2007

Trust Indicator Modeling for a Reputation Service in Virtual Organizations

T. Winkler
Information Systems and Management, University of Karlsruhe, tw.itm@cbs.dk

J. Haller
SAP Research

H. Gimpel
Information Systems and Management, University of Karlsruhe

C. Weinhardt
Information Systems and Management, University of Karlsruhe

TRUST INDICATOR MODELING FOR A REPUTATION SERVICE IN VIRTUAL ORGANIZATIONS

Till J. Winkler[2], Jochen Haller[2], Henner Gimpel[1], Christof Weinhardt[1]

[1] Information Systems and Management, University of Karlsruhe

Englerstr. 14, 76131 Karlsruhe, Germany

{firstname.lastname}@iism.uni-karlsruhe.de

[2] SAP Research

Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany

{firstname.lastname}@sap.com

Abstract

In today's Internet economy, new business models emerge to respond to business opportunities that one organization alone can not exploit. Virtual organizations (VOs) are a prominent example for such models currently investigated in, e.g., collaborative engineering and aggregated services provisioning. The partner selection process is a problem that needs to be swiftly performed for a VO to become operational. In the global Internet community, previously unknown partners have to be considered for important business transactions, taking a risk in expecting partners to behave reliably. A reputation service can help to reduce this risk by supporting the (automated) decision process of system integrators inquiring about potential partner organizations. This paper presents a service-based reputation system rooting trust in an organization's inherent observable properties, called trust indicators. A taxonomy to classify trust indicators according to their semantic meaning is proposed. Furthermore, a stochastic trust indicator model based on distribution functions is presented, taking updates and trust indicator aggregation towards an overall reputation using Bayes theory into account as well.

Keywords: *Trust management, risk management, reputation systems, virtual organization, eOrganisation, stochastic modeling, Bayesian networks, design science research*

1 INTRODUCTION

Trust became an accredited aspect not only in social, but also in computer science. Virtual organizations (VOs) are one of the environments where trust is indispensable. A VO is a temporary coalition of otherwise independent organizations or individuals, collaborating to achieve a goal one party alone could not master. Typically, a VO follows a phased lifecycle consisting of identification, formation, operation, and dissolution phase (Strader et al. 1998). The strongest influence of trust becomes apparent in the identification phase, entailing the selection of suitable VO partners for defined business roles by a VO manager. A VO can be set in diverse, highly dynamic markets like high-tech industries (e.g. chip manufacturing) or collaborative engineering in, e.g., the aerospace or automotive industry. Since time to market and thus speed is essential, partner selection has to take previously unknown partners into account besides already well known ones (Haller 2006).

In this paper, we present a reputation service for VOs. The contribution of the paper is fourfold: it outlines (1) a set of requirements for trust management in VOs, (2) a taxonomy of objective trust indicators, (3) a model of a reputation service rooting reputation in such trust indicators, and (4) an implementation as proof-of-concept.

1.1 A VO Application Scenario from Collaborative Engineering

To analyze the requirements for a reputation service and its underlying trust management in detail, we present a motivating application scenario from collaborative engineering in the aerospace industry: An aerospace systems integrator won an airplane maintenance contract. A VO needs to be formed to analyze the design data, verify the design or report back flaws and missing details. The following description scopes the scenario to the initial VO phases, identification and formation, that entail the partner selection process. The systems integrator may act as the VO manager and triggers the process of VO formation, cycling through above mentioned phases (Robinson et al. 2005). Since time and speed are of essence while trying to exploit the cheapest of frequently changing service offerings, the VO manager identifies potentially required VO partners who meet the business requirements during the identification phase. The business roles' skill sets required for the VO – besides the VO manager – are those of an airplane design data analyst and a storage provider. Potential VO partners may be located anywhere in the world offering their services via standardized interfaces such as Grid services. A reputation system is maintained by a trusted third party (TTP) in contrast to distributed reputation systems e.g. in P2P architectures, offering reputation values for potential VO partners as a supporting service.

During the formation phase, the VO manager queries the reputation service for each potential partner's reputation. The reputation should be based on business criteria directly characterizing a partner organization's business reliability within the VO context. For instance "in time delivery of results" would be a valid business criterion for a design data analyst. The TTP providing the reputation based on observable data is hereby explicitly trusted.

Upon receipt of the requested set of reputation values, the VO manager decides on a set of VO partners and invites them to join the VO. This may be repeated until the required roles are filled with VO partners accepting the invitation. The formation phase concludes with the instantiation of the service choreography required to conduct the VO's engineering task. The operation phase then starts with the intended actual work and the partners provisioning their Grid services. After the operation phase, the VO manager's feedback about the past business transaction is a valuable piece of information for the TTP, to improve the reputation service for future service

1.2 Requirements for Trust Management

A more detailed version of this scenario was published in (Robinson et al. 2005). Having analyzed this scenario, we discovered that a VO oriented trust management approach for a reputation service has to meet the following set of requirements also following from general properties of trust:

Directed relationship (R1). Trust is a bidirectional relationship between a trustor and one or more trustees, but not inherently symmetric (Jøsang et al. 2005). If the VO manager (trustor) trusts a particular storage provider (trustee), an equal trust in the opposite direction does not automatically follow. Nevertheless mutual behavior can play a big role in trust relationships (Gambetta 1988). Furthermore, overlapping trust relationships do not necessarily extend to their transitive closure. If a VO manager trusts an analysis expert who in turn has a trust

relationship with a particular storage provider, it is not automatically implied that the VO manager also trusts the storage provider. Transitivity of trust is an ongoing research topic, e.g. in (Jøsang et al. 2006).

Subjective (R2). Trust is a subjective matter. It depends on a trustor's subjective evaluation of past experiences and it depends on the characteristics of the trustee (Jøsang 2001, Gambetta 1988). In this contribution, we focus on organizations enacting the roles of trustor and trustee.

Objective basis (R3). Although the evaluation of trust itself is subjective, its sources, which we will later introduce as trust indicators (TIs), can be objective (Tan 2003). Trust needs to be soundly rooted in an organization's characterizing properties, already implying that such roots are typically multi-facetted instead of relying on one single root of trust (Dellarocas et al. 2003). This approach supports especially a VO manager's decision making when participating in multiple VOs and therefore needing an objective basis for trust across different VO contexts.

Automated management (R4). Trust needs to be modeled by a formal approach in order to be usable in computer systems. Those can either act as decision support system or even decide autonomously. In this paper, we will focus on the latter, supporting executable business processes in a highly dynamic VO environment (Strader et al. 1998, Robinson et al. 2005, Jøsang et al.2005).

Comparable (R5). Trust should be comparable among different organizations in order to model them within a shared reputation service and support a fair decision process, e.g. when selecting among several potential business partners (Haller 2006).

Dynamic (R6). Trust develops and changes over time (Ismail et al. 2002). It may increase or decrease with further experience and it should decay over time (Ruohomaa et al. 2005). A trust model needs to dynamically adapt to such changes.

Besides these trust-specific requirements, generic requirements for information systems are obvious; these are, for example, availability (of the system itself and required data sources), correctness, and efficiency.

1.3 Outline

The remainder of the paper is structured as follows: Section 2 reviews related work and in Section 3 we present a trust model as core of the reputation service. The model has three main building blocks: Firstly, a taxonomy of trust indicators and their respective attributes, secondly the update mechanisms for the trust indicators once new data is available and thirdly the aggregation concept taking objective and subjective trust information into account. As proof-of-concept, Section 3 also describes an implementation of the reputation service. Section 4 concludes and enumerates future work.

2 RELATED WORK

Trust is a complex sociological phenomenon. The purpose of this section is to review notions of trust and related concepts that are relevant for automated trust management in VOs. For a complete overview of all facets of trust we recommend related surveys from (Grandison et al. 2000; Ruohomaa et al. 2005; Jøsang et al. 2004).

In the context of a VO, we define trust as the subjective probability by which the trustor expects the trustee to perform actions captured in a role specification within the context of a VO. This definition relates to work from (Gambetta 1988) and (Jøsang et al. 2004). It would harm the entire VO if one partner organization, e.g. the storage provider, would not perform as expected.

In the area of information technology, the term trust management was invented by (Blaze et al. 1996) who define the term "trust management (problem)" as the collective study of security policies, security credentials and trust relationships. This purely technical perspective resulted in a system simply providing access control for distributed environments. Following this groundbreaking publication, a multitude of trust management approaches were developed and published in parallel. The most recent and successful ones are surveyed in (Jøsang et al. 2004). On the higher level of business to consumer e-commerce, a model of trust relevant, directly observable factors that for instance characterize online vendors is presented by (Egger 2003). While the general approach to root trust in observable indicators is comparable to our work, the application domain and hence the relevant indicators are different.

Reputation is a known concept in many disciplines, equally broad as and closely related to trust (Mui et al. 2002). Reputation can be seen as the general opinion of a group towards a person, another group of people or an organization. Broken down to the field of trust management in VOs, reputation can be defined as a perception a VO has about the intentions and norms of another organization. This perception develops through past actions and through objective indicators. A recommendation then is an attempt to communicate reputation from one party to another. A general reputation can thereby be mapped to an individual binary (directed) trust relationship.

Risk commonly refers to a potential harm that may arise from some present process or from some future event. At this point, the differentiation among risk (i.e. known probabilities) and uncertainty (i.e. unknown probabilities) is irrelevant and hence omitted. There is an inherent risk when collaborating in a VO. Risk and trust are intrinsically related (Luhmann 1988). Obviously, if risk did not exist, there would be no need for trust, as stated in (English et al. 2004).

Risk management is the process of identifying, measuring, and controlling risk as well as developing strategies to manage or reduce it. Risk management frameworks can be used for the exact assessment of input risk levels and the transfer of related concepts in general (Grandison et al. 2000). Unlike trust modeling, risk modeling and risk management are established fields in economic research and practice, covering many different domains where risks emerge. Similar to our approach, such risk management frameworks assess risk based on risk indicators that map to well established key performance indicators (KPIs). Some risk indicators behave stochastically and have an impact on trust intersecting with our set of proposed TIs.

Presumed that we have a formalized basis on how to relate risk to trust, we can derive trust measures from the indicators that risk management already provides.

3 MODEL PROPOSITION

3.1 A Taxonomy of Trust Indicators

While most of the previously proposed reputation systems assume given data, rely only on externalized, subjective sources such as feedback or simple binary measures, an improved system roots trust in the inherent properties of a trustee's organization. Adapting the concept of risk indicators from risk management, we define a trust indicator (TI) to be a regular measurement based on data that has an impact on trust in a certain area of the trustee's organization. In the following, we will identify these areas and subordinate them in a top-down approach to a reasonable classification.

3.1.1 Taxonomy

Since trust is inherently related to risk, existing operational risk categories play a big role for TIs. On an abstract level, operational risk is commonly divided to derive from staff, technology, process and environment (King 2001). Technology and process refers to risks surging in the operational processes of a firm and thus **operational TIs**. Herein a sub classification according to the functional units of the firm seems applicable. Staff points to more hidden risks caused by human behavior. These can occur on different decision levels, strategic, managerial or simply on employee level. This class is denoted as **organizational TIs**.

External TIs refer to influences and risks that stem from sources external to the organization. These can be caused by other parties like customers or competitors, the legislation but also non-entities like the general economic environment, labor and factor markets or natural resources and catastrophes. Further also **financial TIs** impact the reliability of an organization that becomes apparent in case of a firm's financial bankruptcy. Financial information can be based on balance sheet data or from non-direct measures like stock market prices. Popular indicators for performance measuring are for example the cash flow quote, economic value added, earnings per share ratio etc. (Schultze 2003).

At last, trust related information may also stem from a third party. Various commercial information providers have tackled the task of providing meaningful ratings about potential business entities. Prominent examples are financial stock ratings from Standard & Poors and Moodys as well as the company database by Dun&Bradstreet amongst others providing extensive information about credit-worthiness of organizations. This information as well as information from other instances of the same type of reputation service, can be integrated to a trust system as a **third party TI** carrying condensed reputation information content, cp. (Tan 2003).

Figure 1 depicts the TI taxonomy, summarizing our classification effort. The subcategories specialize the top-level classes and are drawn according to a bottom-up approach that collected and clustered a total number of 146 and 56 verifiably unique different key indicators (Winkler 2006) into several classes described in the relevant literature (Schultze 2003; Arndt 1985) and related areas like Financial Risk (Hager 2004; Allen 2003), Operational Risk (King 2001; Cruz 2002), and particularly Supply Chain Risk Management (Brindley 2004; Chan 2003) in parallel to the overall top-down classification.

The taxonomy represents an extensible reference framework for trust management in VOs. For an implementation of the model in a specific setting, domain specific indicators need to be defined within these categories. Of course, newly discovered TIs can be added to the taxonomy as can additional (sub-) categories. The following section will show that adding a TI encompasses defining its unique identifier and implementing a set of attributes. Trust indicators then can be aggregated according to the categories, whereas the arrows in the diagram show the specific dependencies.

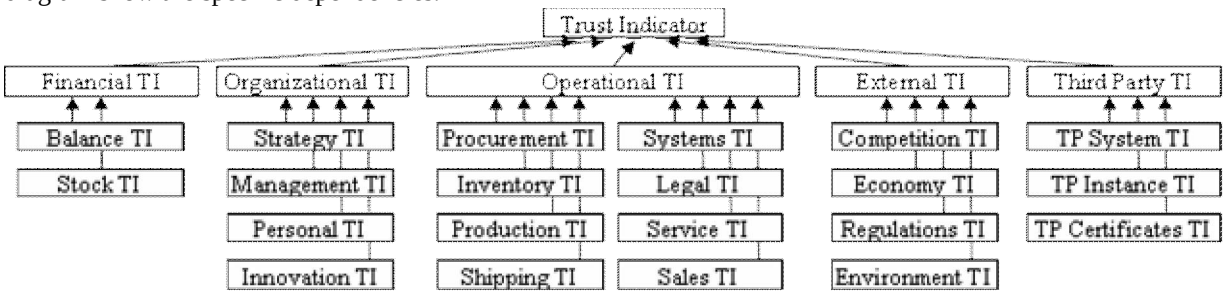

Figure 1: Taxonomy of Trust Indicators

3.1.2 Examples for Trust Indicators

As mentioned before, trust indicators have to meet the set of requirements implied by 1.2, namely availability, comparability and automation. TI modeling hereby has to cope with incomplete data since it can in general not be assumed that complete datasets are available at any given time for each TI. Furthermore, similar to risk management, a decision maker such as a VO manager wants to predict a potential business partner's behavior based on his TI model. The list of possible TIs has to be filtered according to these criteria that motivated us to pursue a stochastic TI model based on density functions.

The specific trust indicators to be used depend on the application domain of the reputation service. In the context of our collaborative engineering scenario, the following trust indicators are considered most applicable. Due to the complexity of trust, the TIs that contain aggregated information are preferred.

The Cash flow (CF) is a measure for the actual cash generated by a business. The ***cash flow quote*** is the quotient of CF and turnover and is used to make the CFs of different organizations comparable. Cash flow can also be seen as a measure for financial trustworthiness. Adopting (Hayne 1999) we model the likelihood for the cash flow quote as a lognormal distribution.

In general, VO networks operate on a global scale. In risk literature country risk is understood as consequences caused by the economic, political and social environment (Lehrbass 1999). A widely used daily measure of country risk is the ***country bond spread***, i.e. the yields on bonds issued by a country (Damodaran 2003). This measure also incorporates currency and interest volatility, whereas a higher spread likewise reflects a higher risk. Herein we find an appropriate and highly aggregated indicator for external influences. Empirical studies show, that country bond rates are best modeled by fat-tailed distributions like the student-distribution (Romeike 2005).

There are only a few quantitative measures that express organizational trust. Among the simplest and most popular ones is the ***employee fluctuation rate***, indicating the employee satisfaction and organizational climate. The members of an organization know best about the overall situation of their entity. In (Teitelbaum et al. 2005) a statistical study is conducted, finding that member fluctuation on a longer term follows a Pareto distribution.

Availability of the technological systems is a common measure of operational risk and, thus, system downtime can serve as a TI (Cruz 2002). For a storage provider in a VO this availability even turns to be crucial for offering his service. Several studies report on statistical modeling of ***system downtime*** in general (Williams 1994). Due to the possibilities for parameterization, a gamma distribution is suggested to be most flexible in modeling this TI.

3.2 Attributes and Updates of Indicators

The previous section outlined a general taxonomy for trust indicators and pointed out examples. In this section we model TIs in more detail. Every TI comes with a set of attributes that details its usage within the model. These attributes are:

Name N. Every TI is uniquely identified by a name *N*.

Domain D. A TI can be based on observations of a continuous or discrete variable *x*. The possible values of *x* are the domain of the TI. In general, x can be multi-dimensional and is then represented as a component vector.

States S. The TI measure is discretized by defining certain bounds $x_b \in D$ dividing the TI domain into intervals, so-called states *S*. The states consolidate discrete and continuous measures for a common random variable handling.

Update time period Δt_{upd}**.** Trust information is likely to arrive at different times. The attribute Δt_{upd} defines a fixed time grid telling the reputation service, how often to update a TI.

Observation time period Δt_{obs}**.** The time period Δt_{obs} defines a maximal time window to look into the past. Beyond that, observations are regarded to carry no more significance.

Time weighting function ω**.** Among *n* observations x_i at times t_i, $i \in \{1,...,n\}$ within the time window, old ones are less likely to carry significance for future TI development. Each TI incorporates a monotonically increasing weighting function $\omega(t)>0$ that implements forgetting of older observations putting emphasis on newer ones.

Empirical distribution E. Within the observation time period, historical data *X* is assigned to states and counted to an empirical frequency distribution *E*(*X*), taking the weighting function into account. *E*(*X*) is primarily providing information about the past development of that particular TI.

Likelihood distribution L. Further on, every TI observation, due to its stochastic nature, follows a certain statistical distribution. *L* reflects the likelihood $L(\theta|X)=P(X|\theta)$, that θ is the "real" parameter underlying the distribution of the TI, given a set of observations *X*. Its distribution assumption itself has to be derived from statistical analysis.

Trust preference mapping π**.** In order to judge the level of trustworthiness displayed by a TI, we define an ordinal scale 1 to $p_{\max}$, where 1 represents the lowest and $p_{\max}$ the highest level of trust indicated by the TI, for example with $p_{\max}$=5 {1:very low trustworthiness, 2:low trustworthiness, ... , 5:very high trustworthiness}. To compare TIs, the scale is the same for all TIs. π defines a function $\pi : S \longrightarrow \{1,..., p_{\max}\}$ mapping the states *S* to the different levels of trust indicated by them. This mapping enables an expert to incorporate his knowledge on the particular TI domain.

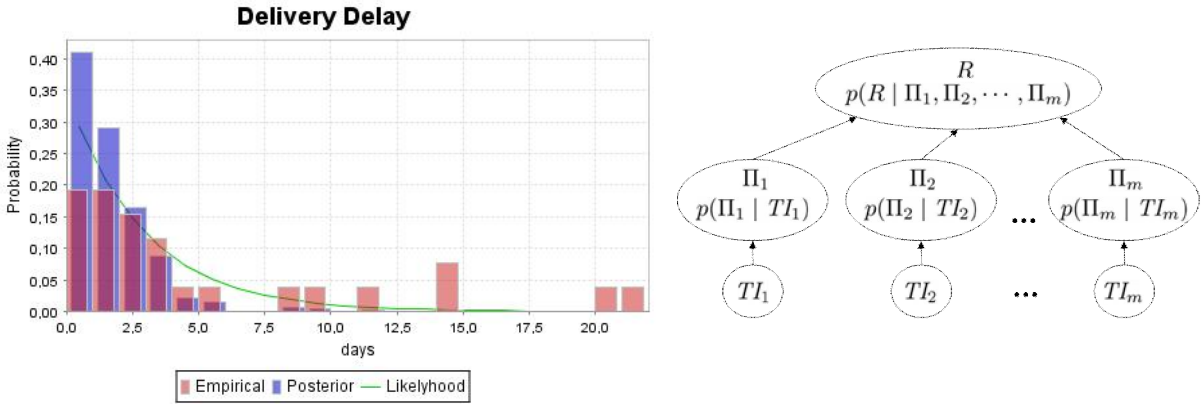

Figure 2: Trust Indicator Updating and Bayes Network Topology

For the update of each TI we propose a Bayesian update with observed data over time, e.g. explained in (Press 2003). According to Bayesian theory the prior distribution $P(\theta)$ represents an uncertainty distribution of the prior

belief about the real value θ of the trust indicator. In our case the prior can be derived from the empirical distribution $E(X)$ by calculating the relative frequency distribution $P(X)=\frac{1}{n}E(X)$. The posterior $P(\theta|X)$ represents the best knowledge of θ after having observed new data X discretized over states S, and is connected to the prior function with the likelihood $L=P(X|\theta)$ via the Bayes' Theorem. This way a mathematically justified "fit" between epistemic knowledge represented by the empirical distribution and incorporated assumptions represented by the likelihood function is achieved. The left hand side of Figure 2 provides an example with the TI "Delivery Delay".

3.3 Trust Indicator Aggregation

Up to now, we considered single TIs. In order to derive an overall reputation value, these TIs have to be aggregated. For the aggregation of m different Trust Indicators $TI_k, k \in \{1,...,m\}$ to a reputation value R, we propose a Bayesian Network (BN) with a tree topology of depth three (see right hand side of Figure 2):

1. The input layer entails the information leaf nodes TI_k maintaining the trust indicator state distributions
2. The middle layer holds mediating variables Π_k incorporating the TI's trust mapping π_k
3. The output layer only holds a single target variable R representing the resulting reputation distribution in the root node

The BN is used to infer a reputation R from TI states and to learn and forget these dependencies. It can also be utilized to incorporate structural learning of the dependencies among the TIs, see (Jensen 2001) for a detailed introduction to BNs. The BN tree structure is inspired from related problem structures in risk management. Established guidelines for BN modeling are still a research topic (Fenton et al. 2004). In our case, the tree shaped BN structure persists, but the choice of a TI set for a particular application setting is the design time task of a domain expert that can be modified at runtime.

As any other modeling method, the BN's advantage depends on the amount of knowledge that serves as modeling input plus the data. Therefore they are generally criticized for the subjectivity of the information they incorporate (Adusei-Poku 2005). In trust management, however, the use of subjective data is generally accepted, due to the inherent subjectivity of trust itself, which turns this property into an advantage.

3.3.1 Bootstrapping

For bootstrapping the BN with a first update, i.e. in case there is no epistemic knowledge available, there are basically two alternatives: Bayesian theory proposes to set the empirical distribution to uniformly distributed values over the whole TI domain in order to represent the given uncertainty. The other possibility is to consult the missing fields from a model of a similar organization in the same trust context and copy those values, incorporating a certain belief discount.

We currently support both options: the first automatically, the second currently involves a manual BN migration. This means in practice that each node's Conditional Probabilities Table (CPT) has to be set. The *TI* nodes each maintain a conditional probability depending on the random variables of their child nodes and are (initially) not dependent on other nodes, thus their respective CPT is simply set to the unconditional prior distribution P(θ) over the states *S*, representing the empirical belief about the indicator distribution.

The mapping nodes Π_k have $p_{\max}$ states, representing the trust preference scale. Their CPT deterministically incorporates the mapping from the TI states *S* to the preference $\pi(S)=p$ and are defined by

$$CPT_{\Pi} = P(\Pi = p \mid TI = S_s) = \begin{cases} 1, \ \pi(s) = p \\ 0, \ else \end{cases}$$

The aggregation of the mapping nodes is represented by the CPT of the reputation node. Obviously a higher TI value on the preference scale also refers to a higher reputation. Say we divide the domain of *R*, $dom(R)=[0,1]$ into $p_{\max}$ equidistant intervals R_r, $r \in \{1,..., p_{\max}\}$ likewise representing the states of *R*, we define a conditional

probability function $P(R = R_r \mid \Pi = p)$ that has its maximum, where *r*=*p*, that means where *R* falls in the preference interval given by Π.

As a first simple approach we propose a linear conditional probability function $P(R \mid \Pi)$, normalized by its sum in the denominator:

$$P(R \mid \Pi) = P(R = R_r \mid \Pi = p) = \frac{p_{\max} - \mid p - r \mid}{\sum_{r=1}^{p_{\max}} p_{\max} - \mid p - r \mid}$$

For the purpose of bootstrapping we assume (initial) stochastic independence between the TIs and aggregate the *m* trust mapping nodes Π_k by defining the reputation CPT with $p_{\max}^{(m+1)}$ entries as the joint conditional probability function of the single conditional probability functions $P(R \mid \Pi_k)$:

$$CPT_R = P(R = R_r \mid \Pi_1 = p_1, \ldots, \Pi_m = p_m) = \frac{\prod_{k=1}^{m} P(R \mid \Pi_k)}{\sum_{r=1}^{p_{\max}} \prod_{k=1}^{m} P(R \mid \Pi_k)}$$

3.3.2 Reputation Inference

To inquire about the reliability of a certain trustee, the reputation service infers a probability distribution *P*(*R*) (depicted as the lighter belief bars in Figure 3) from the BN by setting the evidence of the TIs given by its posterior function $P(TI_k) = P(\theta_k \mid X_k)$. The evidence is propagated through the trust mapping nodes Π to the root node R.

In order to create more intuitive measures for the resulting distribution of *R*, one can meter the level of reputation by any measure of central tendency, most commonly the expectation value or the median. The uncertainty included in this reputation prediction is expressed by any variability measure, e.g. the variance or a certain quantile. For further illustration, the 5% quantiles are drawn in Figure 3 which shows a typical reputation distribution from Figure 2 (right) after having bootstrapped CPT_R.

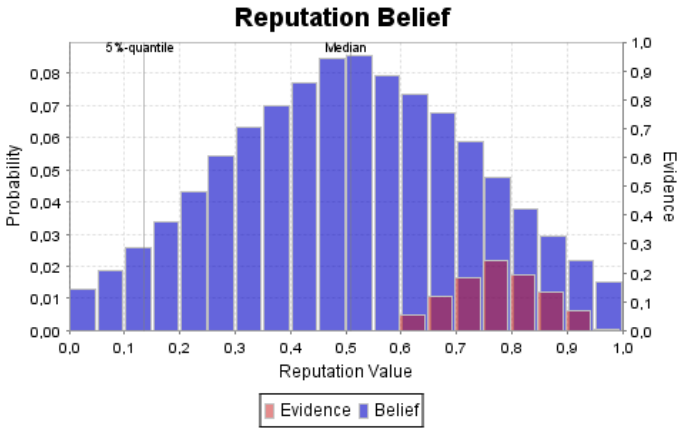

Figure 3: Reputation Belief with Feedback Evidence

3.3.3 Learning and Forgetting

The BN learns via actions, i.e. if a trustee has performed the action *a* at time t_a, the trustor subsequently has the possibility to feed back his experience, represented by a single reputation value $r_a \in [0,1]$. In contrast to the

objective TI data which is raised by the service, the feedback r_a from the trustor represents a highly subjective measure.

r_a directly updates the root's R conditional distribution. Regarding the evidence $P(TI_k)$ of the TIs at t_a, the trust mapping nodes Π_k also show a particular evident probability distribution $P(\Pi_k)$. Based on r_a the entries in CPT_R that refer to the evident states in $P(\Pi_e)$ are strengthened. In Figure 3, the effect of the feedback is depicted by the smaller, darker evidence bars in the graph's lower right corner. The positive feedback shifts the mass of the belief bars slightly to the area of higher reputation. This way for the next request under similar conditions in the TI evidence, the resulting reputation value will be closer to the previous value r_a was referring to at time t_a .

The correlations guarded in CPT_R also have to be blurred from time to time, to represent planned forgetting and to preclude overfitting of the data. Forgetting in BNs, also often referred to as softening or fading, basically abbreviates functions that approximate the probability distributions to a uniform distribution. The maximum observation time attribute Δt_{obs} provides a basis for initiating this procedure.

3.4 Evaluation

The two major paradigms in Information Systems research are behavioral science and design science (Hevner et al. 2004). Our study clearly falls in the design science category and the question on how to evaluate the designed artifact, i.e. our model of a reputation system rooting trust in an organization's inherent observable properties, arises. In general there are numerous possibilities how to evaluate an artifact: case studies, field studies, controlled experiments, simulations. In this work, the argument for the utility, quality, and efficacy of our approach bases on four basic evaluation methods: scenario, prototypical implementation, informed argument, and architectural analysis (cf. Hevner et al. 2004).

3.4.1 Scenario

The rational behind using scenarios for evaluation of design artifacts in Information Systems is that scenarios can demonstrate the utility of an artifact. To this end we presented a VO application scenario from collaborative engineering in Section 1.1. This scenario points out clearly the necessity of a reputation service during the formation phase of a VO to support the VO manager.

3.4.2 Prototypical implementation

As a proof-of-concept, we prototypically implemented the model outlined so far for our application scenario. Artifact instantiation in general and a prototypical implementation in particular demonstrate feasibility of the designed artifact. The construction of the prototype that automates trust management in VOs demonstrates that the process can, in fact, be automated – it provides proof by construction (Nunamaker 1991; Hevner et al. 2004).

For the implementation we chose a centralized architecture deployed as three web services. The reputation service can be easily integrated with an existing VO framework, e.g. hosted by a TTP, as an additional supporting service consulted during the partner selection process. Furthermore, a centralized topology fits the central role of a VO manager better in such an environment (Robinson et al. 2005). The prototype is implemented as Java web services using Axis as a SOAP Engine and deployed into an Apache Tomcat web container. For the implementation of the Bayesian Network (BN) operating on the aggregator service we utilize the Netica API by Norsys[1] as the BN engine.

[1]Netica and the Netica API are available as a free limited version at http://www.norsys.com

3.4.3 Informed argument

The basic concept of informed arguments is to use information from relevant related research to build an argument for the artifact. To this end, we derived a set of six requirements for trust management systems in Section 1.2 – these requirements build on the relevant research in the domain of trust management and reputation. In the following, we argue that the approach presented so far satisfies all these requirements.

The service evaluates reputation on basis of single requests and differentiates trustor and trustee. Thus, the subjectivity of a directed trust relationship is respected (R1 and R2). Trust is rooted in observable, objective and organization inherent trust indicators (R3). The prototypical implementation of our model proofs that automation based on a Service Oriented Architecture (SOA) is feasible (R4), though a scenario driven model evaluation is still subject of future work. The model considers a domain-specific set of several trust indicators that are aggregated to a single reputation. The prototype integrates feedback data as well as data from enterprise business software and from commercial information providers. In case normalization or transformation of data is necessary for comparability, a domain expert can model this via the domain and state attributes of each TI hereby enriching the model with expert knowledge (R5). The dynamics of trust are addressed by several features of our model: first of all, reputation values are request specific and base on up to date information. Every TI comes with an observation period, an update time period and a time weighting function to account for changes over time (R6). The approach allows integrating new trustees on the fly by two techniques: on the one hand, trust bases on objective characteristics of the newbie and does not depend on a history of transactions and experience. On the other hand, we propose specific bootstrapping methods to get the service working even in case data is missing.

3.4.4 Architectural analysis

In an architectural analysis one studies the fit of an artifact into the technical architecture of the overall information system. For the reputation management system, the most important aspect of integration is whether the system can be combined with existing business applications that provide the necessary data. The prototypical implementation as three loosely coupled web services shows general interoperability with existing information systems by having well defined interfaces and message types. Referring to the storage provider in our scenario we assumed a fictitious emerging mid-sized technology company located in Brazil. Data for this entity's *delivery delay* and *employee fluctuation* are, for example, retrieved from the infocubes of an SAP Business Warehouse database.[2] This shows the interoperability of our reputation service with standard software tools and data sources. *Cash flow quotes* are approximated based on the study by (Hayne 1999). The data for *country risk* is assembled by calculating the bond yields from Brazilian DL-Bond prices with different maturity taken from Onvista.[3] This exemplifies the connection to commercial information providers. *System downtime* data however is simulated by applying a gamma distribution, as proposed by (Williams 1994).

4 CONCLUSIONS AND FUTURE WORK

In this paper, we presented a trust management approach that stochastically models so-called organization inherent trust indicators serving as root of trust. The presented taxonomy classifies a set of trust indicators along with their attributes that are required for stochastic modeling. Trust is used as support in business oriented decision processes, e.g. for the partner selection in VOs. We achieve that goal by presenting a model on aggregating trust indicator values to reputation using Bayesian networks. The model is implemented in a software prototype. Revisiting our initial list of reputation service requirements, we showed that our approach caters for all of them. Overall the evaluation methods employed in this design research are scenario, prototypical implementation, informed argument, and architectural analysis.

Besides the virtues of the presented trust indicator model, there are, obviously, drawbacks. The two most sever ones are domain knowledge and data availability. The model does not crucially depend on domain specific

[2]http://www.sap.com/

[3]http://www.onvista.de/

knowledge, but it greatly improves performance and reliability of reputation values. With the prototype, we showed that different data sources can be integrated. However, this depends on whether information providers or companies themselves grant access to the data, a difficult task, but not impossible to overcome. As stated in the beginning, we focused on reputation systems supporting VOs that are hosted by a TTP. In such environments, there is precedence in existing business relationships of otherwise sovereign organizations allowing a TTP controlled access to confidential data in order to enter new, profitable business collaborations. Dun & Bradstreet[4] is such an example, compiling financial reports and credit statements based on such confidential data without disclosing details. Another business relationship granting access to required data sources is the case of an enterprise application hosting provider. In a hosting environment, such a provider has access to a multitude of application instances hosted for different customers with associated business data that can be used for a reputation – or other web-based decision support system delivering business intelligence. Of course, an explicit contractual agreement with each customer is required to use their data to provide an added value service. For the latter, Salesforce.com[5] is a hosting company example offering Customer Relationship Management services with added business analytics based on data aggregated from a variety of customers. Another concern is the maintenance of the Bayesian network. Each TI update requires the update of the entire net in terms of numerical re-calculation of the conditional probabilities. By modeling the update frequency as an attribute tailored for each TI, we already constrain the updates to the required amount. Exploring the benefit of localized updates within the Bayesian network based on direct TI dependencies and similar localization assumptions might be a way to further reduce the amount of calculations. The current simple BN structure is based on independence assumptions for TIs. Future work will include interdependent TIs in the BN structure as well. Modeling too many cursory dependencies will increase the BN maintenance effort while too few will result in an unrealistic model demanding for a balanced approach.

Here, we presented the trust indicator taxonomy and its use within a formal trust model. The set of trust indicators is not yet considered to be either complete or exhaustive. Future work will reveal additional trust indicators and their applicability with respect to different scenarios. We plan to investigate how we can put an emphasis or preference on TIs and categories from different application domains, e.g. manufacturing industries or high-tech industry, by adding such weights/preferences already to a user's request. This work may lead to the introduction of trust indicator profiles for user groups from different application domains. The work on aggregation of trust indicators we used can be extended, e.g. by stochastic processes and other techniques from stochastic system theory. An interesting point will be the adaptability and configurability of such techniques with respect to the stated user preferences and trust indicator dependencies.

References

Adusei-Poku, K. "Operational Risk management - Implementing a Bayesian Network for Foreign Exchange and Money Market Settlement", Faculty of Economics and Business Administration, University of Goettingen, 2005.

Allen, S. Financial risk management: a practitioner's guide to managing market and credit risk, Wiley, Chichester, 2003.

Arndt, E. S. Kennzahlen und Kennzahlensysteme: Grundlagen zur Entwicklung und Anwendung - Bibliographie deutschsprachiger Veröffentlichungen - praxisorientierte Literaturauswertung, Erich Schmidt, Berlin, 1985.

Blaze M., Feigenbaum J. and Lacy J.,*Decentralized Trust Management*, SP '96: Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996.

Brindley, C. *Supply chain risk*, Ashgate, Aldershot, 2004.

Chan, F. T. S. a., "Performance Measurement in a Supply Chain" *Journal Advanced Manufacturing Technology*, (21) 2003, pp. 534–548.

Cruz, M. G. Modeling, measuring and hedging operational risk, John Wiley and Sons Ltd., 2002.

Dellarocas C. and Resnick P., "Online Reputation Mechanisms, A Roadmap for Future Research", *First Interdisciplinary Symposium on Online Reputation Mechanisms*, 2003.

Damodaran, A. "Measuring Company Exposure to Country Risk: Theory and Practice", Stern School of Business, September, 2003.

[4] http://dbswitzerland.dnb.com/

[5] http://www.salesforce.com/

Egger, F. N. "From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce", Eindhoven University of Technology, 2003.
English, C., Terzis, S., and Wagealla, W. "Engineering Trust Based Collaborations in a Global Computing Environment", in Trust management : Second International Conference, iTrust 2004, Proceedings , Jensen, C. (Ed.), Oxford, UK, 2004, pp. 120-134.
Fenton, N.E. and Neil, M, "Combining evidence in risk analysis using Bayesian Networks", Safety Critical Systems Club Newsletter 13 (4), pp 8-13 Sept 2004
Gambetta, D. "Can We Trust Trust?", in *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, 1988.
Grandison, T., and Sloman, M. "A Survey of Trust in Internet Applications", in Surveys, I. C. (Ed.), 2000.
Hager, P. Corporate risk management: cash flow at risk and value at risk, Bankakad.-Verl., Frankfurt am Main, 2004.
Haller, J. "A Stochastic Approach for Trust Management", in International Workshop on Security and Trust in Decentralized/Distributed Data Structures (STD3S), 2006.
Hayne, R. M. "Modeling Parameter Uncertainty in Cash Flow Projections", *Financial Analysis Discussion Papers*, 1999 CAS Summer Forum, 1999.
Hevner, A. R., March, T. S.. Park, J., and Sudha, R. ”Design Science in Information Systems Research”, MIS Quarterly, 28(1), pp. 75-105, 2004
Ismail R. and A. Jøsang A., “The beta reputation system”, *Proceedings of the 15th Bled Conference on Electronic Commerce*, 2002.
Jensen, F. V. Bayesian networks and decision graphs, Springer, Tokyo, 2001.
Jøsang, A., "A Logic for Uncertain Probabilities", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001.
Jøsang, A., Ismail, R., and Boyd, C., "A Survey of Trust and Reputation Systems for Online Service Provision" *Decision Support Systems*, August 2004.
Jøsang, A., Keser C. and Theo Dimitrakos, "Can we manage Trust?", Proceedings of the Third International Conference on Trust Management, Paris, 2005.
Jøsang A., Gray L. and Kinateder M. Simplification and Analysis of Transitive Trust Networks 4(2) 2006, pp.139-161 . *Web Intelligence and Agent Systems Journal*. 2006
King, J. L. Operational risk: measurement and modelling, Wiley, Chichester, 2001.
Lehrbass, F. "A Simple Approach to Country Risk", Zentrales Kreditmanagement, WestLB, November, 1999.
Luhmann, N. "Familiarity, Confidence, Trust: Problems and Alternatives", in *Trust: Making and Breaking Cooperative Relations*, Gambetta, D. (Ed.), Basil Blackwell, 1988.
Mui, L., Mohtashemi, M., and Halberstadt, A. "A Computational Model of Trust and Reputation", in *Proceedings of the 35th Hawaii International Conference on System Science (HICSS), 2002*, 2002.
Nunamaker, J., Chen, M., and Purdin, T. D. M. „Systems Development in Information Systems Research“, *Journal of Management Information Systems*, 7(3), 1991, pp. 89-106.
Press, S. J. Subjective and objective Bayesian statistics: principles, models, and applications, Wiley-Interscience, 2003.
Robinson, P., Karabulut, Y., and Haller, J. "Dynamic Virtual Organization Management for Service Oriented Enterprise Applications", in *The First International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2005)*, 2005.
Romeike, F. Modernes Risikomanagement: die Markt-, Kredit- und operationellen Risiken zukunftsorientiert steuern, Wiley-VCH, Weinheim, 2005.
Ruohomaa, S., and Kutvonen, L. "Trust Management Survey", in *Trust Management: Third International Conference, iTrust 2005. Proceedings*, Springer, Oxford, UK, 2005.
Schultze, W. Methoden der Unternehmensbewertung: Gemeinsamkeiten, Unterschiede, Perspektiven, IDW-Verl., Düsseldorf, 2003.
Strader, T. J., Lin, F., and Shaw, M. J., "Information structure for electronic virtual organization management" *Decision Support Systems*, 1998, pp. 75-94.
Tan, Y. "A Trust Matrix Model for Electronic Commerce", in *Trust management: First International Conference, iTrust 2003, Proceedings*, Nixon, P., and Terzis, S. (Ed.), Heraklion, Greece, 2003, pp. 33-45.
Teitelbaum, D., and Axtell, R., "Firm Size Dynamics of Industries: Stochastic Growth Processes, Large Fluctuations, and the Population of Firms" *Small Business Research Summary*, (247) 2005.
Williams, E. J. "Downtime Data - Its Collection, Analysis, and Importance", in *Proceedings of the 1994 Winter Simulation Conference*, Tew, J. D., anivannan, S., Sadowski, D. A., and Seila, A. F. (Ed.), 1994.
Winkler, Till J. “Trust Indicator Modeling for a Reputation Service in Virtual Organisations”, *Diploma Thesis – Universität Karlsruhe (TH)*, http://www.eorg.uni-karlsruhe.de/publications/Winkler_06.pdf, 2006.