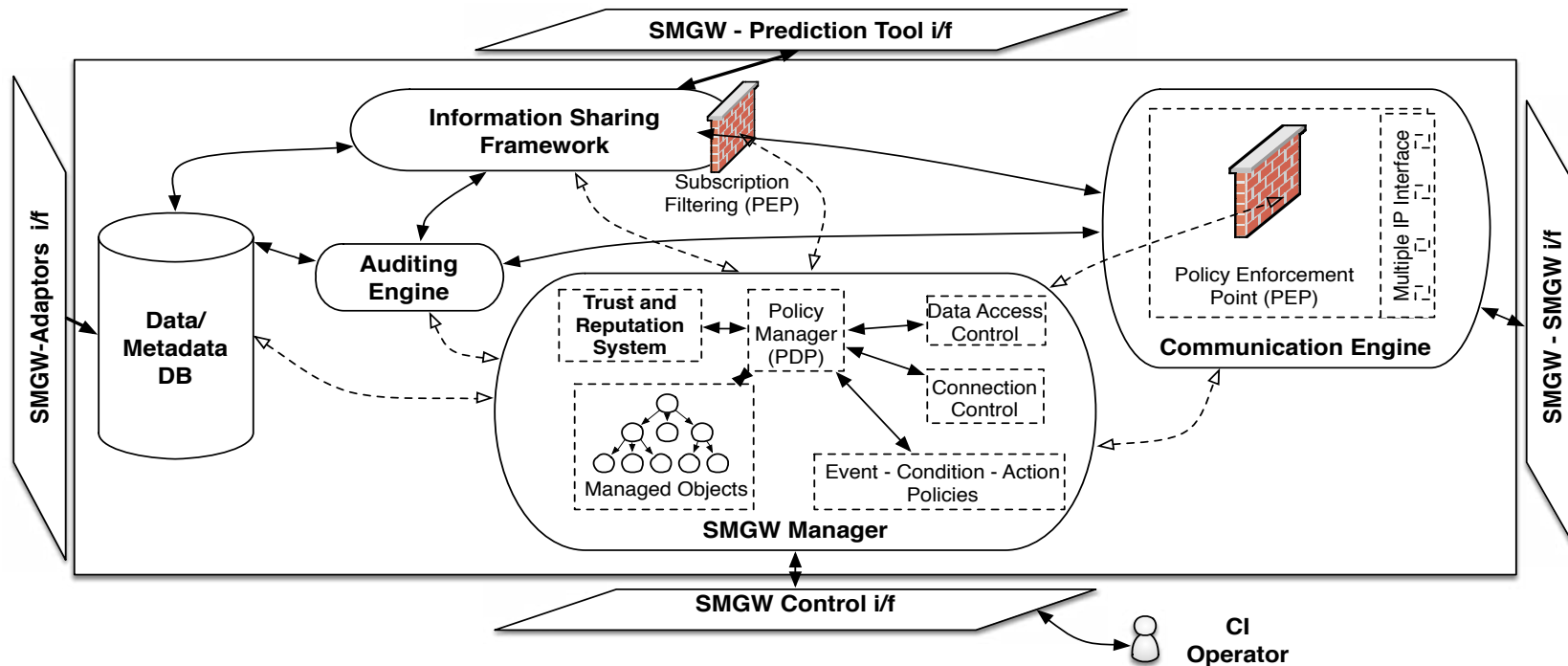
- Each CI collects, in “real-time”, information regarding the status of its components.
 - The adaptor selects proper information and handles format and semantic conversions.
 - The Prediction Tool make use of risk models to assess the risk level of monitored services.
 - CI own risk level is associated with the risk levels related to services received from partners (interdependent) CI.
 - Status information can be exchanged across CI using the SMGW allowing CI to work in a fully cooperative distributed environment for risk prediction.



MICIE SMGW - Secure Mediation Gateway

- SMGW main functions:
 - Provision of a secure and trustfully cross-CI communication infrastructure;
 - Collect information about the local CI;
 - Retrieve information about the other interdependent CIs in the system;
 - Send information related to local CI to remote CIs;
 - Composition of CIs critical events and semantic inference;
 - Provide all the collected information to the prediction tool
 - Provides a real-time view about identified risks and alerts.
- The SMGW design guarantees multiple security requirements:
 - e.g. , confidentiality, integrity, availability, non repudiation and auditability/traceability.
- Trust and reputation is part of the SMGW.

SMGW Architecture



- The **SMGW MANAGER** intends to manage all SMGW aspects.
- Developed according to the policy based management paradigm.
- It also performs monitoring with the help of the Auditing Engine
 - can also act as Intrusion Prevention and Detection Engine by configuring firewalls in the communication engine.

SMGW Manager

- Provides a tool where the CI operator can define, in a high level manner, the behaviour he pretends for the system.
- Handles authorization, authentication and accounting, for both interaction with peer SMGWs and all the internal operations.
- The CI operator can define policies addressing the relations between local SMGW and foreign SMGWs.
- Key Components:
 - Policy Database – stores all defined policies.
 - Policy GUI – interface with the administrator of the SMGW.
 - SMGW Manager/Policy-based Management:
 - The SMGW component responsible for authorizing access to the SMGW and to its data. It acts as the SMGW Policy Decision Point (PDP).
 - PEP - Policy Enforcement Points:
 - The PEPs control the access to the SMGW (communications, data) based on the rules received from the SMGW Manager. May include the firewall, the VPN server, Web Server, Data Access Services, ...
 - Trust and Reputation System.

Trust and Reputation for CI Protection

- Can we trust information received from peer CIs / Services?
 - Monitoring components can be faulty;
 - The peer CI ICT system can be compromised, sending false information;
 - The peer CI may intentionally provide inaccurate information.
- Is the behaviour of peer CIs / Services acceptable?
 - Has the monitoring framework been compromised?
 - Repeatedly trying to read non-authorized information?
- Answers to this questions are important as
 - The CI uses received alerts to infer its own risk levels;
 - Trusting false information affects risk assessment;
 - Shared information is highly confidential.

Trust Model

- Main Goal - Maintain real-time trust information about (inter)dependent CIs and CI services.
- There are two main areas where trust and reputation is applied:
 - A trust indicator about the risk alerts received from (inter)dependent CIs / Services (**Risk alerts trust**).
 - This indicator is evaluated at two levels:
 - **Service level**, evaluating each service received from a remote CI, reflecting trust on the risk alerts received from each dependent service;
 - **CI level**, evaluating an indicator for each interconnected CI, representing the reputation of that particular CI.
 - Understanding the (inter)dependent CIs behaviour in terms of ICT security (**Behaviour trust**).

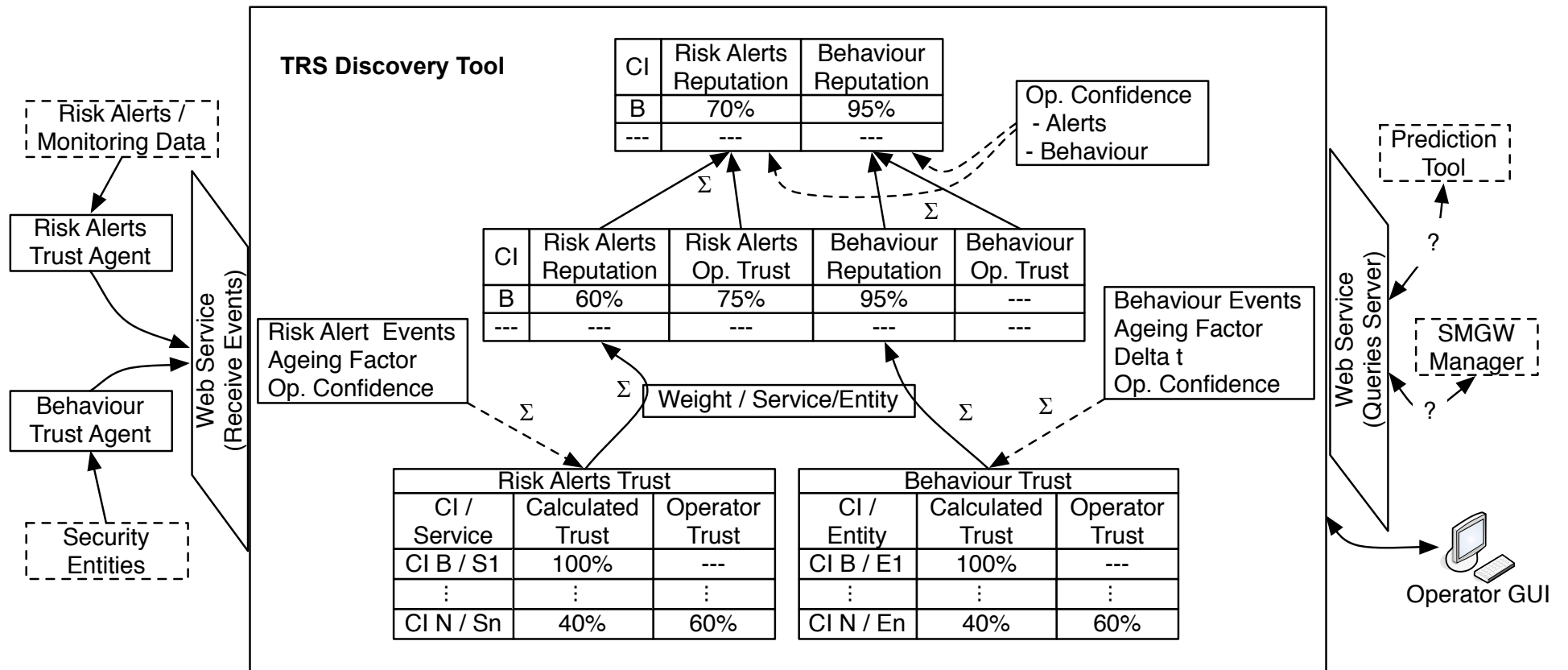
Trust and Reputation System

- An extension to the MICIE core framework
- The Trust and Reputation System allows:
 - To associate a level of trust to the data received from peer CIs, as well as to its own internal monitoring data (e.g. SCADA systems)
 - To use this associated trust level to enhance the accuracy of MICIE Risk Prediction Tools.
 - To detect defective components at local level (e.g. faulty hardware sensors, software bugs) which consistently provide inaccurate information.
 - To detect partner CIs / Services which provide inconsistent information.
 - To Incorporate trust indicators into:
 - The risk assessment tools (thus limiting the impact of inconsistent information)
 - The access policies of the MICIE framework (limiting the access of non-trusted partners to sensitive data)

Trust and Reputation Service – Input sources

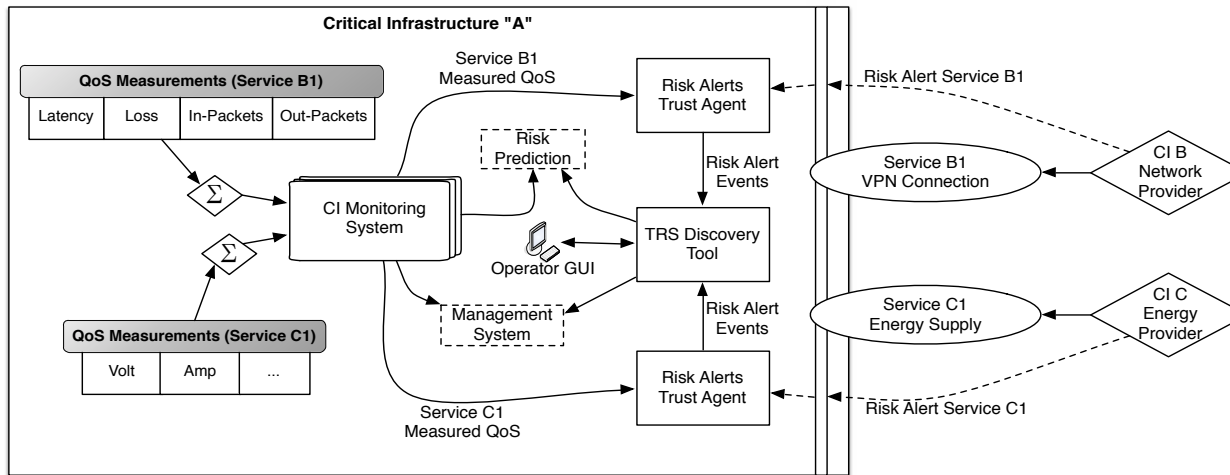
- **Analysis of past data provided by partner/“service”**
 - Each partner CI provides and/or receives a number of “services” (the interdependency links)
 - For each provided “service” the partner CI also provides a risk assessment estimate, related to its availability or QoS.
 - Compare the risk estimates provided over time, for each “service”, against the actual service levels, to infer the trustiness of future estimates.
- **Analysis of partner behavior**
 - If the partner CI behaves abnormally (for instance trying to access non-authorized data or using non-authorized credentials) downgrade the global level of trustiness associated with that partner CI.
- **Human factor (Optional)**
 - Incorporate the perception of the human operator about each partner or “service”.

Trust and Reputation System

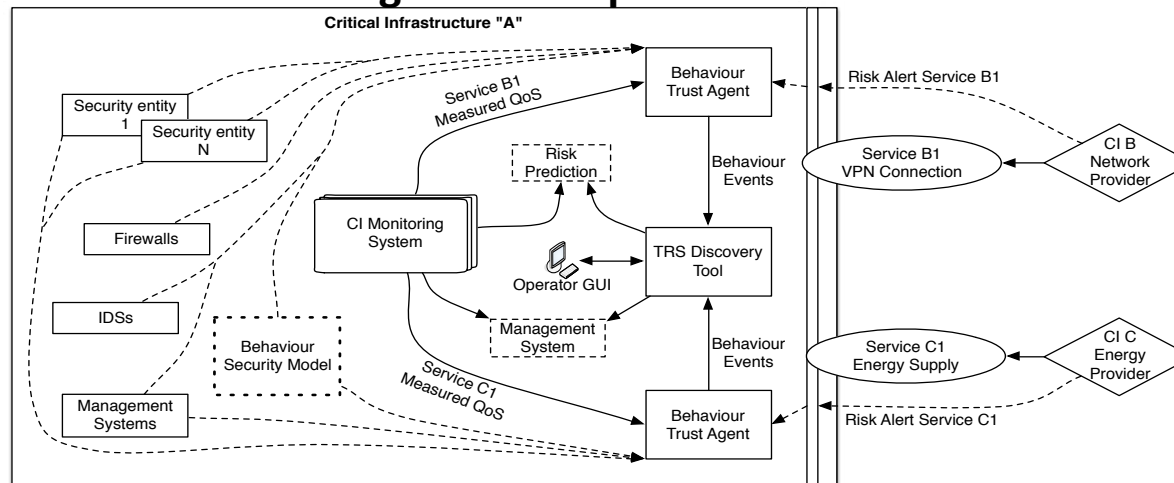


TRS Agents

Risk Alerts Trust Agents example



Behaviour Trust Agents example



Risk Alerts Trust Evaluation (1)

- An Event is triggered in a situation in which the received risk is different from normal, the monitored service QoS decreased or both.
- The Event accuracy is defined as the average of all comparisons made during the event.
- The trust that one CI has in the risk estimates received for a “service” provided by another CI is based on the accuracy of each past event between those two CIs (for that specific “service”) with defined factors depending on the context:
 - Penalization factor (penalize larger estimation errors)
 - Aging factor (recent events are granted more weigh than old events, using an aging factor applied to each event).

Risk Alerts Trust Evaluation (2)

- Event accuracy:

$$A(Event_n) = \frac{\sum_{t=1}^T (f(Sl_t, Rl_t))}{T}$$

$$f(Sl_t, Rl_t) = |Sl_t - Rl_t|^\kappa, \kappa \in R^+$$

- Trust that CI has for service X provided by CI B :

$$T'_{(A,B,X)} = \frac{(D * (N - 1) * T_{(A,B,X)}) + A(Event_N)}{D * (N - 1) + 1}$$

$$T(final)_{(A,B,X)} = \alpha(T_{(A,B,X)}) + \beta(TO_{(A,B,X)}), (0 < \alpha, \beta < 1), (\alpha + \beta = 1)$$

- K - Penalization factor (penalize the bigger differences)
- D - Aging factor (weigh recent events more than old events using a discount factor applied to each event).
- N – Event Number
- T(final) – Incorporating Operator trust (TO)

Reputation - Multiple Services

- It is possible to weight each service according to his relevance.
 - for instance, giving more weight on more critical services and less weight to services that have less impact on our CI.

$$GT'_{(A,B,t)} = \frac{(D * (N - 1) * GT_{(A,B)}) + \frac{\sum_{i=1}^S (T(final)_{(A,B,i)} * W_i)}{\sum_{i=1}^S W_i}}{D * (N - 1) + 1}$$

$$GT(final)_{(A,B,t)} = \theta(TO_{A,B}) + (1 - \theta)(T_{(A,B)}) \quad , (0 < \theta < 1)$$

- D - Aging factor (weigh recent events more that old events using a discount factor applied to each event).
- N – Event Number
- S – Number of services
- Wi – Service i weight
- GT(final) – Incorporating Operator trust (TO)

Behaviour Trust Evaluation (1)

- It is usual for CIs ICT system to gather a collection of data related to security aspects of the system
 - It is possible to use this valuable information in order infer a Trust indicator on each CI / Service behaviour.
- Normalization of received information - Security model

Failed Authentication Attempts/Minute		
Trust Indicator Level	Description	Received Values
100	No Failures	0
80	One/Three Failures	1-3
20	Four/Ten Failures	> 3 and < 10
0	More that 10 Failures	>= 10

- Security Indicators can be evaluated based on:
 - Intrusion Detection System
 - QoS measurements
 - Monitoring Systems

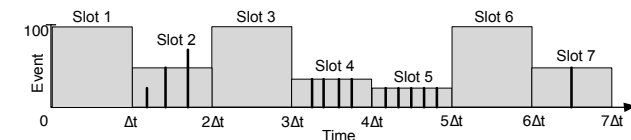
Behaviour Trust Evaluation (2)

- In order to consider aging in trust calculation, we consider time as a set of time slots. Each time slot will have a defined duration and represents an Event in the calculations.
 - No activity in one time slot means that peer behavior was as expected so the maximum value should be given to this event.
 - If alarms are received during the time slot, the estimated value for the slot will take into account all events that took place.
 - Size of time slot should be dependent on the context.
 - An aging factor is also applied.
 - A Penalization factor may also be used.

Behaviour Trust Evaluation (3)

- In order to consider time in trust calculation, we consider time as a set of time slots, each one representing an event.
 - Size of time slot should be dependent on the context

$$Event_{(Slot\ s)} = \begin{cases} 100, & \text{if } NEvents_{(Slot\ s)} = 0 \\ \frac{\sum_{i=1}^N Event_i}{N}, & \text{if } N = NEvents_{(Slot\ s)} > 0 \end{cases}$$



- Behaviour Trust :

$$T'_{(E,B,s)} = \frac{(D * (s - 1) * T_{(E,B)}) + Event_{(Slot\ s)}}{D * (s - 1) + 1}$$

$$T(Final)_{(E,B)} = \theta(TO_{(E,B)}) + (1 - \theta)(T_{(E,B)}) \quad , (0 < \theta < 1)$$

- D - Aging factor (weigh recent events more than old events using a discount factor applied to each event).
- t - Time
- T(final) - Incorporating Operator trust (TO)

Reputation on CI/Service Behaviour

- Global Trust on CI Behaviour :

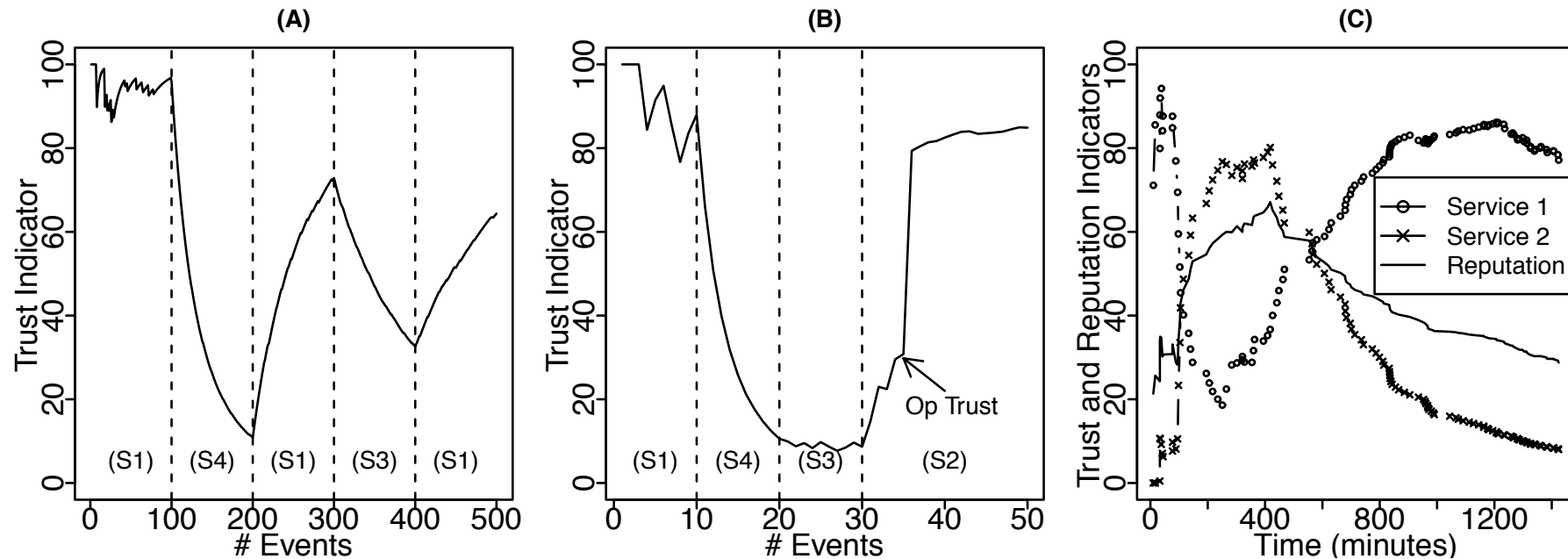
$$TBehaviour'_{(B,t)} = \frac{(D * (t - 1) * TBehaviour_{(B)}) + \frac{\sum_{i=1}^E (T(Final)(i) * W_i)}{\sum_{i=1}^E W_i}}{D * (t - 1) + 1}$$

- D - Aging factor (weigh recent events more that old events using a discount factor applied to each event).
- t – Time
- E – Number of security entities
- Wi – Entity i weight
- TBahaviour(final) – Incorporating Operator trust (TO)

Validation (Small scenario)

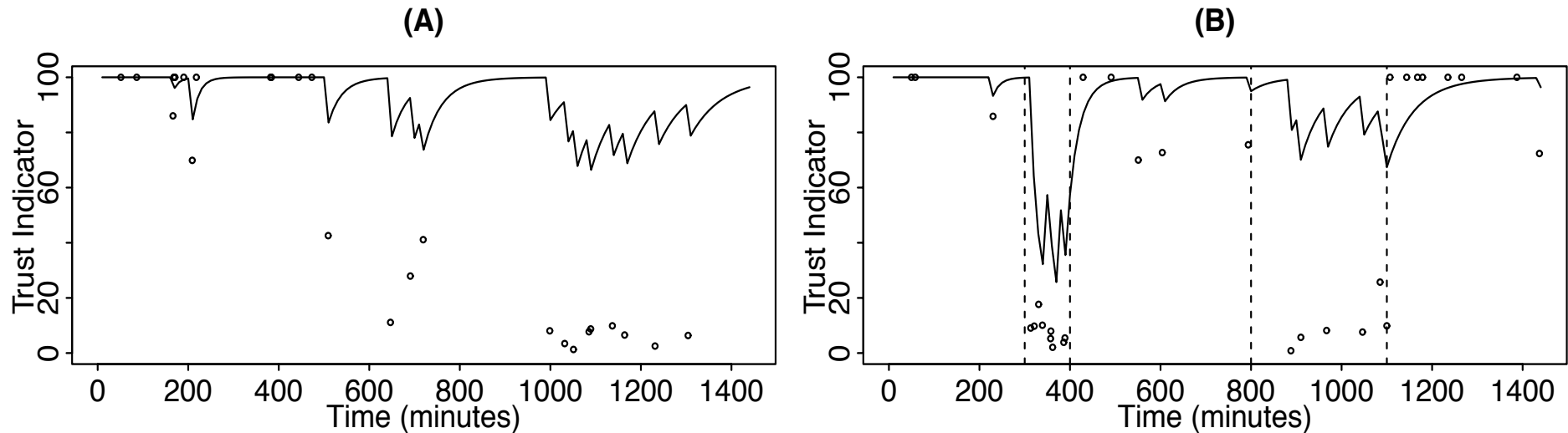
- Simulation example:
 - The events are generated using a normal distribution
 - Threshold =10% (trust values above 90% are rated as 100%)
 - 4 scenarios defined:
 - (S1) The system behaves as expected with only small errors with the event accuracy always above 60% and mainly between 90% and 100%;
 - (S2) System is not accurate but can still be trustworthy, as evaluated event accuracy is always above 40%;
 - (S3) Received alerts are not as expected with above 40% of inaccurate indications but never rising above 60%;
 - (S4) System is inaccurate.

Simulation: attack or faulty component situation



- Figures (A),(B) - It is visible that the trust indicator decreases rapidly and next starts to grow gradually depending on the scenario.
 - Figure (B) describes the use of the Human Factor showing that the operator can rapidly change the trust in a service. Less information is used for this simulation.
- Figure (C) – Two different services (weights: 0.7 to service 2, 0.3 to service 1).
 - In this simulation, when the service more important is becoming unreliable, then the CI reputation is decaying even when the other service is trusty.

Simulation: Behaviour Trust



- Fig (A) has a rate of 1 event per hour from scenarios S1, S3 and S4.
 - With few events, the indicator does not drop below 60% - influence of the slots where the system is behaving well. Demonstrate how important the values defined for the time slot.
- Fig (B) - Possible attack or misbehaviour in a small period of time.
 - First 300 minutes - 1 event/hour from S1; Next 100 minutes - 5 event/hour from S4.
 - The trust indicator rapidly decays below 50% clearly indicating that something is wrong.
 - Next, the behaviour is simulated using (S2) with a lower event rate leading the indicator to raise.
 - Between the 800th and 1100th minutes, the scenario changes to (S4) with a event rate of 1/60 minutes.
 - It is observable that even with only a few events, the CI Operator can infer that the peer behaviour is not normal.

TRS MICIE Implementation

Reputation Service – Admin Tool

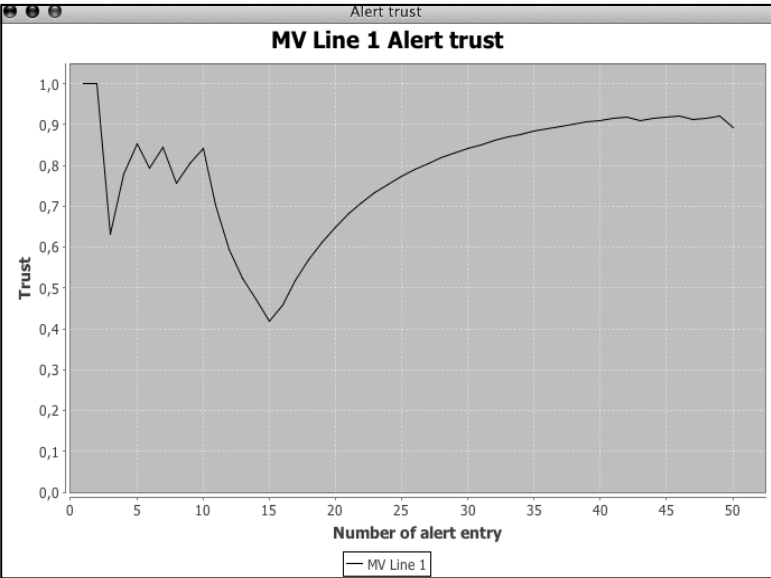
Data

ICT Behavior trust | **Alert trust** | CI trust | Global CI trust | Global trust | CI Settings | Service Settings | Entity Settings

CI Name	Service Name	Calculated Trust	Operator Trust
CI B	(4) Authentication	100 %	50.0 %
CI A	(3) IDS System 1	100 %	50.0 %
CI B	(2) MV Line 2	100 %	50.0 %
CI A	(1) MV Line 1	89 %	50.0 %

Alert trust

MV Line 1 Alert trust



Trust

Number of alert entry

MV Line 1

MICIE Reputation Service – Event Discovery Agent

File Help

MICIE Reputation Service

MICIE

Event type: ICT Beha... ▾

Input file:

Interval: 1.000 ▾ Start timer

MICIE Reputation Service – Event Discovery Agent

File Help

MICIE Reputation Service

MICIE

Event type: Alert ▾

Input file: Load

Interval: 1.000 ▾ Start timer Stop timer

Application to CI Security Model¹

- **CI Security Model**

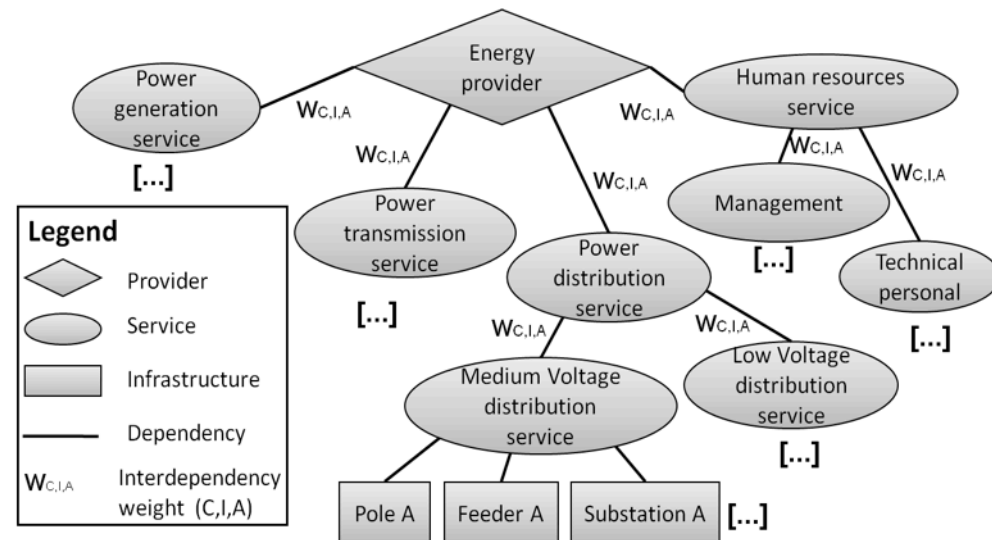
- CI model based on CI services and the dependencies among services
- To enable on-line monitoring of CI service risk
- Estimate current (on-line) risk of a CI service
 - Real-time measurements defining the state of CI service (base measurements)
 - Estimated risk received from dependent services
 - Expressed in terms of confidentiality, integrity and availability (CIA)
 - Aggregation using averaged weighted sum method
 - Using a weight determining the importance of an entity to the CIA of a service
- **How can shared information be evaluated for correctness?**

¹ Proposed by Thomas Schaberreiter

CI security modelling - Infrastructure analysis

- Decomposition into provided services

- Tree-like representation
- Each service can be composed of sub-services and infrastructure
- Weight sub-services according to their contribution to C,I,A of the service

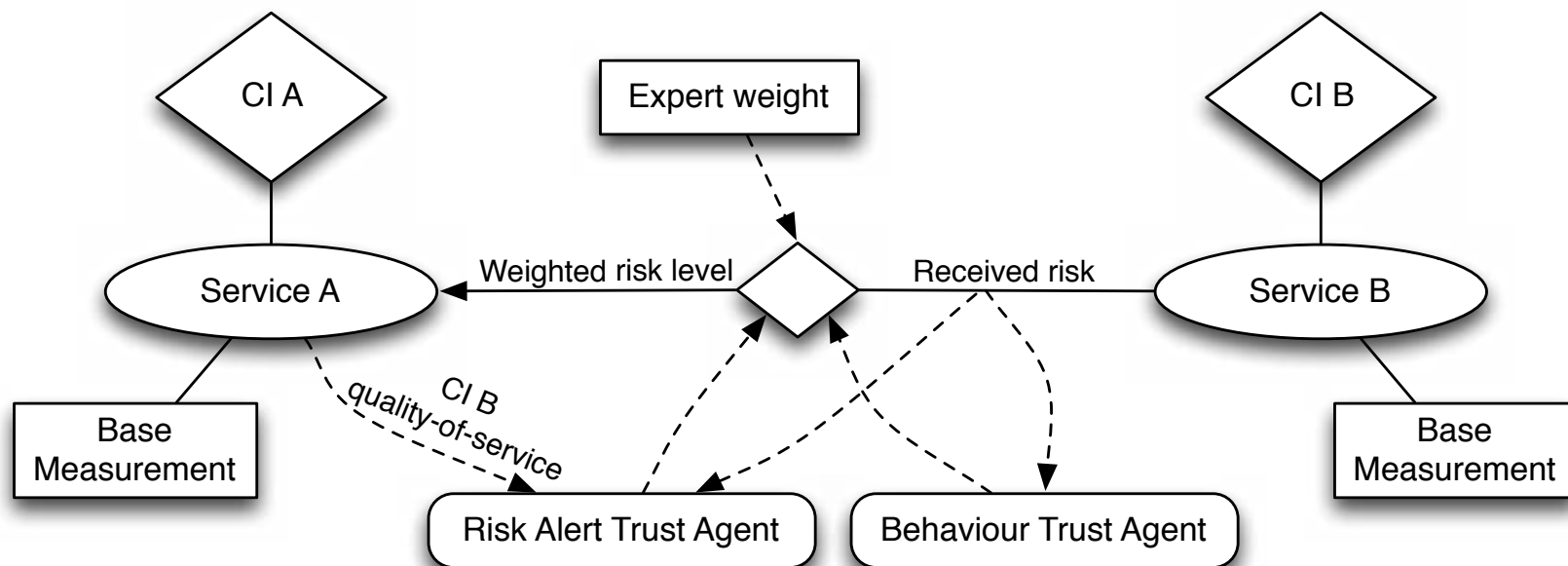


- Identification of base measurements

- Weight according to contribution to C,I,A of the service
- Determine normal behaviour and allowed deviation from normal behaviour

Trust and CI Security Model

- To evaluate the trust that each CI as on received risk alerts (risk alert trust), an entity has to be found that can be compared with each risk alert for the evaluation of its correctness.
 - Local risk indicators can be aggregated that can be compared with the received risk alert.



Trust Based Dependency Weighting

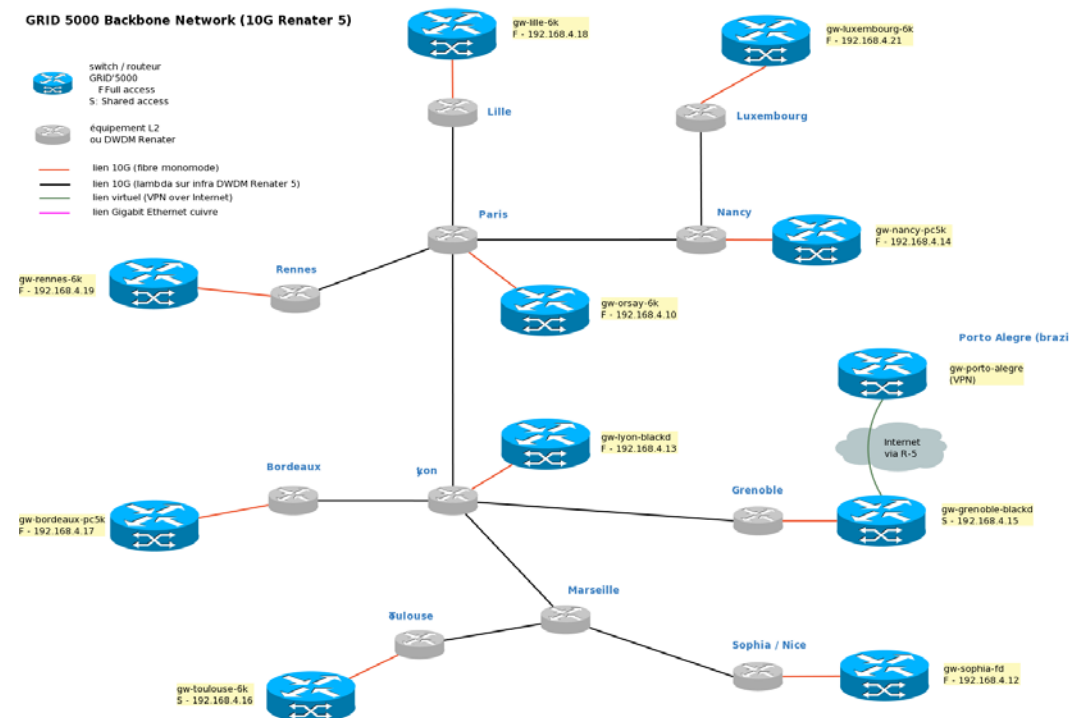
- CI security model shortcoming
 - The weights for dependencies and sub-services have to be assigned by experts and are thus prone to human error and inaccuracies.
- Trust based weighting
 - Calculate trust for the risk alerts received from each (inter)dependent CI or CI service and to combine the calculated trust with the initial weights assigned by experts;
 - Result in a more precise estimate of the influence one service has to another.
- The weight assigned by an expert now represents the maximum assumed influence a dependent service can have to a service.
 - According to the current risk alert trust provided by the dependent service, this weight can be lowered accordingly.

Case study: the Grid'5000 project

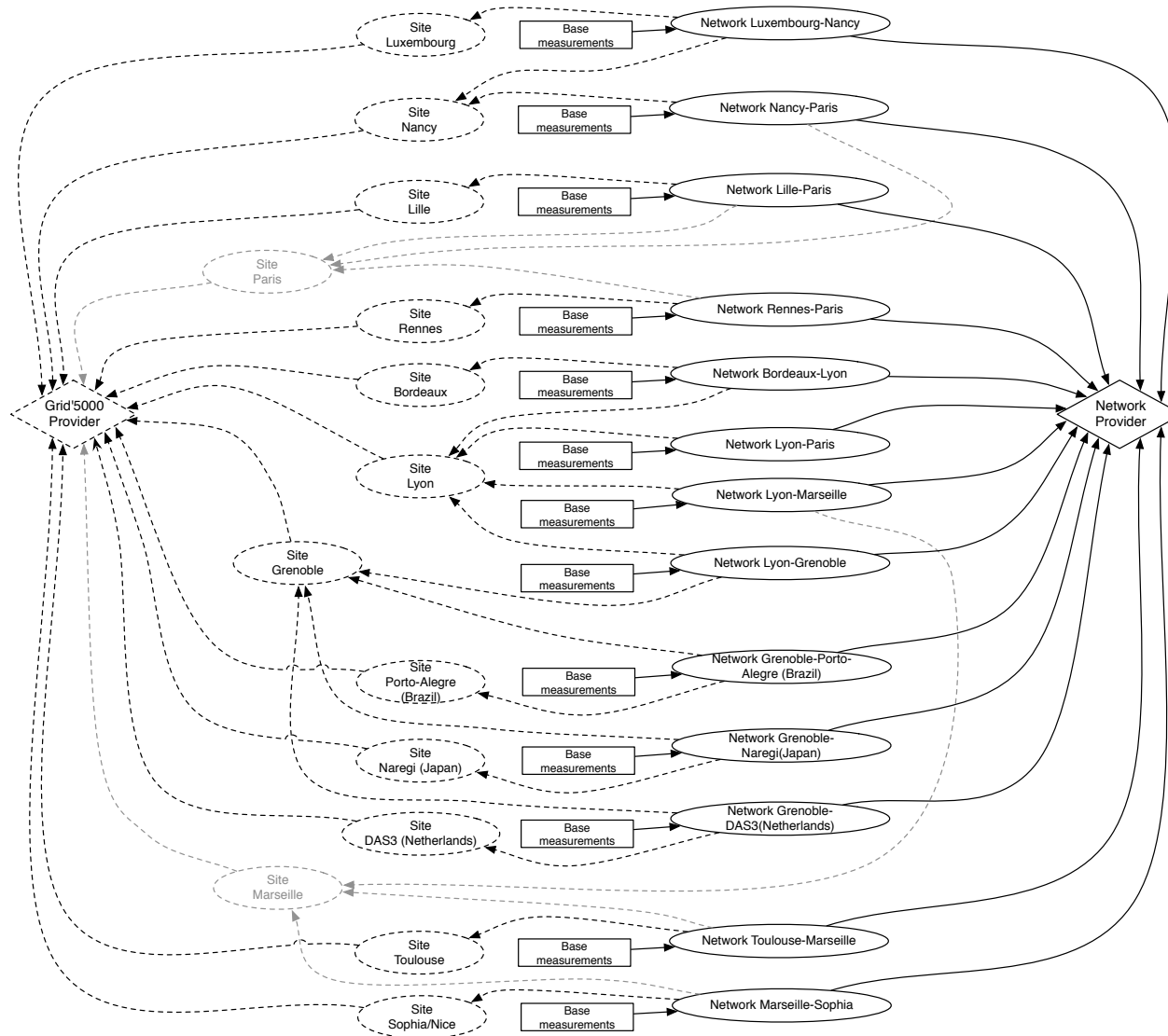
- Validation example - Case study based on a realistic scenario
- The Grid'5000 grid platform.
 - Provides a fully customizable testbed for advanced experiments in areas as parallel, large-scale or distributed computing and networking.
 - Grid'5000 can be seen as a CI involving several crucial security components:
 - the Puppet infrastructure, responsible for the configuration of all grid services within Grid'5000;
 - the Chef and Kadeploy infrastructure, which pilot the deployment of the computing nodes of the platform;
 - the resource manager of Grid'5000 (OAR);
 - **the network backbone**, operated by independent providers, namely Renater in France and Restena in Luxembourg.

Case study: the Grid'5000 project

- Components are distributed among a set of nine geographical sites that compose Grid'5000
 - eight in France (Bordeaux, Grenoble, Lille, Lyon, Nancy, Reims, Rennes, Sophia, Toulouse)
 - one in Luxembourg.
 - extra international connections to Brazil, Japan and the Netherlands are operated via the site of Grenoble.

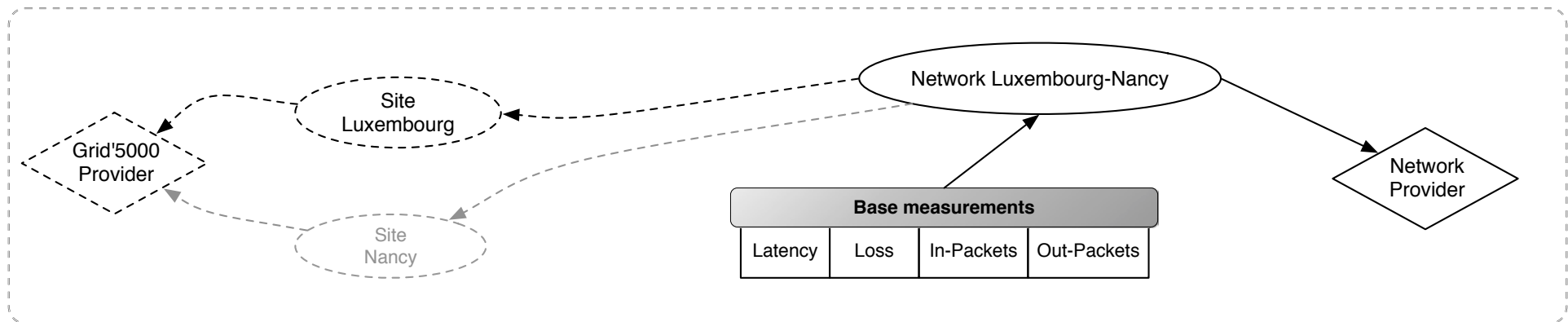


Dependency Grid'5000 / Network infrastructure

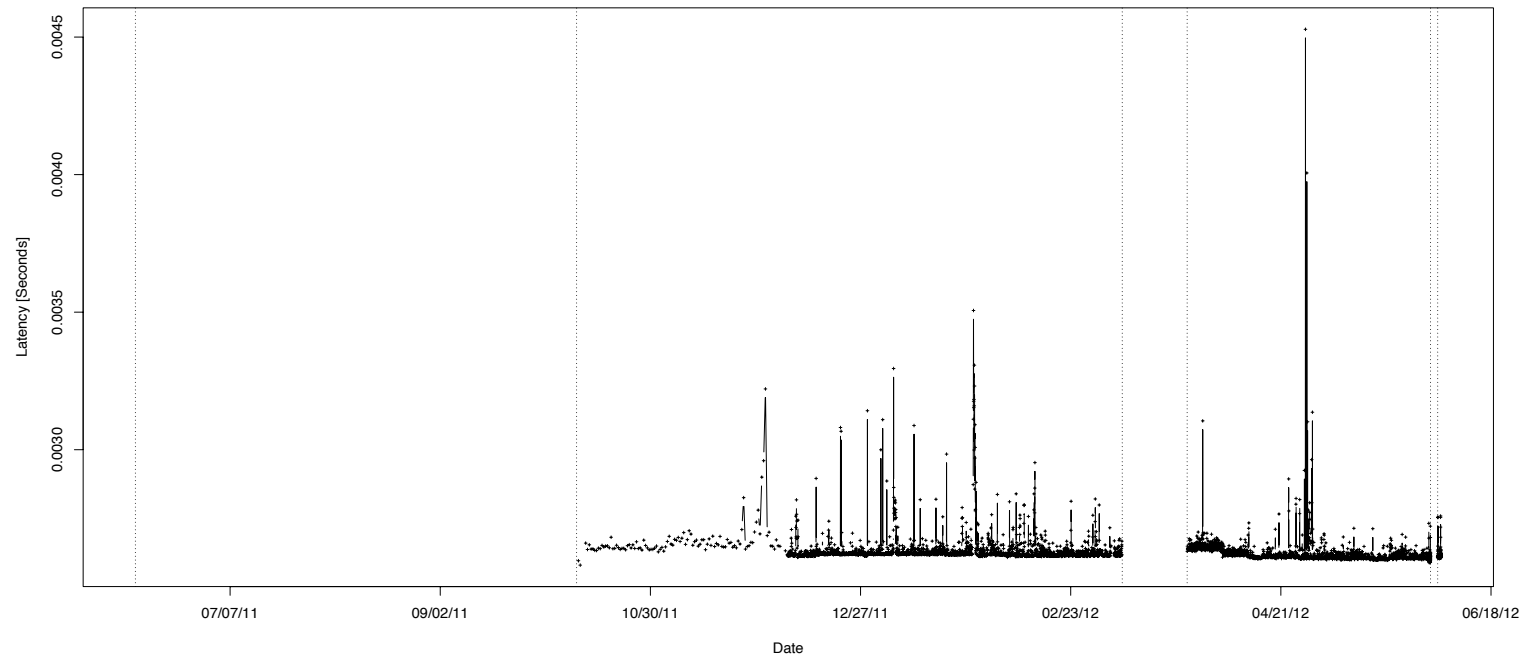


Luxembourg-Nancy network segment

- Four base measurements were identified that characterize this network segment:
 - **Latency:** The time a packet travels from source to destination and back again (in seconds).
 - **Loss:** The number of packets that are lost while measuring the latency.
 - **In-Packets:** The number of packets entering the segment (in packets/second).
 - **Out-Packets:** The number of packets leaving the segment (in packets/second).



Latency dataset for network segment Luxembourg-Nancy

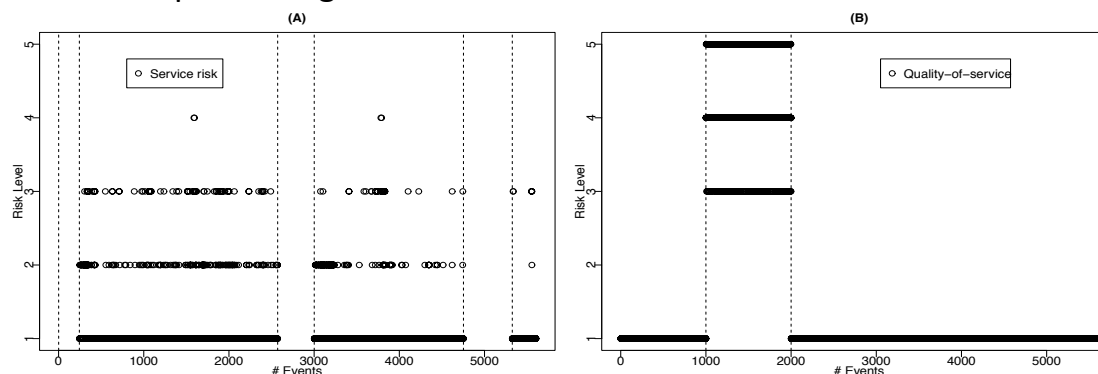


- To create an interesting example with the existing data, it was decided to lower the boundaries for what is considered a risk to the intervals illustrated in the presented table.
- Following representations will not consider date but events.

Risk Level	Latency in Seconds
1	≥ 0 and < 0.00265
2	≥ 0.00265 and < 0.0027
3	≥ 0.0027 and < 0.0033
4	≥ 0.0033 and < 0.005
5	≥ 0.005

Grid'5000 Case study

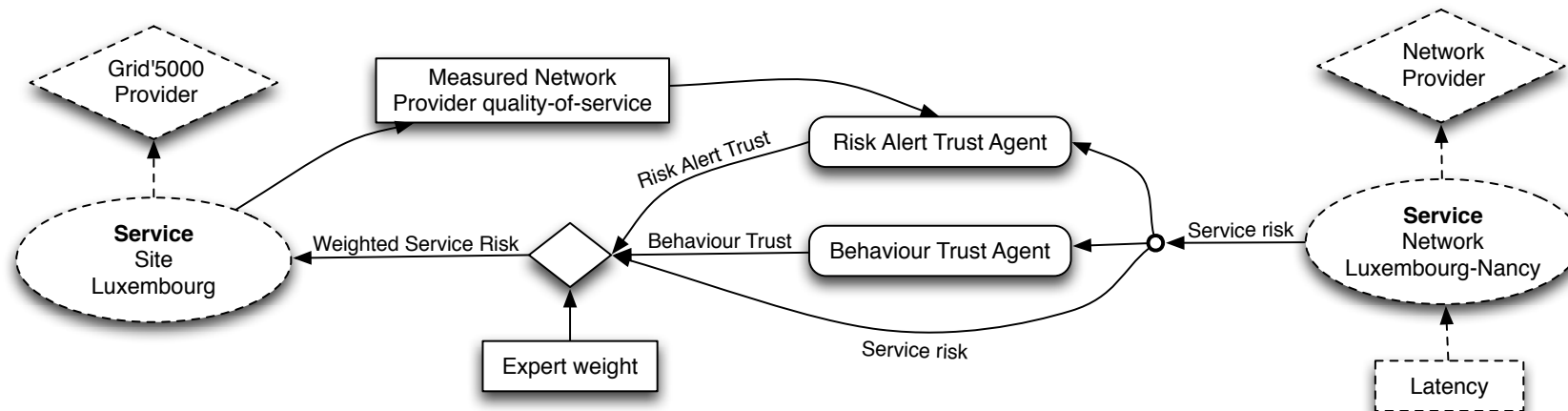
- (A) Service risk for network segment Luxembourg-Nancy;
 - Results obtained by using previous table for evaluate service risk
- (B) Network provider quality-of-service for network segment Luxembourg-Nancy
 - Defined values representing the measured QoS for the received servic.



- We assume that a risk level should be sent by the network provider at fixed and defined time intervals
 - To evaluate risk alert trust, we defined:
 - When a NaN value is received (or nothing) it is assumed that the risk alert is 1 (no risk). With more consecutive missing values, the received risk is increased until 5 (maximum risk).
 - This can be seen dangerous as it implies that the worst-case is assumed if no information is received. This is where the behaviour trust indicator is used
 - The behaviour trust is evaluated based on the absence of information.
 - If NaN value (or nothing) is received, this is seen as abnormal behaviour and the behaviour trust is lowered (an isolated missing value triggers a behaviour event with a value of 80 (in a scale of 1..100). Next consecutive missing values trigger events with a value decreasing by 20. Therefore, the high assumed risk values during periods where no information is received will have less influence in service risk estimation.

Experimental set-up

- Set-up overview

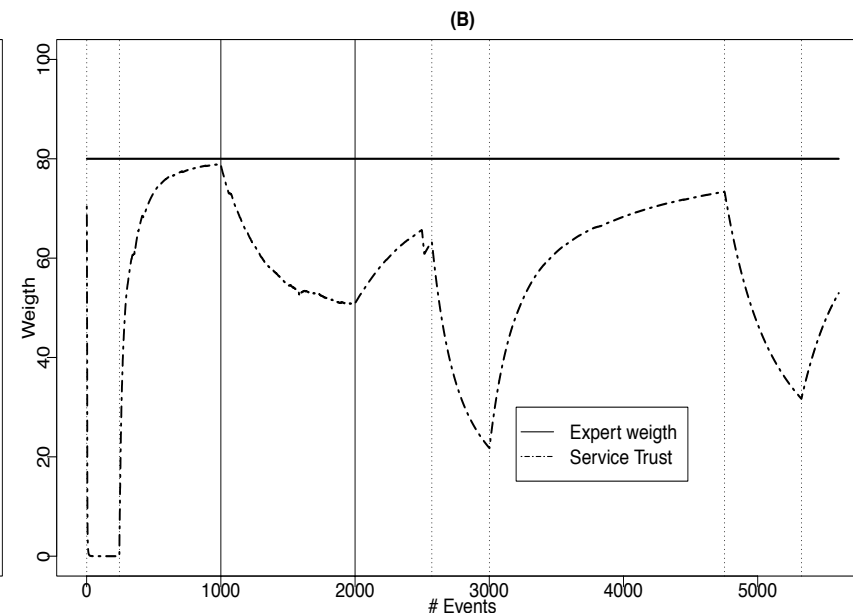
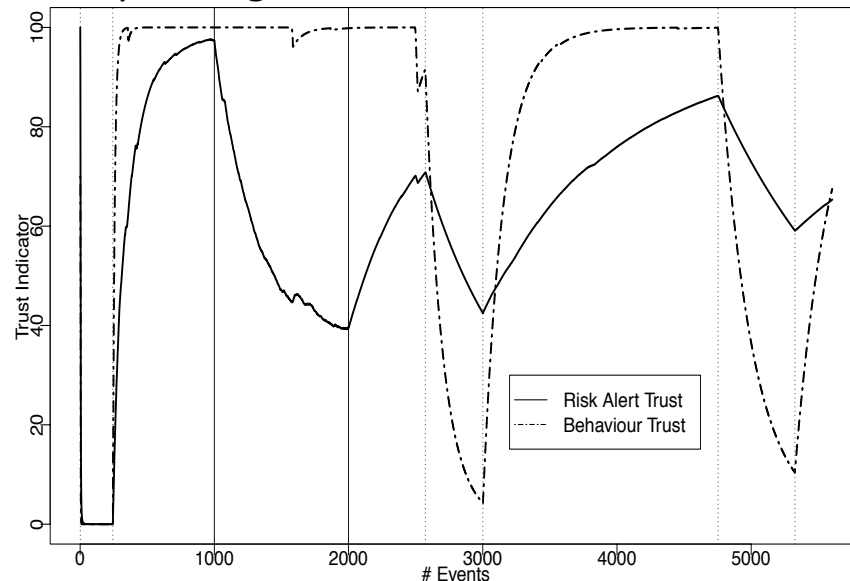


- The simulation was conducted in the statistical simulation tool R. Following parameters were used for the simulation:
 - Risk alert trust: penalisation factor $k = 1.25$; ageing factor $D = 0.3$.
 - Behaviour trust: $\Delta t=2$ and $D=0.3$.
 - Service trust: $\beta=0.6$ (60% risk alert trust and 40% behaviour trust).
 - Expert weight: $\omega_E = 80\%$.

Details on how risk alert and behaviour trust are computed can be found in the references given in the last slide.

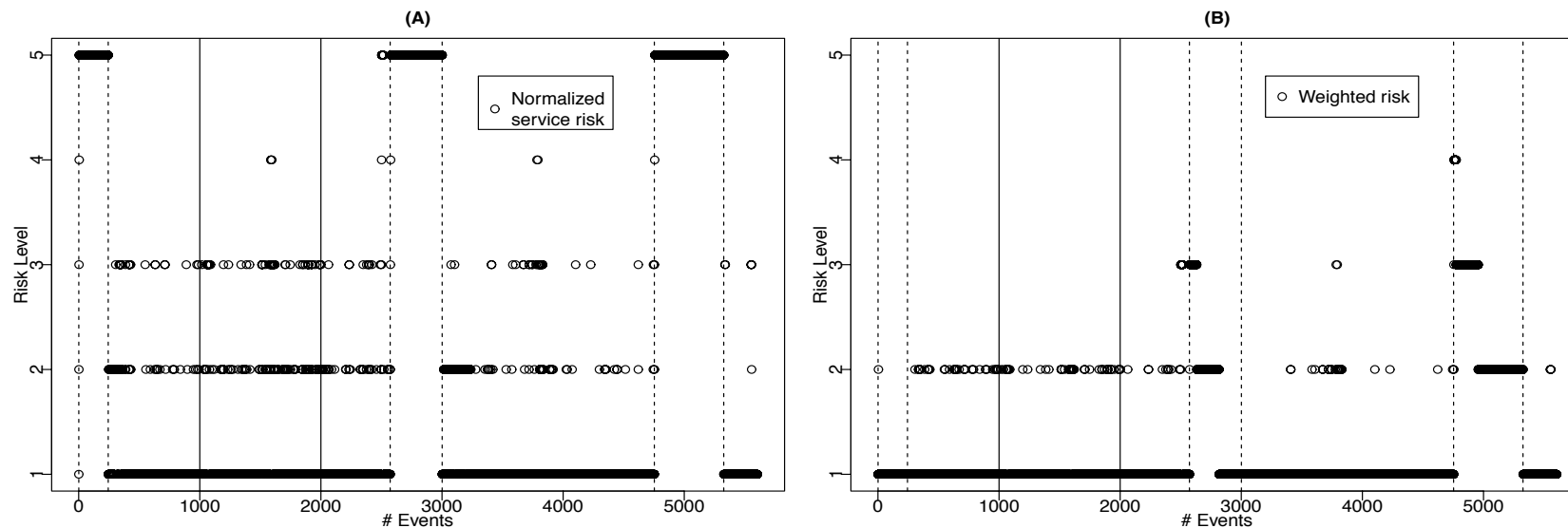
Results

- (A) The behaviour trust rapidly decreases where information is missing, growing again when the system behaviour goes back to a normal state.
 - Missing just a few values will have low influence in the confidence we have in the received risk alert.
- The measured risk is defined as 1 except for the interval [1000..2000] where there is a significant change between the measured service risk and the received risk.
 - This situation makes the risk alert trust indicator to decrease rapidly before starting to grow gradually.
 - It is also visible that when assuming high risk in periods where no information is received, the risk alert trust indicator also decreases due to the discrepancy between the values.
- (B) In this case, the expert has given a maximum weight of 80% to this risk. With the application of the model, the final weight (expert*trust) value will change gradually depending on the service trust indicator.



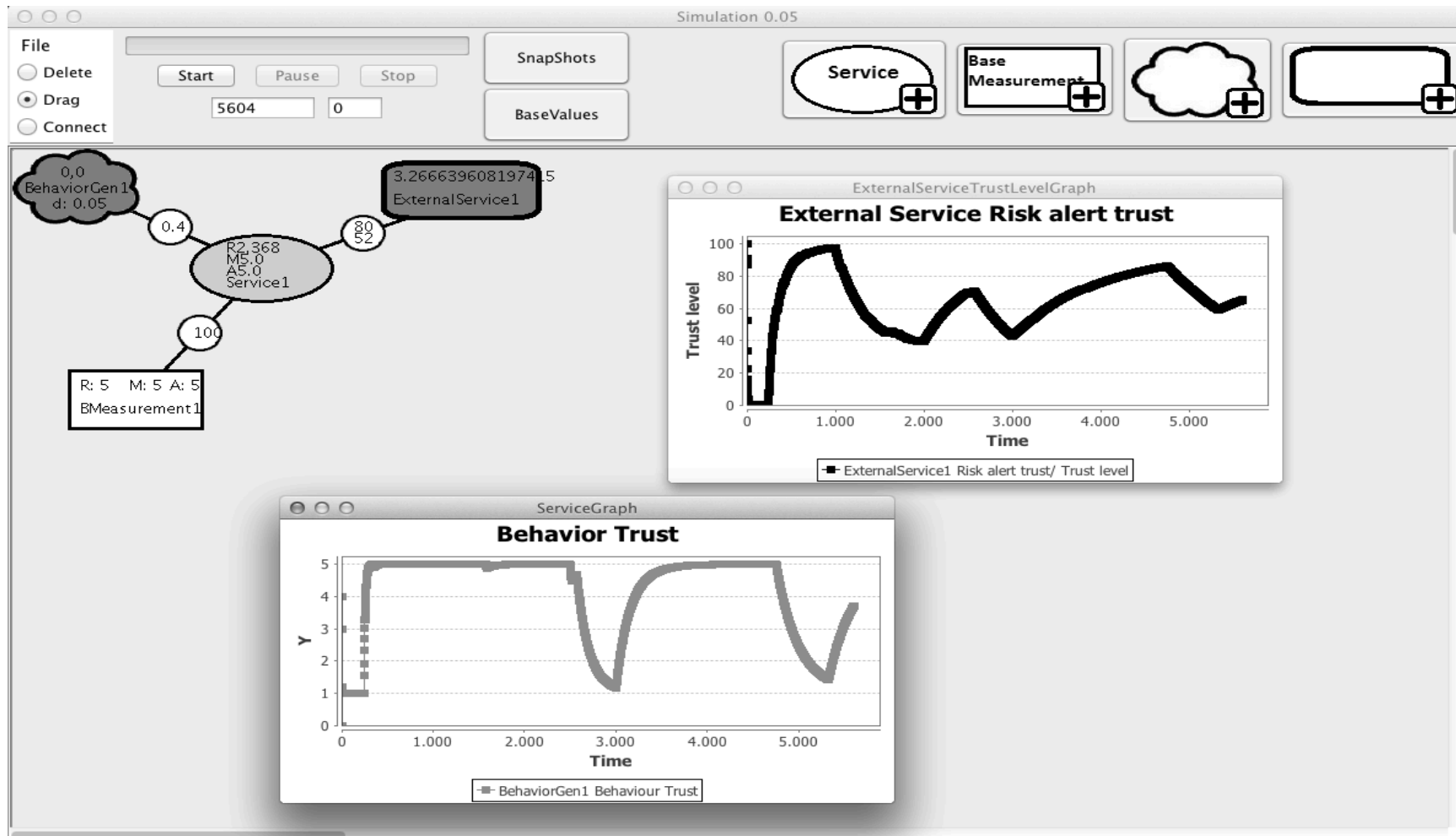
Results

- (A) - Received risk assuming growing values when information is missing.
- (B) - Contribution that both trust indicators (service trust) and the expert weight have on the final weighted risk level.
 - When the service trust gets lower, is given less importance to the received risk, maintaining a low risk level.
 - The weight represents the impact a received risk alert has to the aggregated risk of a service.
 - A low trust in the correctness of the received risk alerts, lowers its importance to the service.
 - Low trusted High-risk alerts will then represent only a low risk for the service.



(A) Normalized service risk for segment Luxembourg-Nancy; (B) Weighted service risk for segment Luxembourg-Nancy

Proof-of-concept implementation



Conclusions

- Able to answer questions like “how much can we trust in received risk alerts or in the CI behaviour?”.
- Trust and Reputation indicators can be incorporated in CI risk assessment as a means to improve its accuracy and its resilience to inconsistent information provided by peer CI / Services.
- MICIE System manager can act dynamically using trust and reputation indicators and reacting autonomously when those indicators change.
- A trust based approach was introduced to evaluate the correctness of information received from dependencies.
- Integrating the security model with the trust and reputation framework allow that:
 - Trust can be calculated from aggregated risk parameters and does not need to access actual infrastructure information.
 - The trust and reputation calculation is generalized and can be applied without modification to any CI that are using different security models.
- Validation
 - Inaccuracies in risk calculation can be captured using the proposed indicators
 - Real-world case study
 - The results are promising an in-line with previous simulation only results

Some References

- Caldeira, F., Monteiro, E., and Simões, P. (2010). Trust and reputation for information exchange in critical infrastructures. 5th Int. Conf. on Critical Infrastructures Information Security (CRITIS 2010), Athens, Greece.
- Caldeira, F., Monteiro, E., and Simões, P. (2010). Trust and reputation management for critical infrastructure protection. In Tenreiro de Magalhães, S., Jahankhani, H., and Hessami, A. G., editors, *Global Security, Safety, and Sustainability*, volume 92 of *Communications in Computer and Information Science*, pages 39–47. Springer Berlin Heidelberg.
- Caldeira, F., Monteiro, E., and Simoes, P. (2010). Trust and reputation management for critical infrastructure protection. *Int. J. Electronic Security and Digital Forensics*, 3, Number 3:187–203.
- Caldeira, F., Schaberreiter, T., Monteiro, E., Aubert, J., Simoes, P., and Khadraoui, D. (2011). Trust based interdependency weighting for on-line risk monitoring in interdependent critical infrastructures. 6th International Conference on Risks and Security of Internet and Systems (CRiSIS 2011), Timisoara, Romania.
- Caldeira, F., Schaberreiter, T., Varrette, S., Monteiro, E., Simoes, P., Bouvry, P., and Khadraoui, D. (2013 - To be published). Trust based interdependency weighting for on-line risk monitoring in interdependent critical infrastructures. *International Journal of Secure Software Engineering (IJSSE)*.
- Schaberreiter, T., Caldeira, F., Aubert, J., Monteiro, E., Khadraoui, D., and Simoes, P. (2011b). Assurance and trust indicators to evaluate accuracy of on-line risk in critical infrastructures. 6th Int. Conf. on Critical Infrastructures Information Security (CRITIS 2011), Lucerne, Switzerland.
- Schaberreiter, T., Aubert, J., and Khadraoui, D. (2011a). Critical infrastructure security modelling and rescu-monitor: A risk based critical infrastructure model. In *IST-Africa Conference Proceedings, 2011*, pages 1-8.

Questions and Comments

