# On Time, Conflict, Weighting and Dependency Aspects of Assessing the Trustworthiness of Digital Records

Jianqiang Ma*†, Habtamu Abie†, Torbjørn Skramstad* and Mads Nygård*
* *Department of Computer and Information Science*
*Norwegian University of Science and Technology, Trondheim, Norway*
*Email: {majian, torbjorn, mads}@idi.ntnu.no*
† *Norwegian Computing Center, Oslo, Norway*
*Email: {Jianqiang.Ma, Habtamu.Abie}@nr.no*

***Abstract*—In the area of digital records management, the reliability of a digital record's operator varies over time, and consequently affects the trustworthiness of the record. The quality of the reliability of the operator is a measure of the quality of the record's evidential value that is, in turn, a measure of the record's trustworthiness. In assessing the trustworthiness of a record using evidential value, it is essential to combine evidence from various sources, which may be conflicting and/or interdependent. In this paper we describe our research on these problems, and develop a trustworthiness assessment model which addresses these problems and integrates a beta reputation system in combination with a forgetting factor to assess the temporal aspects of the evidential value of an operator, a weighting mechanism to detect and avoid conflicts, and a weighted sum mechanism to combine dependent evidence. Our results show that the integrated model can improve the objective assessment of the trustworthiness of digital records over time using evidential value as a measure of trustworthiness.**

***Keywords*-Trustworthiness Assessment, Trust, Digital Record Management.**

## I. Introduction

In the area of digital records management, research on the trustworthiness of digital records is an issue that has received much attention mainly in two areas, Security [1], [2] and Trustworthy Repositories [3], [4]. In our previous work [5], we proposed a complementary method, which assesses the trustworthiness of digital records based on their evidential values using the Dempster-Shafer (D-S) theory of evidence [6]. Four challenges to the assessment model have been identified, i.e., time, conflict, weighting, and dependency aspects. In this paper, we improve our previous model by addressing all four aspects.

This paper describes the time aspect of the trustworthiness assessment model using the reliability of a digital record's operator, since the reliability of an operator varies over time, and, which in turn, affects the assessment result of the trustworthiness of the digital record. Inspired by [7], historical information about the behaviours of operators, which can be obtained from the logs of digital repositories, is used to evaluate their reliability. Correct or incorrect behaviours of operators can be recognised as positive or negative ratings of their reliability. In this way, the widely-researched reputation system mechanism [8]–[10] can be used here for the evaluation of operators' reliability. In this paper, we adopt the beta reputation system [8] to evaluate the reliability of operators, and to create a function to map the evaluated result to the mass function, which can later be used in the D-S theory for the assessment of the trustworthiness of digital records.

Many researchers have criticized the way conflicts are handled in the D-S theory [11], [12]. When using the D-S theory to combine evidential values of evidence around digital records, we have paid attention to these criticisms. We first investigate how to detect conflicts between evidence, and then avoid those conflicts by assigning different weighting, since different evidence may have different importance to the assessment. In addition, we study the combination of evidential values from interrelated evidence, since Dempster's rule of combination is based on independent evidence. We use an alternative approach to combine evidential values from dependent evidence.

As the time aspect deals with evidential values assigned to records' operators, and the other three aspects deal with the combination of evidential values, these four aspects together improve the assessment model by increasing the quality of the evidential values assigned to the evidence, and by improving the way they are combined.

We note that the investigation and evaluation of operators' reliability over time is not fundamentally different from research in the domain of reputation systems [8]. The applicability to the area of trustworthiness assessment of digital records and the integration with the D-S theory are two of the main contributions of this paper. The third is the integration of a conflict detection mechanism, a weighting mechanism, and a dependent evidence combination mechanism in the D-S theory for assessing the trustworthiness of digital records.

The rest of this paper is organised as follows. Section II describes the related work. Section III briefly introduces the Trustworthiness Assessment Model proposed in our previous work. Section IV, V, VI, and VII give an account of our research on the temporal, conflict, weighting and dependency aspects of the trustworthiness assessment model, respectively. Finally, the conclusion and future work are presented in Section VIII.

## II. Related Work

Reputation systems allow users to rate on an agent that they have had a transaction with, and use these ratings to assess the reliability of the agent. It was first used in online shopping websites, such as eBay, to assess the trustworthiness of online sellers [13], and was later further developed in the Peer-to-Peer (P2P) networks area to assess the reliability of agents [9], [10]. An extensive survey and overview of trust and reputation systems can be found in [14]. Among these reputation systems, the beta reputation system together with a forgetting factor proposed by Jøsang [8] is capable of assessing one's reliability at a particular time, based on historical information. It has been adopted in many areas [15]. In this paper, we adopt the beta reputation system to evaluate the reliability of records' operators in the trustworthiness assessment model because of its "flexibility and simplicity as well as its foundation on the theory of statistics". The beta reputation system was presented as a stand-alone mechanism in [8]. By mapping the evaluation results to the basic belief assignments (bbas), we integrate it with the D-S theory for the assessment of the trustworthiness of digital records.

The D-S theory of evidence has been applied in many different areas to combine evidence from different sources [16], [17]. One feature of the D-S theory that has received criticisms is its way of handling conflicts [11], [12]. Many alternatives to Dempster's rule of combination have been proposed. The most famous alternatives are conjunctive [18], disjunctive [19] and Yager's [20] combination rules. In the area of belief conflict detection, Josselme et al. [21] proposed a method for measuring the distance between two bbas. Liu [22], however, argued that by only using this distance one cannot distinguish whether two bbas are in conflict or not. Consequently, after formally defining the conflict between two bbas, the author proposed an approach to analyse conflicts, which uses the mass of the combined belief allocated to the empty set before normalisation and the distance between betting commitments (see Section V). Our method of detecting possible conflicts is similar to this method. It differs from it in that our method resolves these conflicts by assigning different weighting to the sources.

Regarding the dependency aspect of different sources, Ferson et al. [23] have done a thorough analysis of dependencies in the D-S theory and probabilistic modelling, including copulas and Fréchet bounds. The weighted sum operator was proposed by McClean and Scotney [16] for the integration of distributed databases. They proved that "the weighted sum operator is a mass function and it is both commutative and associative". It was later adopted by Hong et al. [17] to combine bbas of dependent sensor data in smart homes. They assigned equal weight to the dependent sensors. However, this might not be true in most cases. In this research, we integrate the weighted sum operator into our assessment model to solve the dependency problem by assigning different weighting to sources based on their importance to the assessment.

## III. The Trustworthiness Assessment Model

In this section, we briefly introduce the model for the assessment of the trustworthiness of digital records in order to improve the understanding of the aspects addressed in this paper. For detail information about the model, readers are referred to our previous paper [5].

In order to assess the trustworthiness of digital records, we have identified, analysed and specified a list of evidence that shall be stored in the metadata related to digital records [24]. These metadata, named Evidence-Keeping Metadata (EKM), are a subset of the Record-Keeping Metadata [25], but limited only to the metadata, which contain evidence of the trustworthiness or untrustworthiness of digital records. A digital record associated with its EKM can be structured as a tree based on a proposed record's life-cycle model [24].

As shown in Fig. 1, the trustworthiness of a digital record is built up of trustworthiness during different phases of the record's life cycle, which in turn can be categorised by the trustworthiness of various components. Finally, the trustworthiness of each component is assessed using evidence stored in EKM. After receiving the linguistic evidential values of EKM as well as their "trustworthiness hypotheses" (either trustworthy or untrustworthy) from a panel of experts, the assessment model maps them into bbas, and uses these bbas in the D-S theory to assess the trustworthiness of a digital record from the bottom to the top.

In [5], we have proposed this model and identified a number of challenges that still need to be met, to wit the temporal aspect, conflicts, dependencies, and weighted differences among EKM. In the ensuing sections, we describe these challenges, respectively. Note that the model uses bbas assigned to the EKM as basic units for the assessment of the trustworthiness of digital records. Hence, as long as the solutions to these challenges can be mapped to bbas, it is fairly easy to integrate the solutions into the trustworthiness assessment model.

## IV. Temporal Aspect

In this section, we describe the temporal aspect of the trustworthiness assessment model briefly introduced above. Inspired by [7], we studied the temporal aspect by looking into the reliability changes of digital records' operators over time. Using long-term observations, the history of digital records as well as the behaviours of records' operators can be logged. On the basis of that historical information, the behavioural patterns of the operators can be learnt, which

Copyright (c) IARIA, 2011. 

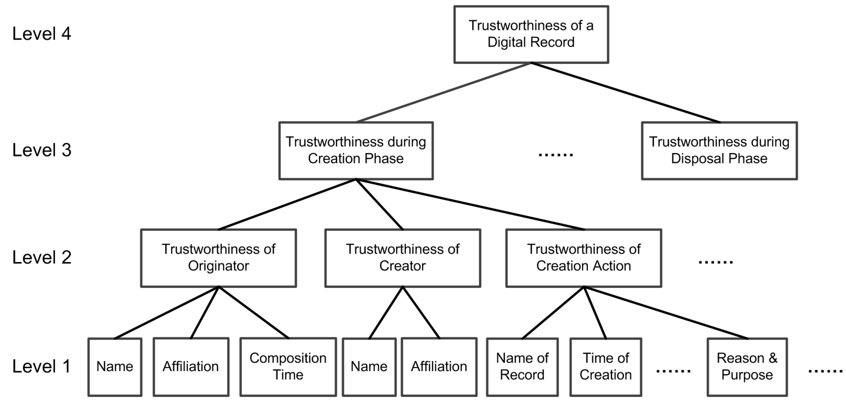


Figure 1. Structure of the EKM for the assessment of the trustworthiness of a digital record [24]

provide us with the possibility to evaluate the reliability of the operators' operations on the records.

Good and bad behaviours of an operator $P$ can be documented and used to learn his/her behavioural pattern. A good behaviour means that the operation on a digital record does not compromise the trustworthiness of the record. While a bad behaviour means that the operation decreases the trustworthiness of the record. Good or bad behaviours of $P$ can be discovered through verifications performed by one or more other operators or by verification software. The way of detecting good or bad behaviours in a digital library system is outside the scope of this paper. Instead, this paper focuses on how to learn $P$'s behavioural patterns.

The reliability of $P$ can be predicted using the numbers of good and bad behaviours. It can further be interpreted as the evidential value of $P$, because both reliability and evidential value present the degree to which $P$ can be used as evidence to prove the trustworthiness of the record $P$ operated on. The reliability - evidential value - of $P$ varies along with the accumulation of the number of behaviours. In this study, the beta reputation system [8] is adopted to assess the reliability - evidential value - of $P$.

In our case, we map a good behaviour of $P$ to a good feedback on $P$, and a bad behaviour to a bad feedback. Thus, the evidential value of $P$ can be calculated as:

$$EV(P) = \frac{g+1}{g+b+2} \tag{1}$$

with the restriction that $g, b \geq 0$, where $g$ is the number of good behaviours that have been exhibited by $P$, and $b$ is the number of bad behaviours that have been exhibited by $P$.

In order to integrate the evaluated evidential value of $P$ into the trustworthiness assessment model and combine it with evidential values of other EKM, $EV(P)$ needs to be mapped to the bbas defined in the D-S theory. In addition, a "trustworthiness hypothesis" $H_P \in \{true, false\}$ should be specified, where $H_P = true$ or $H_P = false$ mean that $P$ (presented as "Name" of operator in Fig. 1, e.g., "Name of Creator"), as evidence, can be used to prove that $P$'s higher level node is either trustworthy or untrustworthy.

When $P$ exhibits more good behaviours than bad behaviours ($g > b$), it shows that $P$ tends to be reliable, and should be used to prove that its higher level node is trustworthy to a certain degree, thus, $H_P = true$, and vice versa. In the case when $g = b$, $H_P = \phi$, which means that it cannot prove its higher level node is either trustworthy or untrustworthy. When $H_P = false$, instead of using $\frac{g+1}{g+b+2}$, the evidential value of $P$ is assigned as $EV'(P) = 1 - \frac{g+1}{g+b+2} = \frac{b+1}{g+b+2}$, since in this case, it is used to present the degree of its higher level node's untrustworthiness.

It is obvious that both $EV(P)$ and $EV'(P)$ are in the interval $[0.5, 1]$. Since bba is in the interval $[0, 1]$, it is necessary to scale $EV(P)$ and $EV'(P)$ into that interval. Hence, the mapping rules are defined as follows:

$$\text{if } g > b\text{, then } H_P = true \text{ and } \begin{cases} m_P(T) = \frac{2g+2}{g+b+2} \\ m_P(\overline{T}) = 0 \\ m_P(U) = \frac{g-b}{g+b+2} \end{cases} \tag{2}$$

$$\text{if } g < b\text{, then } H_P = false \text{ and } \begin{cases} m_P(T) = 0 \\ m_P(\overline{T}) = \frac{2b+2}{g+b+2} \\ m_P(U) = \frac{b-g}{g+b+2} \end{cases} \tag{3}$$

$$\text{if } g = b\text{, then } H_P = \phi \text{ and } \begin{cases} m_P(T) = 0 \\ m_P(\overline{T}) = 0 \\ m_P(U) = 1 \end{cases} \tag{4}$$

where $g, b \geq 0$ are the numbers of good or bad behaviours of $P$, as defined in Equation (1).

As presented in Equation (1), the evidential value of $P$ changes with the accumulation of good or bad behaviours. However, from the long-term perspective, the old behaviours may be less relevant in the revelation of $P$'s evidential value, because the behavioural pattern of $P$ might have changed. Therefore, we introduce the forgetting factor $\delta$ proposed in [8] into the calculation in order to reduce the impact of the old behaviours on modelling of $P$'s current behavioural pattern. That is, exhibiting $G$ good behaviours at an older time $t_1$ equals exhibiting $G\delta^{t_2-t_1}$ good behaviours at a more recent time $t_2$, where $t_2 > t_1$ and $0 \leq \delta \leq 1$. When $\delta = 0$, it forgets every old behaviours, and uses the most recent behaviour to calculate the evidential value of $P$. In other words, the old behaviours have no impact on the calculation at all. When $\delta = 1$, it never forgets, and the old behaviours have the same impact as the recent behaviours on the calculation of the evidential value of $P$.

In the calculation of the trustworthiness of a digital record, users of the calculation system can assign a number between 0 and 1 as the forgetting factor, to designate how much the old behaviours should impact the calculation. Since the operator identity and the time of each operation on the digital record are already documented as EKM, together with the forgetting factor assigned by the user, they can be used to calculate the evidential value of an operator for every operation. Hence, even if the same operator operated on the same digital records, his/her evidential value can be different due to the different operation times. For example, operator $P$ created a digital record at time $t_1$, and later (say after months), migrated the record to another repository at time $t_2$, the evidential value of $P$ for those two operations could be different, because the reliability of $P$ may be different at time $t_1$ and time $t_2$. In this way, the assessed trustworthiness of the digital record will be more accurate than using the same evidential value of $P$ for different operation times.

After adopting the beta reputation system as well as the forgetting factor, the assessment method for the trustworthiness of digital records that reflects the temporal aspect is as follows.

$$\begin{aligned} m_{record}(T) &= m_{creation}(T) \oplus m_{modification}(T) \oplus \\ &\quad m_{migration}(T) \oplus m_{retrieval}(T) \oplus m_{disposal}(T) \\ &= m_{Originator}(T) \oplus m_{Creator}(T) \oplus m_{CreationAction}(T) \\ &\quad \oplus \ldots \oplus m_{DisposalExecutor}(T) \oplus m_{DisposalAction}(T) \\ &= m_{EKM_1}(T) \oplus \ldots \oplus m_{EKM_m}(T) \\ m_{record}(\overline{T}) &= m_{EKM_1}(\overline{T}) \oplus \ldots \oplus m_{EKM_m}(\overline{T}) \\ m_{record}(U) &= m_{EKM_1}(U) \oplus \ldots \oplus m_{EKM_m}(U) \end{aligned} \quad (5)$$

where $\{EKM_1 \ldots EKM_m\}$ stands for all the EKM related to the digital record - nodes in Level 1 in Fig. 1. Particularly, for $EKM_i \in \{EKM_1 \ldots EKM_m\}$, which stands for the reliability of the operator $P$ at a certain time, its bbas are calculated based on Equation (2), (3), and (4).

## V. Conflict Aspect

In our research, the D-S theory is used to combine the evidential values from different EKM. However, the way of handling conflicts in the D-S theory has received some criticisms [11], [12]. It is defined in [22] that "a conflict between two beliefs in D-S theory can be interpreted qualitatively as one source strongly supports one hypothesis and the other strongly supports another hypothesis, and the two hypotheses are not compatible." Here we present an example of a conflict that may happen in the trustworthiness assessment model. Suppose there are two experts $E_1$ and $E_2$ who assign evidential value for a piece of EKM, say $EKM_1$. $E_1$ suggests that $EKM_1$ is a strong evidence, which supports that its higher level node is trustworthy, hence, bba of $EKM_1$ assigned by $E_1$ is $m_1(T) = 0.8, m_1(\overline{T}) = 0$, and $m_1(U) = 0.2$. Actually, experts assign linguistic evidential values to EKM that will later be mapped to numerical evidential values and further bbas of EKM by the trustworthiness assessment model. For simplicity, we only present the mapped bbas here. $T$ and $\overline{T}$ are propositions that $EKM_1$'s higher level node is either trustworthy or untrustworthy. $U$ is the universal set. $E_2$ also suggests that $EKM_1$ is a strong evidence, however, it supports that its higher level node is untrustworthy, and the bba assigned by $E_2$ is $m_2(T) = 0, m_2(\overline{T}) = 0.8$, and $m_2(U) = 0.2$. Using Dempster's rule to combine the assignments from two experts, the result is $m_{12}(T) = 0.44, m_{12}(\overline{T}) = 0.44$, and $m_{12}(U) = 0.12$, which is very near to the average of the two bbas. This is not a good way of handling conflicts, because it hides the conflicting opinions between experts, which may further lead to an imprecise assessment of the final results. Thus, it is necessary to prevent conflicts occuring, and to detect them if they do.

### A. *Conflict Detection*

In this section, we demonstrate the method for detecting conflicts from different sources. This method is proposed in [22], which uses two indicators to detect conflicts between two bbas, i.e., the combined belief allocated to the empty set before normalisation ($m_{\oplus}(\phi)$) and the distance between their betting commitments.

As defined in [26], the pignistic probability function $BetP_m$ associated to bba $m$ on the universe is:

$$BetP_m(\omega) = \sum_{A \subseteq U, \omega \in A} \frac{1}{|A|} \frac{m(A)}{1 - m(\phi)} \quad (6)$$

where $|A|$ is the cardinality of subset $A$ on $U$. The transformation from bba $m$ to $BetP_m$ is called the pignistic transformation. It can be further extended to $2^U$ that $BetP_m(A) = \sum_{\omega \in A} BetP_m(\omega)$. $BetP_m(A)$, referred to as the *betting commitment to* $A$ in [22], presents the total mass value that $A$ can carry.

Thus, the distance between two betting commitments to $A$ from two sources is considered as the maximum of the differences between their betting commitments to all the subsets, defined as

$$\Delta BetP_{m_1}^{m_2} = max_{A\subseteq U}(|BetP_{m_1}(A) - Bet_{m_2}(A)|) \quad (7)$$

While the combined belief allocated to the empty set before normalisation ($m_\oplus(\phi)$) in the D-S theory is defined as

$$m_\oplus(\phi) = \sum_{B,C\subseteq U, B\cap C=\phi} m_1(B)m_2(C) \quad (8)$$

It is discussed in [22] that the sole use of either $m_\oplus(\phi)$ or $\Delta BetP_{m_1}^{m_2}$ cannot detect the conflicts between two beliefs, they should be used together in order to detect conflicts. Thus, based on the definition presented above, two beliefs $m_1$ and $m_2$ are defined as in conflict if and only if both $\Delta BetP > \epsilon$ and $m_\oplus(\phi) > \epsilon$, where $\epsilon$ is the factor that indicates the tolerance of conflict. The higher $\epsilon$ is, the more tolerance of conflict the system is.

Let us see the two beliefs in the example above where

$$m_1(T) = 0.8, \quad m_1(\overline{T}) = 0, \quad m_1(U) = 0.2,$$
$$m_2(T) = 0, \quad m_2(\overline{T}) = 0.8, \quad m_2(U) = 0.2.$$

Using Equation (6), (7), and (8), the $\Delta BetP_{m_1}^{m_2}$ and $m_\oplus(\phi)$ of $m_1$ and $m_2$ are calculated as

$$BetP_{m_1}(T) = 0.9, \quad BetP_{m_1}(\overline{T}) = 0.1, \quad BetP_{m_1}(U) = 1,$$
$$BetP_{m_2}(T) = 0.1, \quad BetP_{m_2}(\overline{T}) = 0.9, \quad BetP_{m_2}(U) = 1,$$
$$\Delta BetP_{m_1}^{m_2} = 0.8, \quad m_\oplus(\phi) = 0.64.$$

Thus, if assigning $\epsilon = 0.6$, the opinions from those two experts will be recognised as in conflict, while if assigning $\epsilon = 0.7$, they will not be seen as in conflict, even though $\Delta BetP_{m_1}^{m_2} > \epsilon$.

When conflicts occur, it does not necessarily mean that the use of D-S theory to assess the trustworthiness of digital records is wrong, but simply that, due to the conflicts in beliefs from difference sources, the results may be imprecise. Thus, together with the assessment results, the assessment model will also inform users that conflicts between different elements have occurred during the assessment. Users can consider this information together with the assessment result to determine whether a digital record is trustworthy or not.

### B. Conflict Avoidance

By analysing the sources of conflicts in the assessment model, it can be found that conflicts may exist among experts' opinions, EKM, components, and life-cycle phases of a digital record. For a certain piece of EKM, due to the differences in observations or experience, experts can have different opinions on its use as evidence, therefore, different evidential values and trustworthiness hypotheses may be assigned to it, which may further induce conflicts among bbas assigned to this piece of EKM. It is also similar for other elements in the assessment model, such as EKM, components, and life-cycle phases.

Notice that until now, all the elements in the assessment model have been recognised as equally important. However, it is more realistic to assign different weighting to different elements. For instance, some of the experts may have more knowledge or experience than others, hence, their opinions deserve to be considered as more important than others'. In addition, by assigning different weighting, many conflicts can be avoided, because beliefs from less weighted sources will be discounted.

In the following section, we discuss the weighting difference as well as how to discount bbas in the D-S theory.

## VI. Weighting Aspect

Weighting difference can be used to differentiate the importance among different elements in the assessment model. Also, as presented in the section above, it is a way to avoid conflicts from different sources.

The discounting method in the D-S theory [6] is introduced to assign weighting to elements, as shown in Equation (9).

$$m_1^{discounting}(A) = \begin{cases} \alpha m_1(A) & \text{if } A \neq U \\ \alpha m_1(U) + (1-\alpha) & \text{if } A = U \end{cases} \quad (9)$$

where $\alpha$ ($0 \leq \alpha \leq 1$) is the weighting assigned to $m_1(A)$.

Recall the example introduced in Section V, suppose expert $E_1$ has more knowledge and experience than expert $E_2$, and they are assigned with different weighting as $\alpha_1 = 0.9$ and $\alpha_2 = 0.4$, respectively. Using the discounting method in Equation (9), new bbas of the two experts are

$$m_1'(T) = 0.72, \quad m_1'(\overline{T}) = 0, \quad m_1'(U) = 0.28,$$
$$m_2'(T) = 0, \quad m_2'(\overline{T}) = 0.32, \quad m_2'(U) = 0.68.$$

Then apply Equation (6), (7), and (8), $\Delta BetP_{m_1}^{m_2}$, and $m_\oplus(\phi)$ of the two bbas can be calculated as

$$BetP_{m_1}'(T) = 0.86, \quad BetP_{m_1}'(\overline{T}) = 0.14, \quad BetP_{m_1}'(U) = 1,$$
$$BetP_{m_2}'(T) = 0.34, \quad BetP_{m_2}'(\overline{T}) = 0.66, \quad BetP_{m_2}'(U) = 1,$$
$$\Delta BetP_{m_1}'^{m_2} = 0.52, \quad m_\oplus'(\phi) = 0.23.$$

In this case, if the conflict tolerance is still set to $\epsilon = 0.6$ as in Section V-A, bbas from those two experts will no longer be recognised as in conflict, hence conflict avoided.

Another issue arising together with the use of weighting difference is how the weighting of each element can be assigned. In the absence of a completely objective weighting assignment method, Wang and Wulf [27] use the Analytic Hierarchy Process (AHP) to identify the importance of different elements. This approach can also be used in the trustworthiness assessment model to assign different weighting to different elements. However, due to limitations of space, we will not discuss it any further here. For details of this approach, readers can refer to [27].

After assigning different weighting to different elements, the calculation of the trustworthiness of a digital record (similar to Equation (5)) is

$$\begin{aligned} m_{record}(T) = m^{discounting}_{creation}(T) \oplus m^{discounting}_{modification}(T) \oplus \\ m^{discounting}_{migration}(T) \oplus m^{discounting}_{retrieval}(T) \oplus m^{discounting}_{disposal}(T) \\ = m^{discounting}_{Originator}(T) \oplus m^{discounting}_{Creator}(T) \oplus m^{discounting}_{CreationAction}(T) \\ \oplus \ldots \oplus m^{discounting}_{DisposalExecutor}(T) \oplus m^{discounting}_{DisposalAction}(T) \\ = m^{discounting}_{EKM_1}(T) \oplus \ldots \oplus m^{discounting}_{EKM_m}(T) \\ m_{record}(\overline{T}) = m^{discounting}_{EKM_1}(\overline{T}) \oplus \ldots \oplus m^{discounting}_{EKM_m}(\overline{T}) \\ m_{record}(U) = m^{discounting}_{EKM_1}(U) \oplus \ldots \oplus m^{discounting}_{EKM_m}(U) \end{aligned}$$

## VII. Dependency Aspect

In the trustworthiness assessment model, dependencies may exist in some pieces of the EKM. For instance, “Name of the Creator” and “Affiliation of the Creator” of a digital record are interrelated. Since Dempster’s rule of combination is based on independent evidence, it is not suitable for the combination of evidence from interrelated EKM. Thus, an alternative approach should be found to combine dependent EKM in the trustworthiness assessment model.

In this work, we adopt the weighted sum operator [16] as the alternative approach for combining dependent EKM for its applicability. Because the output of the weighted sum operator is still a basic belief assignment, it can be easily integrated into the trustworthiness assessment model.

The weighted sum operator ($\widehat{\oplus}$) is defined in Equation (10)

$$m_1 \widehat{\oplus} m_2(A) = \frac{w_1}{w_1 + w_2} m_1(A) + \frac{w_2}{w_1 + w_2} m_2(A), \quad \text{where } w_1, w_2 \geq 0. \tag{10}$$

In [17], when using the weighted sum operator, all dependent elements are equally weighted. While in our research, different weighting is assigned in the combination of dependent EKM. Note that the weighting here is different from the weighting in Section VI. The weighting in Section VI presents the importance of one element in the assessment of the trustworthiness of a digital record, whereas the weighting here denotes the different importance of dependent elements in the determination of their combined result, for example, in the assessment of the trustworthiness of a creator. In the case where the creator creates the record on behalf of his/her organisation, the affiliation should be recognised as more important. Thus, in the adoption of the weighted sum operator, the affiliation is heavily weighted, say $w_{name} = 2, w_{aff.} = 10$, for instance. In another case, the creator only creates a record for personal use, where the affiliation is recognised as less important, and thus, is less weighted, say $w_{name} = 10, w_{affiliation} = 4$.

To differentiate weighting for the weighted sum operator, the AHP method as mentioned in Section VI can also be used. In addition, users of the trustworthiness assessment model may want to assign weighting to EKM based on their different use.

After integrating the weighted sum operator into the trustworthiness assessment model, the calculation of the trustworthiness of a digital record (similar to Equation (5)) is

$$\begin{aligned} m_{record}(T) = m^{discounting}_{EKM_1}(T) \oplus \ldots \oplus (m_{EKM_i} \widehat{\oplus} \\ m_{EKM_j}(T))^{discounting} \oplus \ldots \oplus m^{discounting}_{EKM_m}(T) \\ m_{record}(\overline{T}) = m^{discounting}_{EKM_1}(\overline{T}) \oplus \ldots \oplus (m_{EKM_i} \widehat{\oplus} \\ m_{EKM_j}(\overline{T}))^{discounting} \oplus \ldots \oplus m^{discounting}_{EKM_m}(\overline{T}) \\ m_{record}(U) = m^{discounting}_{EKM_1}(U) \oplus \ldots \oplus (m_{EKM_i} \widehat{\oplus} \\ m_{EKM_j}(U))^{discounting} \oplus \ldots \oplus m^{discounting}_{EKM_m}(U) \end{aligned}$$

where $EKM_i$ and $EKM_j$ are interrelated EKM, combined using the weighted sum operator.

## VIII. Conclusion and Future Work

In this paper, we have described the time, conflict, weighting and dependency aspects in the assessment of the trustworthiness of digital records. We used the beta reputation system together with a forgetting factor to evaluate the reliability of records’ operators over time, which is used as the evidential value of the operators and is the value assigned to a basic belief assignments (bba), which is integrated into the assessment model. Proceeding on the basis of assigned conflict toleration, we detected conflicts between the evidence gained from different sources by examining two factors, the mass of the combined beliefs allocated to the empty set before normalisation, and the distance between betting commitments. Discounting is used to assign weighting differences and avoid conflicts in Evidence-Keeping Metadata (EKM). Finally, we used the weighted sum operator to combine dependent evidence. Because solutions to these four problems are all based on changes in the bbas, they are easily integrated into our model for the assessment of the trustworthiness of digital records.

Our results show that by adopting and carefully revising the reputation systems and the Dempster-Shafer (D-S) theory, they can be integrated in our model and improve the objective assessment of the trustworthiness of digital records over time.

In future work, we shall look into the verification and validation of the trustworthiness assessment results.

## References


[1] H. M. Gladney, "Trustworthy 100-year digital objects: Evidence after every witness is dead," *ACM Transaction on Information System (TOIS)*, vol. 22, no. 3, pp. 406–436, 2004.

[2] H. M. Gladney and R. A. Lorie, "Trustworthy 100-year digital objects: durable encoding for when it's too late to ask," *ACM Transaction on Information System (TOIS)*, vol. 23, no. 3, pp. 299–324, 2005.

[3] Center for Research Libraries, "Trustworthy repositories audit & certification: Criteria and checklist," Jul. 2008, [accessed 01-Apr-2009]. [Online]. Available: http://www.crl.edu/PDF/trac.pdf

[4] Consultative Committee for Space Data Systems, "Reference model for an open archival information system (OAIS)," National Aeronautics and Space Administration, Jan. 2002.

[5] J. Ma, H. Abie, T. Skramstad, and M. Nygård, "Assessment of the trustworthiness of digital records," in *Fifth IFIP WG 11.11 International Conference on Trust Management*, ser. IFIP Advances in Information and Communication Technology (AICT). Springer, Jun. 2011, pp. 300–311.

[6] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[7] B. Alhaqbani and C. Fidge, "A time-variant medical data trustworthiness assessment model," in *Proceedings of the 11th international conference on e-Health networking, applications and services*, 2009, pp. 130–137.

[8] A. Jøsang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th Bled Electronic Commerce Conference*, vol. 160, 2002, pp. 17–19.

[9] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th International World Wide Web Conference*. ACM Press, 2003, pp. 640–651.

[10] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Transaction on Knowledge and Data Engineering, IEEE Transactions on*, vol. 16, no. 7, pp. 843–857, 2004.

[11] P. Smets, "Analyzing the combination of conflicting belief functions," *Information Fusion*, vol. 8, no. 4, pp. 387–412, 2007.

[12] L. A. Zadeh, "A simple view of the dempster-shafer theory of evidence and its implication for the rule of combination," *AI Magazine*, vol. 7, no. 2, pp. 85–90, 1986.

[13] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system," *Advances in Applied Microeconomics: A Research Annual*, vol. 11, pp. 127–157, 2002.

[14] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision." *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[15] Y. L. Sun, Z. Han, W. Yu, and K. Liu, "Attacks on trust evaluation in distributed networks," in *Information Sciences and Systems, 2006 40th Annual Conference on*. IEEE, 2006, pp. 1461–1466.

[16] S. McClean and B. Scotney, "Using evidence theory for the integration of distributed databases," *International Journal of Intelligent Systems*, vol. 12, no. 10, pp. 763–776, Oct. 1997.

[17] X. Hong, C. D. Nugent, M. D. Mulvenna, S. I. McClean, B. W. Scotney, and S. Devlin, "Evidential fusion of sensor data for activity recognition in smart homes," *Pervasive and Mobile Computing*, vol. 5, no. 3, pp. 236–252, 2009.

[18] P. Smets, "The combination of evidence in the transferable belief model," *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 12, pp. 447–458, May 1990.

[19] D. Didler Dubois and H. Prade, "Representation and combination of uncertainty with belief functions and possibility measures," *Computational Intelligence*, vol. 4, no. 3, pp. 244–264, 1988.

[20] R. R. Yager, "On the dempster-shafer framework and new combination rules," *Information Sciences*, vol. 41, no. 2, pp. 93–137, 1987.

[21] A.-L. Jousselme, D. Grenier, and É. loi Bossé, "A new distance between two bodies of evidence," *Information Fusion*, vol. 2, no. 2, pp. 91–101, 2001.

[22] W. Liu, "Analyzing the degree of conflict among belief functions," *Artificial Intelligence*, vol. 170, no. 11, pp. 909–924, 2006.

[23] S. Ferson, R. Nelsen, J. Hajagos, D. Berleant, J. Zhang, W. Tucker, L. Ginzburg, and W. Oberkampf, "Dependence in probabilistic modeling, dempster-shafer theory, and probability bounds analysis," *Albuquerque, New Mexico: Sandia National Laboratories*, pp. 1–141, 2004.

[24] J. Ma, H. Abie, T. Skramstad, and M. Nygård, "Development and validation of requirements for evidential value for assessing trustworthiness of digital records over time," *Journal of Information*, (to appear).

[25] National Archives of Australia, "Australian government recordkeeping metadata standard," Tech. Rep., Jul. 2008, [accessed 01-Apr-2009]. [Online]. Available: http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm2-12630.pdf

[26] P. Smets, "Decision making in the tbm: the necessity of the pignistic transformation," *International Journal of Approximate Reasoning*, vol. 38, no. 2, pp. 133–147, 2005.

[27] C. Wang and W. A. Wulf, "Towards a framework for security measurement," in *20th NIST-NCSC National Information Systems Security Conference*, 1997, pp. 522–533.


Copyright (c) IARIA, 2011. ISBN: 978-1-61208-149-6