

Trust and Reputation for Information Exchange in Critical Infrastructures

Filipe Caldeira^{1,2}, Edmundo Monteiro¹, and Paulo Simões¹

¹ CISUC - DEI, University of Coimbra, Coimbra, 3030-290, Portugal
{fmanuel, edmundo, psimoes}@dei.uc.pt

<http://www.dei.uc.pt>

² Polytechnic Institute of Viseu, Viseu, 3504-510, Portugal
<http://www.ipv.pt>

Abstract. *Today's Critical Infrastructures (CI) are highly interdependent in order to deliver their services with the required level of quality and availability. Information exchange among interdependent CI plays a major role in CI protection and risk prevention for interconnected CI where cascading effects might occur because of their interdependencies. This paper addresses the problem of the quality of information exchanged among interconnected CI and also the quality of the relationship in terms of trust and security. The use of trust and reputation indicators associated with the information exchange is the proposed solution.*

The proposed solution is being applied to information exchange among interconnected CI in scope of the European FP7 MICIE project, in order to improve information accuracy and to protect each CI from using inconsistent and non trustable information about critical events.

Key words: Critical Infrastructures, ICT security, Trust and Reputation Management

1 Introduction

The human society is becoming more and more dependent on services provided by Critical Infrastructures such as telecommunications, electricity and water supply. As stated by former USA President Bill Clinton, "Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security" [1]. Growing interest on this matter is clear from governments initiatives such as the Critical Infrastructure Protection (CIP) Program, started in 1998 by USA Administration, the European Programme for Critical Infrastructure Protection (EPCIP) in 2006 and the European initiative to establish a Critical Infrastructure Warning Information Network - CIWIN.

There are several models in the literature that provide the means to understand the interdependencies occurring among heterogeneous CI, and highlight the relevance of a system able to use these models to provide concrete instruments to CI owners in order to reduce the risk of service unprovisioning. This is

the main goal of MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) an FP7-ICT project aiming at the design and implementation of a real-time risk level dissemination and alerting system [2].

As ongoing research in this area is mainly focused on understanding interdependencies among CI, on the development of secure communication systems and on the use of received information for risk prediction models, we have identified the lack of mechanisms that allow reasoning on the trust level of received information and on the partnership behaviour. In this paper we present a framework that incorporates trust and reputation mechanisms on information exchange among Critical Infrastructures, describing the developed framework, presenting validation results and a discussion on foreseen results.

The rest of this paper is organised as follows. In Section 2 we discuss related work. The key components of the MICIE Alerting System (including the Secure Mediation Gateway) are presented in Section 3 as being the application scenario. Section 4 presents our approach to trust and information management. Section 5 presents validation work and Section 6 concludes the paper.

2 Related Work

In current research in ICT areas a growing interest in trust and reputation [3] can be found. In particular, current research is focusing on the development or refinement of trust models, usually developed for specific application areas like e-commerce web sites or more generally for the use in distributed environments where electronic transactions occur between persons and computer systems.

Among existing definitions for trust, we adopted a definition from [4] - “Trust: a subjective expectation an agent has about another’s future behaviour based on the history of their encounters.” Also we can refer that trust is the opinion of one entity (services, computer, person, etc.) about another single entity, while reputation is the community opinion about one entity.

Most of the research work in this area is focused on P2P systems [5–7], wireless sensor networks [8–10], on-line personal interactions, software agents, and generic models and formalisms for trust and reputation systems [11–14].

While most work integrates observed trust with reputation information received from partners, we are, for the moment, focusing our work on building trust information based on observed services and on deriving trust from evidences directly related with the entity whose trustworthiness is being evaluated. In this context, most of the work reviewed evaluates trust using the amount of positive or negative transaction experiences [11, 13, 15]. Our aim is to improve those models allowing that observed events can have a value in a defined range (e.g. [0..100]) for each transaction, introducing more detail about each transaction.

Some existing models give only a single value for trust. This value can be binary (trustee or not trustee) or can also be represented by more than two discrete values using either discrete or continuous numbers or labels. We consider that a trust model should, at least, give the user a value of trust in a defined

discrete range allowing them to be used as more precise indicators. Another important aspect related to trust models, with particular importance when we need to make decisions, is that they should provide measures to express uncertainty, reliability or confidence associated with a trust value. Some authors propose models that are able to express uncertainty [16–18].

Trust may be quantified and computed in many ways. In particular, several methods are proposed to derive trust from the collected evidence [14]. Authors propose simple probability [19], Fuzzy Approaches [20] or Bayesian networks [9]. There are substantial differences among the proposed methods, mainly related to the information used to evaluate trust, the use of reputation information, the use of parameters and the use of inactivity periods [7], etc.

There is also a growing interest on CI Protection, with recent projects such as CRUTIAL [21] and IRRIS [22] providing significant contributions to the field. However, to the best of our knowledge, none of these projects fully addresses the problem of real-time information exchange for on-line CI risk prediction (or the security issues associated with the related exchange of information).

In our work we will address the usage of trust and reputation indicators in the process of information exchange between interdependent CI. More specifically, we will follow the approach of [19, 7] (the use of ageing factors and time slots) on building trust from past experience and use a statistical approach to evaluate trust values. Since trust is evaluated as a simple probability, we can infer that trust value expresses the probability that an entity will behave as expected according to the trust definition we use.

3 Application Scenario

The MICIE project is in line with European developments in the Critical Infrastructure Protection (CIP) field, contributing in three main areas: the identification and modelling of interdependencies among CI; the development of risk models and risk prediction tools; and the development of a framework enabling secure and trustfully information sharing among CI [23]. The main goal of MICIE is to provide, in real time, each CI operator with a CI risk level, measuring the probability that, in the future, one CI can loose the capacity to provide or receive some services. Figure 1 describes the MICIE overall architecture[24].

The status of the CI components is collected, in real-time, in order to have all relevant information for the alerting system. The information is used by the Prediction Tool to assess the risk level of monitored services providing, in real-time, the status of the CI. Internal and external information is associated with the risk models used by the Prediction Tool, allowing the incorporation of interdependencies. Status information can be exchanged across partner CI using a Secure Mediation Gateway (SMGW), allowing CI to work in a fully cooperative distributed environment for risk prediction [24].

Regarding the sensitive nature of exchanged information, MICIE project has dedicated special attention to the security requirements such as confidentiality, integrity, availability, non repudiation and auditability/traceability. The usage

of trust and reputation indicators by the Prediction Tool and the SMGW Manager, contributes to improve information accuracy and to protect each CI from receiving and use inconsistent information.

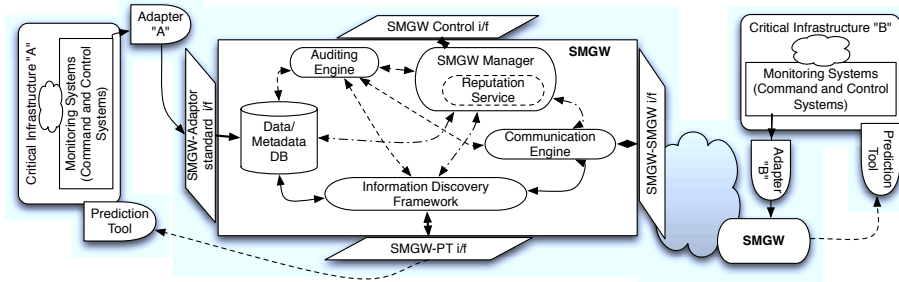


Fig. 1. MICIE overall system and SMGW architecture

The Trust and Reputation Service (TRS) evaluates information exchanged between CI in order to infer a trust level for each transaction. This service incorporates a level of trust on the data received from each partner, allowing that trust levels are incorporated in risk assessments as a mean to improve its accuracy and its resilience to inconsistent information. It will be possible, for instance, to give more weight to highly trusted data or to ignore data provided by low-trust partners.

The information needed to evaluate trust and reputation is gathered and evaluated from multiples sources, namely:

Analysis of past data provided by partner / service: The TRS will compare the risk estimates provided over time, for each service, against the current service levels, in order to infer the trustiness of future estimates.

Analysis of partner behaviour: Based on the knowledge gathered by the SMGW the TRS can analyse the partner behaviour in terms of ICT security. For instance, if the partner CI behaves abnormally (for example trying to access non-authorized data or using non-authorized credentials) the TRS should downgrade the level of trustiness associated with that partner CI as this could indicate that the partner is faulty or does not have good intentions.

Human factor: Operator perception about each partner/service. The operator can have information about each partner/service that can be incorporated in the Reputation Service.

Shared reputation services: The TRS can use the intelligence from multiple CI collectively to define the reputation of a specific partner based in each own partner trust in that partner. This aspect is under preliminary research and needs special attention on a way to maintain source confidentiality.

Trust evaluation can be achieved at two levels: Service Level, where each service subscribed to remote CI is evaluated, reflecting our trust in a particular service; At Global CI Level, where an indicator is added to each interconnected

CI. This indicator represents the reputation of that particular CI. Presented Trust indicators can be used to produce interdependency security indicators.

4 Trust and Reputation Service

The Trust and Reputation Service (TRS) framework presented in Figure 2, gathers needed information using two agents. The Risk Alerts Trust Agent that detects and calculate the risk alert event accuracy and the Behaviour Trust Agent used to receive and normalise behaviour events. Each agent sends events to the TRS Discovery Tool that computes in real-time the trust and reputation indicators. Computed indicators are provided to external entities, namely the CI SMGW manager and the CI Prediction Tool. A graphical interface provides the CI operator with an overall view about trust and reputation indicators.

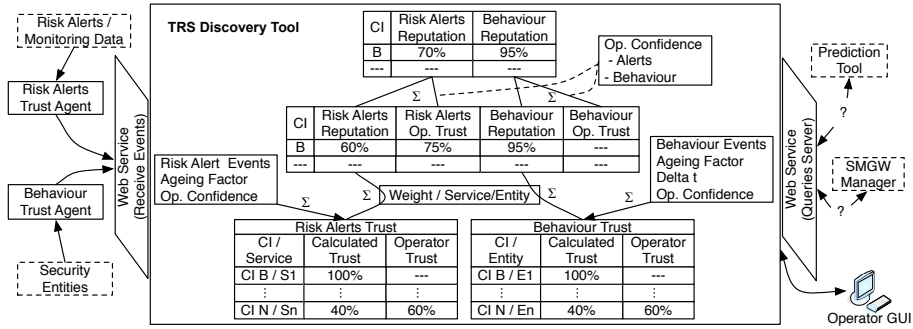


Fig. 2. Trust and Reputation Service (TRS)

4.1 TRS Agents

Risk Alerts Events - In interconnected CI scenarios, one CI can subscribe alert information regarding dependent services and use it to compute its own risk level. To be able to evaluate trust aspects related to receive risk alerts, the first goal is to define an accuracy value for each received risk alert. For this purpose, the concept of Risk Alert Event is introduced as one of the following situations: (1) A service decreases its Quality of Service (QoS) (this event ends when the QoS exceeds the threshold or, if an alert is received, the event ends when the alert is removed); (2) After the reception of a risk alert message.

The Risk Alerts Trust Agent is monitoring, in real-time, received risk alerts levels (Rl_t) and the current service levels (Sl_t) in order to detect events. Both Rl_t and Sl_t belong to the $[0..100]$ range.

For each event $A(Event_n)$, the accuracy is defined as the average of all comparisons made during the event (value T), between observed service level and

announced risk level (1). Function $f(Sl_t, Rl_t)$ is a discrete function so we need to use a sample rate for regarding the time factor. This sample rate can be different for each service and will depend on the information available on the system. One small sample rate yields more realist observations.

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

where $f(Sl_t, Rl_t) = |Sl_t - Rl_t|^\kappa$, $\kappa \in R^+$. The value k allows to penalise the larger differences or the small differences and should be assigned considering the degree of importance of each service. In this approach, the duration of an event is not considered as we are, for now, only focusing on the accuracy of the alert.

Behaviour Events - The SMGW provides the collection and analysis of data related to security aspects used to infer a trust indicator for each peer behaviour.

As data is gathered from heterogeneous sources and can be received in different formats, the information is normalised based on a security model that identifies relevant behaviour patterns. This system consists, basically, of tables mapping possible received values and trust indicators. For instance, it is possible to define that four authentication failures in less that a minute produce a confidence level of twenty on our security model as exemplified in Table 1. This model acts as an adaptor between heterogeneous sources and the trust estimator algorithm. By employing these adaptors it is possible to infer trust indicators, as all security events are quantified and can be used in a common calculation.

Table 1. Adaptor Table Example

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

The events used to evaluate trust on CI behaviour are all the interactions among peer CI in terms of ICT security (internal or external). For instance, the events can be Intrusion Detection Systems (IDS) alerts, failed connection attempts, attempts to read/write information without permission.

The Behaviour Trust Agent receives security alerts from the CI SMGW and, based on the defined security model, normalise the received information and send the event to the TRS Discovery Tool.

4.2 TRS Discovery Tool

The TRS Discovery Tool is responsible for the calculation, in real-time, of the trust and reputation indicators. For each type of indicator (risk alerts and behaviour trust), the TRS Discovery Tool maintains current and past indicators

in a database in order to provide them to the CI operator and to the SMGW Manager and Prediction Tool. In the next sections, the methodology used for trust evaluation is presented.

Trust and reputation indicators on received risk alerts - The trust that CI A has in alerts received for service X provided by CI B is represented by $T_{(A,B,X)}$ and can be calculated by the average of the accuracy of each past event between those two CI for that particular service.

As stated in previous works [7, 19], this solution has already identified weaknesses, for instance, one peer can behave correctly for a series of events and then capitalise gained trust to send false alarms. This problem occurs mainly due to the fact that the trust value will change very slowly as it depends equally on all the past transactions. This weakness can be minimised introducing the concept of ageing, using a discount factor D , to give more weight onto recent events. The ageing factor should always depend on the context. In our model the ageing factor needs to be defined on a per peer/service basis. In this context, $T'_{(A,B,X)}$ can be computed for the N th event as:

$$T'_{(A,B,X)} = \frac{(D * (N - 1) * T_{(A,B,X)}) + A(Event_N)}{D * (N - 1) + 1} . \quad (2)$$

D will be a value in the $[0..1]$ interval and a small value of D will raise the importance of the last events while a value of D near 1 will provide less ageing to oldest events. A large ageing factor will bring progressively the previous identified problems that lead us to introduce ageing. There are several approaches for choosing the ageing parameter D , for instance, a fixed value, make it decay exponentially using a $D = f(t) = x^t$ ($0 < x < 1, t = 1..N$) or, as presented in [19], observe the partner behaviour instability and focus on more recent alerts when observed behaviour reveals strong time correlation.

As discussed in section 3, a Human Factor is also considered in trust evaluation. This factor can be used in two ways: To initialise the trust indicator when there are no past observations available; by the operator reflecting his opinion and contribution to the trust calculations. In the second case the contribution weight needs to be specified. Considering the Human Factor, the final trust value for a specific CI/service is defined in (3).

The α factor is assigned by the CI Operator depending on the confidence he or she has in the opinion ($TO_{(A,B,X)}$). $T(final)_{(A,B,X)}$ represent the TRS confidence in alerts for each service individually taking into account also the CI operator perspective. In order to understand how services evolve over time, and to define a relation among them, a time value is associated with each $T(final)$.

$$T(final)_{(A,B,X)} = (1 - \alpha)(T_{(A,B,X)}) + \alpha(TO_{(A,B,X)}) , (0 < \alpha < 1) . \quad (3)$$

Using a weight factor for each service, the reputation of each CI can be evaluated using (4), where $GT'_{(A,B,t)}$ represents the reputation that CI A as

about CI B on time t . $GT_{(A,B)}$ represents the last evaluated indicator. W_i is the weight associated to service i provided by CI B. N is the number of evaluations. S represents the services that A receives from B and D is the ageing factor. Indicator in (4) should be evaluated every time a service indicator changes. $T(final)_{(A,B,i)}$ represents the last indicator calculated for service i .

$$GT'_{(A,B,t)} = \frac{(D * (N - 1) * GT_{(A,B)}) + \frac{\sum_{i=1}^S (T(final)_{(A,B,i)} * W_i)}{\sum_{i=1}^S W_i}}{D * (N - 1) + 1} . \quad (4)$$

The CI operator also contributes to the reputation indicator with a subjective value as described in (5) where θ is assigned by the CI operator and demonstrates the confidence concerning the subjective reputation value $TO_{A,B}$.

$$GT(final)_{(A,B,t)} = \theta(TO_{A,B}) + (1 - \theta)(GT_{(A,B)}) , (0 < \theta < 1) . \quad (5)$$

Trust and reputation indicators on peers behaviour - From the security monitoring systems, we expect to receive events when a misbehaviour is detected. This fact leads to a situation where almost only negative events are received. Considering only the events on a simple statistical approach, it is expected to have always a low value for the indicator, not representing the complete peer behaviour. To avoid this problem the concept of Inactivity was introduced.

The fact that events are not received during a given time period - Inactivity - indicates that, during this period, the peer CI behaviour is correct. In order to use inactivity periods, time is divided into a set of time slots [7], each slot with Δt duration. Inactivity in one slot means that the peer behaviour has the maximum value. If information is received during one slot, the slot value becomes the average of all events received during that slot. Trust values for each time slot are calculated using (6).

$$Event_{(Slot\ s)} = \begin{cases} 100, & \text{if } NEvents_{(Slot\ s)} = 0 \\ \frac{\sum_{i=1}^N Event_i}{N}, & \text{if } N = NEvents_{(Slot\ s)} > 0 \end{cases} \quad (6)$$

The Δt value needs to be defined for each security entity (behaviour monitoring systems, e.g. firewall, IDS, etc.) and can represent a period of only a few seconds to hours. A larger Δt implies slow changes on the trust indicator, being more evident when few events are received over time.

For the s time slot, the trust on entity E for CI B ($T'_{(E,B,s)}$) is calculated using (7) where D is the ageing factor, $T_{(E,B)}$ is the indicator evaluated for the slot $(s - 1)$ and $Event_{(Slot\ s)}$ is the event value of the slot s . The indicator and the time when evaluation occur are stored in the TRS database.

$$T'_{(E,B,s)} = \frac{(D * (s - 1) * T_{(E,B)}) + Event_{(Slot\ s)}}{D * (s - 1) + 1} . \quad (7)$$

Using (8) operator trust can be included. The θ factor is assigned by the CI operator representing the confidence on the subjective trust ($TO_{(E,B)}$) that he or she has on CI B behaviour concerning security entity E .

$$T(Final)_{(E,B)} = \theta(TO_{(E,B)}) + (1 - \theta)(T_{(E,B)}) , (0 < \theta < 1) . \quad (8)$$

As the event values are already normalised (has described in section 4.1), it is possible to evaluate an indicator encompassing all types of events. Using a weight factor for each entity, the behaviour reputation is known using (9), where $TBehaviour'_{(B,t)}$ represents the reputation of CI B behaviour on time t and W_i is the weight associated to security entity i . $TBehaviour'_{(B)}$ represents the last evaluated reputation indicator. Each weight must be defined along with the definition of the security model, representing the relevance of each entity in maintaining security. An ageing factor D is also included. In a similar way used in (8) it is possible to consider the operator information, including his confidence and reputation opinion related to the CI behaviour.

$$TBehaviour'_{(B,t)} = \frac{(D * (t - 1) * TBehaviour_{(B)}) + \frac{\sum_{i=1}^E (T(Final)(i) * W_i)}{\sum_{i=1}^E W_i}}{D * (t - 1) + 1} . \quad (9)$$

5 Validation

Trust in Received Risk Alerts - The events are generated using a normal distribution and the following parameters are used: penalisation factor $k = 2$; ageing factor $D = 0.3$; a threshold of 10%. The scenarios presented in Table 2 represent the following situations: (S1) The system behaves as expected with only small errors with the event accuracy always above 60% and mainly above 90%; (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; (S4) System in inaccurate.

Table 2. Simulation Scenario (% of events for each range of event accuracy values)

Scenarios	Event % of occurrence									
	[0-10]	[10-20]	[20-30]	[30-40]	[40-50]	[50-60]	[60-70]	[70-80]	[80-90]	[90-100]
S1	0	0	0	0	0	0	5	5	10	80
S2	0	0	0	0	10	10	10	10	20	40
S3	40	20	10	10	10	10	0	0	0	0
S4	80	10	5	5	0	0	0	0	0	0

Figure 3 presents the simulation results obtained from 1000 events of each defined scenario. It is clear that the trust indicator for each service will tend to the average of the generated events. It is also possible to see, that in worst

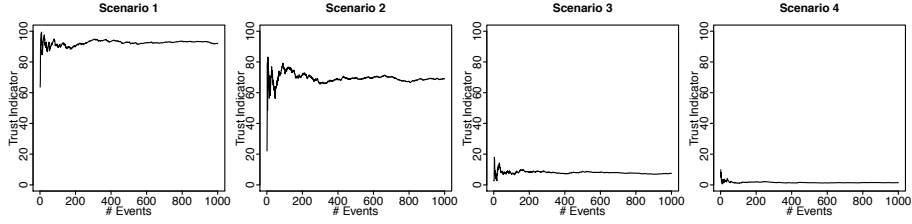


Fig. 3. Simulation for each defined scenario

scenarios (S3 and S4) the trust indicator drops below the average as those events are more penalised due to the chosen value of $k = 2$.

Figure 4 represents an attack or faulty component situation. Two different scenarios are presented in order to demonstrate that the framework behaves as expected, independently of the number of events. In Figures 4(A) and 4(B), the first, 2000 events (20 in Figure 4(B)) belong to S1. Next, received alerts become inaccurate (S4) during 100 (10 in Figure 4(B)) events returning to its normal behaviour after that (S1). It is visible that the trust indicator decreases rapidly and next starts to grow gradually. Figure 4(B) describes the use of the Human Factor. In this case the operator assigned a value of trust as being 90% and defined a contribution of 0.8 to final value. With this Human Factor, the operator can rapidly change the trust in a service.

In Figure 4(C) a simulation was performed using information observed from two services. Each service received an average of 5 events/hour from a mixture of scenarios one to four. The operator assigned a weight of 0.7 to service 2 and 0.3 to service 1. A value of $D = 1$ was used to calculate the Reputation indicator. In this simulation, when the service more important is becoming unreliable, then the CI reputation is decaying even when the other service is trusty.

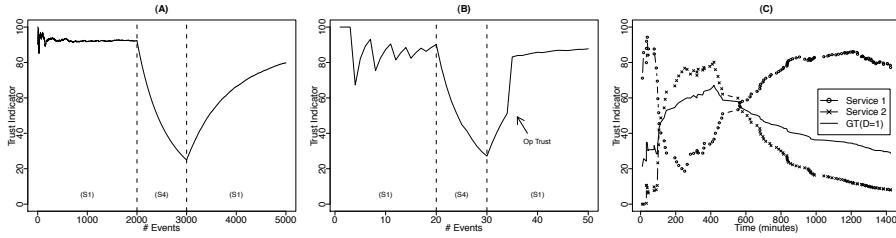


Fig. 4. Simulation - Trust on Received Alerts

Trust on Peers Behaviour - In order to validate behaviour trust indicators, the arrival times of the events are generated using an exponential distribution,

with an average of x per hour. Event values are generated from the scenarios defined in Table 2.

Figure 5 shows the results of four different simulations with common parameters $\Delta t = 10$, ageing $D = 0.05$ and simulation period=24 hours. Chosen ageing factor allows trust indicator to incorporate rapidly new situations.

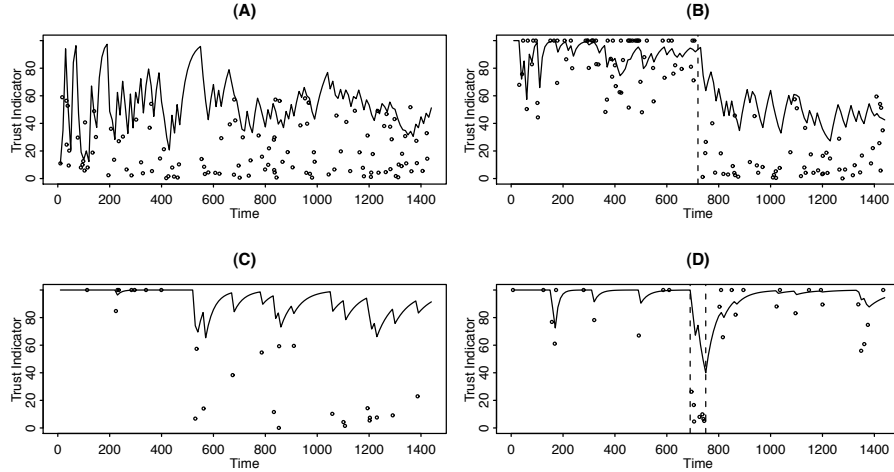


Fig. 5. Security service behaviour simulation

In Figure 5(A), events from scenario S3 arrive at a rate of 5/hour. As the arrival rate is small, the trust indicator starts with no defined tendency but will tend gradually to around 50%. This simulation also demonstrates that even with some incorrect behaviour, the indicator raises in the periods without events.

In the simulation presented in Figure 5(B), the first half of the events belongs to S2 and the last half belong to scenario S3. The event rate is 5/hour. In this simulation it is possible to observe that due to the ageing value each half of the simulation seems independent from the other demonstrating that the trust value rapidly incorporates changes in the peer behaviour.

The 3rd simulation (Figure 5(C)) has a rate of 1 event/hour in all the scenarios, namely, S1, S3 and S4. In this simulation, with few events, the trust indicator does not drop below 60% due to influence of the slots where the system is behaving well. This situation can also demonstrate how important the values defined for Δt are. In this case, a larger value of Δt would lead to a lower trust indicator. It is also important for the CI operator to know how to interpret the received indicators, in order to properly configure the system.

A situation of a possible attack or misbehaviour in a small period of time is demonstrated in Figure 5(D). In this case, during the first 11,5 hours, events from scenario 1 arrive with a rate of 1/hour. During a period of one hour, the

scenario changes to S1 (the worst scenario) with an event rate of 5/hour. In that moment, our trust indicator rapidly decays below 50% clearly indicating that something is wrong. With this indicator, the SMGW manager can act, for instance blocking the access from that CI or that Service. The last simulated hours represent the S2 at a rate of 1/hour. On S2 and with a lower event rate, the trust indicator clearly indicates the resolution of the past situation.

6 Conclusions

The MICIE system aims to provide, in real-time, risk levels measuring the probability that a CI will lose the capacity to provide services. This information is based on CI own data and on data received from peer CI. The proposed framework intends to enhance contributions expected from the MICIE project helping to answer questions like “how much can we trust in received risk alerts or in the peers 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. The proposed indicators are also used by the MICIE SMGW Manager, allowing a more dynamical and adaptable management, reacting autonomously when trust indicators change. For instance, if one peer trust decreases below a defined threshold, a new policy can be triggered and the SMGW stops accepting connections from that peer.

The Trust and Reputation Service prototype was developed allowing an easy integration with the MICIE SMGW. The TRS collects information via its Agents and computes in real-time the trust and reputation indicators, providing them to external entities. A graphical interface has been built providing the CI operator with an overall view about trust in all services/CI.

Results from the validation process are promising, demonstrating the ability to improve CI interoperation security. Authors expect to evaluate this proposal with MICIE project starting with a simple reference scenario that encompasses a small portion of an electricity distribution network and an interdependent telecommunications network [23]. Planned validation work for the MICIE project will also include more complex scenarios, provided by the Israel Electric Corporation and including multiple CI.

Acknowledgments. Work partially financed by FP7 ICT-SEC MICIE project [2] grant agreement no. 225353, and by the Portuguese Foundation for Science and Technology (SFRH/BD/35772/2007).

References

1. Clinton, W.J.: Presidential decision directive 63. (May 1998)
2. Micie: Micie - tool for systemic risk analysis and secure mediation of data exchanged across linked ci information infrastructures. FP7-ICT-SEC-2007.1.7 – 225353 – Annex I – “Description of Work” (2008)

3. Artz, D., Gil, Y.: A survey of trust in computer science and the semantic web. *Web Semantics: Science* (Jan 2007)
4. Mui, L., Mohtashemi, M.: A computational model of trust and reputation. 35th Hawaii International Conference on System Science (HICSS) (2002)
5. Chen, J., Lu, H., Bruda, S.: Analysis of feedbacks and ratings on trust merit for peer-to-peer systems. *E-Business and Information System Security, 2009. EBISS '09. International Conference on* (2009) 1 – 5
6. Chen, S., Zhang, Y., Yang, G.: Trust and reputation algorithms for unstructured p2p networks. *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on* (2009) 1 – 4
7. Spitz, S., Tuchelmann, Y.: A trust model considering the aspects of time. *Computer and Electrical Engineering, 2009. ICCEE '09.* **1** (2009) 550 – 554
8. Ganeriwal, S., Balzano, L., Srivastava, M.: Reputation-based framework for high integrity sensor networks. *Transactions on Sensor Networks (TOSN)* (2008)
9. Momani, M., Challa, S., Alhmouz, R.: Bnwsn: Bayesian network trust model for wireless sensor networks. *Communications, Computers and Applications, 2008. MIC-CCA 2008. Mosharaka International Conference on* (2008) 110 – 115
10. Zahariadis, T., Ladis, E., Leligou, H., Trakadas, P., Tselikis, C., Papadopoulos, K.: Trust models for sensor networks. *ELMAR, 2008. 50th International Symposium* **2** (Sep 2008) 511 – 514
11. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. *Decision Support Systems* **43**(2) (2007) 618–644
12. Malik, Z., Bouguettaya, A.: Reputation bootstrapping for trust establishment among web services. *Internet Computing, IEEE* **13**(1) (Jan 2009) 40 – 47
13. Ray, I., Ray, I., Chakraborty, S.: An interoperable context sensitive model of trust. *Journal of Intelligent Information Systems* (Jan 2009)
14. Sabater, J., Sierra, C.: Review on computational trust and reputation models. *Artificial Intelligence Review* (Jan 2005)
15. Hussain, F., Chang, E., Hussain, O.: State of the art review of the existing bayesian-network based approaches to trust and reputation computation. *Internet Monitoring and Protection, 2007. ICIMP 2007.* (2007) 26 – 26
16. Huynh, T., Jennings, N., Shadbolt, N.: An integrated trust and reputation model for open multi-agent systems. *Journal of Autonomous Agents and Multi-Agent Systems* (13 (2)) (Jan 2006) 119–154
17. Jøsang, A., Ismail, R.: The beta reputation system. *Proceedings of the 15th Bled Electronic Commerce Conference* (Jan 2002)
18. Teacy, W., Patel, J., Jennings, N., Luck, M.: Travos: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems* **12**(2) (2006) 183–198
19. Aime, M., Liroy, A.: Incremental trust: building trust from past experience. *World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (2005) 603– 608
20. Ludwig, S., Pulimi, V., Hnativ, A.: Fuzzy approach for the evaluation of trust and reputation of services. *Fuzzy Systems, 2009. FUZZ-IEEE 2009. IEEE International Conference on* (Aug 2009) 115 – 120
21. Crutial: Crutial project web site. <http://crutial.cesiricerca.it> (2008)
22. IRRIS: Irris project web site. <http://www.irris.org/> (2008)
23. Capodiecì, P., et al.: Improving resilience of interdependent critical infrastructures via an on-line alerting system. In: *COMPENG 2010.* (2010)
24. Caldeira, F., et al.: Secure mediation gateway architecture enabling the communication among critical infrastructures. In: *Future Network and Mobile Summit 2010 Conference.* (2010)