Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
Electronic Notes in Theoretical Computer Science 179 (2007) 87–96
www.elsevier.com/locate/entcs

Trust Mass, Volume and Density - a Novel Approach to Reasoning about Trust

Fredrik Degerlund

Turku Centre for Computer Science
Åbo Akademi University
Joukahainengatan 3-5
FIN-20520 Åbo, Finland

Abstract

The notion of trust has become a major factor in today's networked world. While security is widely recognized as an important aspect of public networked systems, the actions of individual participants is often neglected. Even though the need of trust management is taken into account, there is no universal solution as to what algorithms to use for calculating trust, nor is there any universal representation. In this paper, we propose a novel approach to managing trust by making an analogy between physical matter and abstract trust. We show that this alternative way of reasoning is feasible by proposing a framework based on metrics such as trust mass, volume and density, inspired by the corresponding concepts in physics. Our framework also provides for an intuitive means of representing trust graphically.

Keywords: Trust Metrics, Trust Fusion, Mathematical Models, Analogies.

1 Introduction

Along with the emergence of widespread electronic communications in large-scale computer networks, the problem of malicious or otherwise undesired behaviour among participants has grown into a major problem. The parties involved are often unknown to each other beforehand, and in many cases communication takes place on a temporary basis. Especially in business or otherwise sensitive communication, precaution is crucial in order to avoid fraud, identity theft, or other undesired activities. In light of this, the notion of *trust* has become an important indicator of which parties are benevolent vs malevolent.

There are several ways to gather trust "raw data", or reports, and distribute the information among the parties involved in communication. For example, reports can be divided into categories such as personal, trusted and public opinions, based of the origin on the opinions in question [4]. Exactly what method is used depends on the type of network in question, as well as what properties are emphasized in a particular scenario. For example, gathering data about peer behaviour in a mobile ad hoc

doi:10.1016/j.entcs.2006.08.033

network may differ significantly from the corresponding process in a network where a central server node is present. In addition to the process of gathering information about participants, the reports must in one way or another be interpreted in order to draw conclusions, or in other words, to calculate the actual trust metric. While the gathering of information is a field of research in its own right, so is the calculation of the trust metric based on the reported raw data, or report metric as it will be referred to in the subsequent sections. There is no universal agreement on what is the "best" trust metric. However, various kinds of metrics are used in practice, for example in online auction systems [1]. Trust metrics have also been studied theoretically, both from a general point of view [2] as well as in specific scenarios, such as attack-resistant trust metrics in public key certification [3].

1.1 On the nature of our approach

As the title suggests, this paper is about the process of reasoning about trust, i.e. calculating a trust metric from the raw data, in contrast to the process of collecting it. We also do not take a stand on the propagation techniques which might be needed if our approach is employed for example in ad hoc networks, where no central node is present. What we focus on is the interpretation of raw data, i.e. how to generate a suitable trust metric from the reports received.

Our model is continuous, in the form we present it. For example, we accept real values as input, we assume that time is continuous, and the resulting trust metric is a real number. However, this should not be seen as if the model would mandate a continuous treatment instead of a discrete one. As computers are discrete machines, all implementations will in any case be discrete, at least at the lowest level of abstraction. The model can also easily be translated into a discrete one, whereby for example integrals are changed into sums. The presentation in this paper is, however, of conceptual and mathematical nature, and as such, we feel that it is appropriate to treat the model in a continuous manner.

Our approach is intended to be quite general in nature. As such, it is not "locked" to a specific scenario. Instead, we reason about the foundations of trust, and the main contribution of this paper is to show the possibility of using concepts from physics to describe the behaviour of trust. More specifically, we introduce quantities such as mass, volume and density, which are normally used to describe properties of matter in nature. While many other trust schemes have been proposed, they are normally "artificial" in the sense that they are invented for the sole purpose of representing trust. While artificial approaches may be specifically tailored for their purpose, we also consider it valuable to make analogies between different phenomena, or at least find out in what cases it is *possible* to do so.

1.2 Layout of the paper

The rest of the paper is structured as follows. In section 2, we introduce a number of concepts that are fundamental to our approach. Section 2.1 presents the report metric, which represents feedback about the test entity as given by the observers.

In the following subsection, the concept of trust area is defined by using the report metric. Furthermore, in section 2.3 we define trust volume as an extension of the trust area, by involving a height function. In section 3, we present aging of trust, which is based on trust mass and density, which are introduced in 3.1. Section 4 is concerned with various constraints on the parameters and functions of our approach, so that the model behaves as desired. We present a number of soundness properties that can be expected from a trust metric, and we show that our model fulfils them. Finally, in section 5, we sum up what we have presented in the paper.

2 Fundamental metrics

2.1 Report metric

A quantity, which will be referred to as the report metric, is of fundamental importance for the approach presented in this paper. It represents the level of trust in the object in question as reported by one or several observer(s). The report metric is a continuous and total function of time, $rm = rm(t)$, defined in an interval $[0, t_{now}]$. In the case of several observers, the metric is a function of the individual report metrics, for example a mean value. In that case we calculate the combined trust metric according to the following formula:

$$rm = rm(t) = \frac{rm_1(t)+rm_2(t)+...+rm_n(t)}{n}.$$

Alternative ways of combining trust metrics will be discussed in section 4.2.

2.2 Trust area

The trust base area (or simply trust area or trust base), A, is a quantity calculated directly from the report metric. The trust area is a function, which is defined in an interval $I = [0, t_{now}]$, and calculated as

$$A_I = \int_I rm(t)dt.$$

The graphical interpretation is thus an area, which is bounded by the report metric function. As the report metric is also allowed to be negative, the (sub)intervals of I in which $rm(t) < 0$ imply a decrease in the total trust area. The trust base as a whole may also be negative. An important observation is the fact that the trust area is actually a measure of the total amount of trust over the interval. Intervals with a high report metric contribute to the total trust base in a high degree, whereas intervals of low report metric only add a little to it. Furthermore, negative intervals decrease the trust base; a fact that corresponds well to the intuitive interpretation of a trust metric.

2.3 Trust volume

By multiplying the trust base A_I with a height, we calculate the volume, V, of a three-dimensional body (see figure 1). It is, however, important to note that the volume is also allowed to be negative, in which case the entity in question should

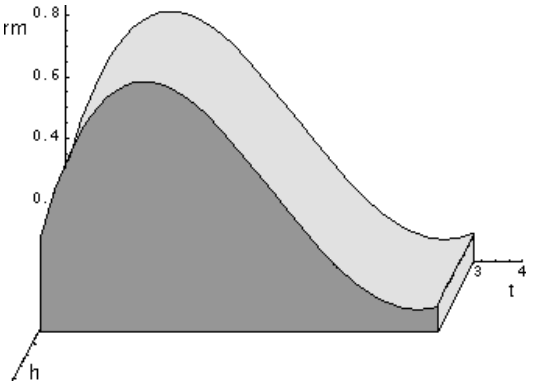

Figure 1. Trust volume (constant height).

be seen as being more untrustworthy than trustworthy. The height, h, is intuitively a value which amplifies the trust base metric, so that a high height implies a large volume. Similarly, a low height leads to a small volume, even though the trust base may be the same. The formula for calculating this volume is:

$$V_I = h * \int rm(t)dt.$$

The usefulness of this amplification, and thus the whole notion of trust volume, may not be evident unless we introduce a height which is variable in time: $h = h(t)$, defined over the interval I. Extending the formula to include this scenario yields:

$$V_I = \int_I h(t)rm(t)dt.$$

This extension increases the expressiveness of the concept of trust volume as compared to the trust area, as different periods of time may now be given different importance. At periods of time when reliability in the test subject is crucial, the function $h(t)$ may be given a larger value, resulting in a larger amplification in the trust volume. In this way, the implications of the report metrics during these periods of time are given a higher impact. We also note that if using the constant function 1 as height function, the formula simply degrades to the one for trust area. Hence, trust volume can also express everything that trust area can, and is thus superior in terms of expressiveness.

3 Mass, density and decay

As the behaviour of people and other entities may change over time, it is often reasonable to believe more in feedback reports given recently than those that have been given at an earlier point in time. As the trust volume does not take this aspect into consideration, it is evident that we need to introduce new concepts in order to adapt the model to these facts. To achieve this goal, we will incorporate aging into the model. However, before doing so, we have to present the notions of trust density and trust mass.

3.1 Density and mass

We first consider the simple case where the trust density, denoted by ρ, is constant. In this case, the density is simply a real value, and the trust mass, m, is calculated as the product of the trust volume and the trust density, i.e. $m = V * \rho$. However, the usefulness of the concepts is not evident unless we allow the trust density to vary over time as a (total) function $\rho(t)$, where $t \in I = [0, t_{now}]$. The trust mass is, in turn, defined as:

$$m_I = \int_I \rho(t)h(t)rm(t)dt.$$

This definition is also valid for the case of constant trust density, as that can simply be seen as a special case of the variable version where $\forall t \in I : \rho(t) = \rho$ (constant). As a result of this fact, the formula for calculating the trust mass simply degrades to the one mentioned above, as $m_I = \int_I \rho(t)h(t)rm(t)dt = \rho \int_I h(t)rm(t)dt = V_I * \rho$.

Trust mass degrades to trust volume if the density function is set to the constant function 1. Hence, it can also express everything that trust volume can. This can be compared to the reduction of trust volume to trust area by setting the height to 1, as stated in section 2.3.

3.2 Decay of trust

To achieve the effect of trust aging, we use another analogy from physics, namely radioactive decay. Still, it is important to stress that this analogy should not be pushed too far. For example, radioactive nuclei decay into other elements and radiation, whereas we consider the decayed trust to completely disappear. Another way in which our concept differs from physics is that we permit decay functions of different forms than the one that takes place in nature (and the trust function itself is expressed in another fashion).

In our model, the idea of decay is intended to reduce trust density over time. It is represented by a higher-order function, which takes the current time as input and returns a specific density function such as presented in the previous subsection. What is important to notice is that this function can be used to calculate the current density of the trust mass generated at earlier points in time. However, this particular function is only valid for the (current) time it was calculated for. In other words, at each point in time, we can calculate a function that gives the current density of the previously generated trust. In this way, we can achieve aging of trust by choosing the decay function carefully. This process can easily be illustrated, as in figure 2, which contains snapshots from an example scenario at time t=2 (left) and t=3 (right). In the graph from t=2, the trust is still relatively fresh. The most recently generated part is still black (high density), while the oldest one is a little greyish, representing a slight decay. However, at time t=3, the oldest part has almost completely decayed, and only the newly generated trust is still dense.

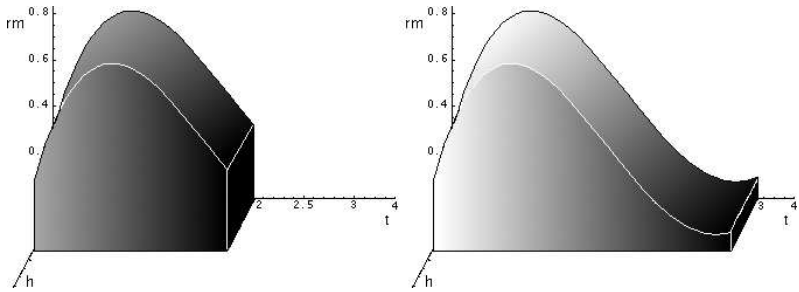

Figure 2. Trust decay. Snapshot when time is 2 (left) and 3 (right). Gradient represents density.

4 Constraints on functions and parameters

In the preceding sections, several functions and parameters have been presented. Many of these can be chosen by the person who sets up the system. They should, however, be chosen carefully, as they have a large impact on the behaviour of the model. The parameters and functions can be tailored to specific scenarios, taking into account what is important in those specific cases. Even though they can be chosen relatively freely, there are also certain values and functions that are not acceptable, simply because they make the model behave in a counter-intuitive way, or make the model unsound. The topic of this section is to pinpoint which choices are appropriate and which are not. An overview is presented in table 1.

4.1 Constraints on the report metric

As the report metric is the quantity which provides input data to the model, the process of calculating this quantity is not within the scope of this paper. Still, trust metric values about the same entity, given by various observers, can be combined to a single trust metric using a combination function. This matter will be discussed in the following subsection, and was also shortly mentioned in section 2.1.

Despite the above statement, the model may put restrictions on the type of values that are accepted as input. The model does not require us to accept only values within a particular interval. However, it is important that the report metric, when seen as a function of time, allows us to calculate a unique trust area value. This implies that the integral in the trust area formula must not diverge. Based on well-known integral calculus we can conclude that the integral will not diverge in case the trust metric function itself does not do so. Hence, trust metric functions that do not diverge are acceptable. However, we can not draw the reverse conclusion, i.e. that if the report metric function diverges, the integral would also necessarily do so. In theory, there are also report metric functions that do diverge, still resulting in a well-defined integral value. Still, for our model, we find it hard to think of a diverging report metric function which would actually make sense from a practical point of view, when taking into consideration that it is supposed to represent feedback about how entities are behaving. From this point of view, we find it appropriate to restrict the report metric function so that it is not allowed to diverge, even though some other cases would also be applicable from a strictly mathematical point of view.

	Explanation	Not.	Formula	Constraints
Report metric	Input raw data, or data calculated using an rm combination function.	*rm*, *rm(t)*	Raw input data, or a function of other rm's. See below.	The report metric, if seen as a function, should not diverge.
Report metric combination function	Function for combining individual report metrics.	-	*For example* a weighted mean value: $rm(t) = c_1 * rm_1(t) + ... + c_n * rm_n(t)$,where $\sum_{i=1}^{n} c_n = 1$ and $c_i > 0$	Non-divergent. Should be somund in practice, e.g. a weighted mean value.
Trust area	A simple trust metric.	A	$A_I = \int_I rm(t)dt$	(Not given as input)
Height / Height function	Amplification of trust metric reports in some intervals.	*h*, *h(t)*	Various functions (however, see restrictions).	Non-divergent, typically non-negative.
Trust volume	A trust metric based on trust area and height.	V	$V_I = \int_I h(t)rm(t)dt$	(Not given as input)
Trust density	Specifies the density of trust. Useful for aging.	ρ	If aging is applied, gener. by decay fun. (see below). If not, various fun. (see constr.).	Non-divergent, typically non-negative and growing.
Trust mass	A trust metric based on trust volume and trust density.	m	$m_I = \int_I \rho(t)h(t)rm(t)dt$	(Not given as input)
Decay function	Generates density functions. Useful for aging.	-	Various. However, see restrictions.	See section 4.3

Table 1
Functions, parameters (and metrics), as well as constraints on them.

4.2 Choosing a report metric combination function

In section 2.1, we suggested that individual report metrics can be combined by calculating a mean value. However, other functions are possible as well. Many kinds of functions would be plausible from a mathematical perspective, but they should also be sound in practice. A mathematical constraint is that the function must not diverge, and practical constraints involve the fact that the resulting report metric should somehow represent the reports given as input values. Not excluding other possible function, we suggest using a linear combination of the individual report metrics, i.e.:

$$rm(t) = c_1 * rm_1(t) + c_2 * rm_2(t) + ... + c_n * rm_n(t).$$

The constants, c_i, should typically be positive, so that each individual report increases the sum if it is positive and decreases it when a negative report is given. Depending on the nature of the scenario in question, one may prefer constraining the constants so that $\sum_{i=1}^{n} c_n = 1$, whereby the linear combination degrades to a weighted mean value. Furthermore, if fixing the weights to equal values, the result will be normal mean value, as we suggested earlier.

4.3 Constraints on the height, density and decay functions

The height function, $h(t)$, is present in the formula for calculating trust volume and mass, the latter also containing the density function $\rho(t)$. By reasoning in a similar way as when constraining the report metric (in 4.1), we do not wish the products $h(t)rm(t)$ (in the volume formula) or $\rho(t)h(t)rm(t)$ (in the mass formula) to diverge. This can be achieved by limiting both $h(t)$ and $\rho(t)$ to non-divergent functions.

Mathematically, the height function could also generate negative values, but as this would imply that positive feedback decreases the amount of trust, and vice versa, most scenarios probably require it to be non-negative. A similar reasoning also applies to the density function, as negative density introduces strange behaviour. Thus, the density function should typically be non-negative. The density function being zero in some intervals might, however, be useful. Also the height function being zero at intervals might come into question, as that would simply imply that the intervals in question are not be taken into consideration when calculating the trust metric.

When deciding density functions, there is one more property that ought to be stressed, especially when density is used to express aging. If the intention is to give new trust a high density, whereas older trust should be less dense, the density function should be growing. The decay function should also, in this case, be chosen in such a way that the a more recently generated density function never attributes a higher density value to a specific piece of trust than a previous function has. That is, if $\rho_2(t)$ is a more recently generated density function than $\rho_1(t)$, then $\rho_1(t) \geq \rho_2(t)$ should apply for all values of t. Even though this rule is reasonable in most cases, we do not claim that it is a universal rule, or that there would be no exotic scenarios where density grows or older pieces of trust should be given more importance than newer ones.

5 Conclusions

In this paper, we have introduced a number of trust metrics, sharing a common property: they are inspired by their corresponding entities in physics. Our model behaves intuitively, provided that certain restrictions are posed on the parameter values and functions. We pinpoint what restrictions are needed, and for what reasons, from a soundness point of view. Apart for those specific values, we allow a large number of parameters, so that the model can be adapted to the specific scenarios. This property can be helpful when adapting the model for use in concrete scenarios. An overview of the concepts, as well as the way they are related to each other, is presented in table 2. We also note that trust mass is the most powerful of the concepts presented, and can express all the properties of trust volume, which in turn has all the capabilities of trust area. The two last mentioned concepts are, however, important from a theoretical point of view, as they are used to build up the theory involved in trust mass. Thinking of trust as physical matter also provides convenient ways of expressing trust graphically, as shown by the various graphs in the paper.

	Provides	**Data required**	**Concepts required**
Report metric	Only feedback raw data	Input from observer(s)	-
Trust area	A simple notion of trust	Report metric	Integral
Trust volume	Same as trust area + Support for variable amplification	Trust area & a height function	Integral
Trust mass	Same as trust volume + Support for trust aging	Trust volume & a decay function	Trust density, trust decay

Table 2
The central concepts of the paper, and how they are related.

One of the most important contributions is, however, that we have shown that it is *possible* to make an analogy between the properties of physical matter and those of abstract trust. While we consider this property valuable in itself, we also believe that by creating a basic framework, further analogies can in the future be used to

incorporate new concepts into the modelling of trust.

References

[1] eBay, *Understanding feedback scores.*
URL http://pages.ebay.com/help/feedback/feedback-scores.html

[2] Jøsang, A. and S. Knapskog, *A metric for trusted systems*, in: *Proceedings of the 21st National Information Systems Security Conference*, 1998, pp. 16–29.

[3] Levien, R. and A. Aiken, *Attack-resistant trust metrics for public key certification*, in: *Proceedings of the 7th USENIX Security Symposium*, 1998, pp. 229–241.

[4] Neovius, M., *An abstract model for incentive-enhanced trust in p2p networks*, in: *Embedded and Ubiquitous Computing: EUC 2005* (2005), pp. 602–611.