A Granular Approach to Source Trustworthiness for Negative Trust Assessment

Davide Ceolin[1](✉) and Giuseppe Primiero[2]

[1] Centrum Wiskunde & Informatica, Amsterdam, The Netherlands
Davide.Ceolin@cwi.nl
[2] Department of Philosophy, University of Milan, Milan, Italy
Giuseppe.Primiero@unimi.it

Abstract. The problem of determining what information to trust is crucial in many contexts that admit uncertainty and polarization. In this paper, we propose a method to systematically reason on the trustworthiness of sources. While not aiming at establishing their veracity, the method allows creating a relative reference system to determine the trustworthiness of information sources by reasoning on their knowledgeability, popularity, and reputation. We further propose a formal rule-based set of strategies to establish possibly negative trust on contradictory contents that use such source evaluation. The strategies answer to criteria of higher trustworthiness score, majority or consensus on the set of sources. We evaluate our model through a real-case scenario.

1 Introduction

Assessing information quality is a challenging task. Assuming a minimal definition of information as ‘data + semantics’, assessing its quality means to establish fitness for purpose for a given piece of information. Given the huge number of possible purposes and to make its computation feasible, information quality is often broken down into ‘dimensions’ [13], like accuracy, precision, completeness. Despite its complexity, humans deal with quality on a daily basis using heuristics to approximate ideal values and using them as a proxy for deciding whether to trust information or not. Notwithstanding the possibility of being deceived by our heuristics, a formalization of such strategies is a useful tool for understanding and prediction. We provide here a framework to mimic such strategies and a relative reference system of sources. When an oracle or fact-checking service is available, such a reference system can be turned into an absolute one, i.e., determining which sources are veracious and which not. Otherwise, our result will still provide a relative ranking of the importance of sources. This task relies on providing appropriate understandings of trust and trustworthiness.

Among the large number of its definitions in the literature, for our purpose trust on contents can be minimally identified with the result of a consistency

Published by Springer Nature Switzerland AG 2019
W. Meng et al. (Eds.): IFIPTM 2019, IFIP AICT 563, pp. 108–121, 2019.
https://doi.org/10.1007/978-3-030-33716-2_9

assessment: a piece of information consistent with the agent's current set of beliefs or knowledge base is trusted when it allows to preserve other information considered truthful. This approach requires a methodology to deal with inconsistent information and it calls upon the problem of assessing source trustworthiness. The logic (`un`)`SecureND` [20] provides a mechanism to deal with this aspect through the introduction of separate protocols to deal with failing consistency. An agent A reading a piece of information ϕ from an agent B, where ϕ is inconsistent with A's knowledge base, has two possibilities: (1) *distrust*: to reject ϕ and preserve $\neg\phi$ and its consequences; and (2) *mistrust*: to remove $\neg\phi$ from her profile and to accept ϕ. (`un`)`SecureND` does not have a selection mechanism for either form of negated trust. In real case scenarios, the choice between distrust and mistrust will be determined by evaluating the source. While *trust* is the mechanism to establish admissible consistent information, we call *trustworthiness* the assessment quality on sources. We introduce an ordering function and several decision strategies aiming at providing computational mechanisms to mimic the subjective quality assessment process called *trustworthiness*. Through any of these mechanisms, A can decide whether the estimated trustworthiness of B is high enough to trust the new information ϕ. Consider a simplified scenario, with a finite set of sources sharing information on a common topic and referencing each other (to a lesser or greater degree): some of them will be in conflict and some will be consistent with one another. We identify three dimensions:

- *Knowledgeability*: the number of sources to whom a source B refers. This value is used as an indicator of B's knowledge of other views;
- *Popularity*: the number of sources referring to B. This counts the number of inbound links, and it does not involve their polarity. Citing a source, even to attack it, is seen as an indication of the popularity of the latter;
- *Reputation*: the proportion between positive and negative evaluations of B.

These dimensions are used for assessing the trustworthiness of B, to compare contradictory sources by a receiver, and to formulate decision strategies.

The paper continues as follows. Section 2 describes formal preliminaries, Sect. 3 describes the different strategies available to resolve the presence of contradictory contents, Sect. 4 translates these strategies in implementable rule-based protocols, Sects. 5 and 6 present and discuss a use case implementation of the proposed logic. Section 7 surveys related work, and Sect. 8 concludes.

2 Formal Preliminaries

Consider a set of sources $\mathcal{S}$ and a (possibly partial) order relation $\leq_t$ over sources $\mathcal{S} \times \mathcal{S}$ expressing source trustworthiness; once defined, this is used as a proxy to establish trust in contents in the rule-based semantics presented in Sect. 4. We define the trustworthiness order $\leq_t$ as a function over three dimensions: reputation, popularity, and knowledgeability.

Reputation is an order relation $\leq_R$ over sources $\mathcal{S} \times \mathcal{S}$: intuitively, $S \leq_R S'$ means that source $S \in \mathcal{S}$ has at least the same reputation as $S' \in \mathcal{S}$. For simplicity, reputation is evaluated on the following criteria:

- we denote with $w(S)_{S'}$ a fixed weight of S received by S';
- $w = \{1, -1\}$, respectively for a positive and a negative assessment;
- we denote each $w(S)_{S'} = 1$ as *pos* and each $w(S)_{S'} = -1$ as *neg*;
- for any source $S \in \mathcal{S}$, a reputation assessment $r(S)$ by other sources in $\mathcal{S}$ is

$$r(S) = \frac{|pos| + 1}{|pos| + |neg| + 2}$$

We note that instead of computing the simple ratio of positive assessments over the total number of assessments, we add a smoothing factor like in Subjective Logic [15]. This allows us to represent assessment as performed in a 'semi-closed world': we base ourselves on the evidence at our disposal, but our sample is limited. The smaller our sample, the more the resulting reputation will be close to the neutral prior 0.5, since no prior knowledge is available to believe the source is fully trustworthy or untrustworthy. The larger our sample, the more the weight of the sample ratio will count on the reputation estimation. On the basis of the reputation assessment, we establish the corresponding order on $\mathcal{S}$:

Definition 1 (Reputation). *For any* $S, S' \in \mathcal{S}, S \leq_R S' \leftrightarrow r(S) \geq r(S')$

A second-order relation $\leq_P$ over sources $\mathcal{S} \times \mathcal{S}$ is defined: intuitively, $S \leq_P S'$ means source S has at least the same popularity as S', where popularity reflects the number of sources which refer to S. We denote the referenced sources as *outbound_links* and the referencing sources as *inbound_links*; non-referenced or non-referencing sources are denoted as *missing_links*. Note that $\forall S, S'$, if $S \in$ *outbound_links*(S') and $S' \in$ *outbound_links*(S), we can assume both sources have explicit knowledge of each other's information. We assume this fact and express that S' reads from S (or alternatively that S writes to S') as $S' \in$ *outbound_links*(S). Note that in the calculus presented in Fig. 1 these access operations are explicit. By our definition of reputation, we can assume that for every source S referenced by S', $w(S)_{S'} \in r(S)$. Hence, the popularity of S is

$$p(S) = \frac{|inbound\_links| + 1}{|inbound\_links| + |missing\_links| + 2}$$

On its basis, we establish the corresponding order on $\mathcal{S}$:

Definition 2 (Popularity). *For any* $S, S' \in \mathcal{S}, S \leq_P S' \leftrightarrow p(S) \geq p(S')$.

Finally, we define a third order relation $\leq_K$ over sources $\mathcal{S} \times \mathcal{S}$: intuitively, $S \leq_K S'$ means that source S has at least the same knowledgeability as S', where knowledgeability reflects the number of sources to which S refers. For simplicity, given the definition of $p(S)$ based on $r(S)$, knowledgeability $k(S)$ is the inverse of $p(S)$, computed as

$$k(S) = \frac{|outbound\_links| + 1}{|outbound\_links| + |missing\_links| + 2}$$

On its basis, we establish the corresponding order on $\mathcal{S}$:

Definition 3 (Knowledgeability). *For any $S, S' \in \mathcal{S}, S \leq_K S' \leftrightarrow k(S) \geq k(S')$.*

The highest value of knowledgeability corresponds to the totality of the available sources. For simplicity, we include in this count the source itself:

Definition 4 (Source Completeness). *A source S satisfies source completeness if $|outbound\_links| = |\mathcal{S}|$.*

The three dimensions of reputation, popularity, and knowledgeability establish a generic computable metric on the trustworthiness of a source S:

Definition 5 (Source Trustworthiness). *Source trustworthiness is computed*

$$t(S) = \Phi(\phi(r(S)), \psi(p(S)), \xi(k(S)))$$

with Φ a given function and ϕ, ψ, ξ appropriate weights on the parameters.

The choice of ϕ, ψ, ξ is essentially contextual, as it determines the role that each parameter has in the computed value of $t(s)$, e.g. to stress knowledgeability as more important than popularity, or reputation as more relevant than knowledgeability. Fixing these parameters to 1 provides the basic evaluation with all equipollent values. Φ can be interpreted e.g. as $\sum X$, $\overline{X}$, $max(X)$: again, this choice can be contextually determined.

To distinguish between different semantic strategies for information conflict resolution, we first weight the notion of source trustworthiness with respect to source order and calculate an average value.

Definition 6 (Sources with Higher Trustworthiness). *Let $\mathcal{S}^{\sim}_{<_t S}$ denote the set of sources with higher trustworthiness $<_t$ than a given source $S \in \mathcal{S}$.*

We now partition this set as follows: we denote with $\mathcal{T}$ the subset of $\mathcal{S}^{\sim}_{<_t S}$ such that $\forall S' \in \mathcal{T}$, S' trusts information ϕ; we denote with $\mathcal{T}_{\perp}$ the complement of $\mathcal{T}$.

Definition 7 (Weighted Trustworthiness). *Average trustworthiness of $\mathcal{T}$ is*

$$t(\mathcal{T}) = \frac{\sum_{\forall S' \in \mathcal{T}}^{|\mathcal{T}|} t(S')}{|\mathcal{T}|}$$

Let $t(\mathcal{T}_{\perp})$ denote the average trustworthiness for the complement partition. If $t(\mathcal{T}) > t(\mathcal{T}_{\perp})$, then S trusts ϕ, else S trusts $\neg\phi$.

In the case of weighted trustworthiness there is a possible parity outcome: either the selection of a different strategy (e.g., the simpler majority trustworthiness) or a random assignment is possible. Finally, on the basis of the trustworthiness assessment, we establish the corresponding order on $\mathcal{S}$:

Definition 8 (Trustworthiness). *For any $S, S' \in \mathcal{S}, S \leq_t S' \leftrightarrow t(S) \geq t(S')$.*

Note that the general definition allows for a partial order, as it is possible that the trustworthiness values of two distinct sources be equivalent or incomparable. The following resolution strategies assume that a strict order is being obtained.

3 Trustworthiness Selection Strategies

We define several strategies to implement negative trust based on the Trustworthiness relation defined in Sect. 2. Recall that distrust requires an agent to reject incoming contradictory information in favor of currently held data. In this context, we establish such a choice on the basis of higher trustworthiness.

Definition 9 (Distrust). *Assume $S <_t S'$, $S \in outbound\_links(S')$. If S' trusts ϕ and ϕ is inconsistent with the profile of S, then S distrust ϕ and trusts $\neg\phi$.*

With this protocol in place, a source with a higher trustworthiness will always reject incoming contradictory information from a lower ranked source. It is also fair to assume that where $t(S) = t(S')$, a conservative source S will not change its current information. The process of modifying currently held information to accommodate for newly incoming one (mistrust) starts therefore on the assumption that the source of incoming information has lower trustworthiness degree than the receiver. On this basis, implementing a mistrust strategy has a complex dynamic: the user can be more or less inclined to a belief change and it can require more or less evidence for it to happen. Therefore, different strategies can be designed. One strategy requires that a *majority* of agents with higher trustworthiness agree on the new incoming data. A stronger strategy requires that the *totality* of agents with higher trustworthiness agree. Reaching the desired number of agents to implement a mistrust strategy might be a dynamic process resulting from a temporally extended analysis of the set of sources. We design the different strategies assuming Definition 6 of the subset $\mathcal{S}^{\sim}_{<_t S}$ of sources with higher trustworthiness as the sources which the receiver S has to consider.

The weakest strategy is defined by an agent which allows for a mistrust operation based on the presence of *at least one* source with higher reputation that contradicts her current belief state:

Definition 10 (Weak Trustworthiness). *If $\exists S' \in \mathcal{S}^{\sim}_{<_t S}$ such that S' trusts information ϕ, then S trusts ϕ.*

To accommodate a contradicting ϕ, the source S has to modify the current set of belief, Γ, to some subset Γ' which can be consistently extended with ϕ, i.e. removing any formula implying $\neg\phi$. A stronger strategy is for the agent to accept the content on which the majority of sources with higher trustworthiness agree:

Definition 11 (Majority Trustworthiness). *Assume $\mathcal{T} \subseteq \mathcal{S}^{\sim}_{<_t S}$ such that $\forall S' \in \mathcal{T}$, S' trusts information ϕ. We denote with $\mathcal{T}_{\perp}$ the complement of $\mathcal{T}$. If $|\mathcal{T}| > |\mathcal{T}_{\perp}|$, then S trusts ϕ, else S trusts $\neg\phi$.*

In the case of a parity outcome, either the selection of a different strategy or a random assignment are possible. Note that the above strategy does not account for the order *within* the subset $\mathcal{S}^{\sim}_{<_t S}$: it only partitions it according to the truth value of a formula and then selects the partition with higher cardinality. A more refined majority strategy will weight each member $S' \in \mathcal{T}$ and $\mathcal{T}_{\perp}$ on the basis of their trustworthiness value $t(S')$. Then an average value will be assigned to the corresponding partition and the strategy will select the formula held by the partition with a higher value. If the cardinality of the partition has to be considered, the sum of the trustworthiness values of the sources can be assigned to each partition. The strongest strategy requires the agent to change her mind if all other agents with higher trustworthiness agree:

Definition 12 (Complete Trustworthiness). *If* $\forall S' \in \mathcal{S}^{\sim}_{<_t S}$, *$S'$ trusts information ϕ, then S trusts ϕ.*

The Majority and Complete Trustworthiness strategies above have a strong effect on knowledge diffusion in the presence of full communication. The Consensus rule below holds even if the content from the most trustworthy source is not initially held by the majority of agents.

Proposition 1 (Consensus). *Assume $S' \in outbound\_links(S)$ holds $\forall S < S' \in \mathcal{S}^{\sim}$. Then $\mathcal{S}$ converges towards consensus on the information trusted by the most trustworthy source.*

4 Rule-Based Semantics for the Strategies

The natural deduction calculus (`un`)`SecureND` [20] defines trust, mistrust and distrust protocols according to the informal semantics described in Sect. 1. It formalizes a derivability relation on formulas from sets of assumptions (contexts) as accessibility on resources issued by sources. In this section, we provide an extension of the calculus with a rule-based implementation of the trustworthiness selection strategies from Sect. 3.

Definition 13 (Syntax of (`un`)`SecureND`**).**

$$
\begin{aligned}
&\mathcal{S}^{\sim} := \{A <_t B <_t \cdots <_t N\}\\
&BF^S := a^S \mid \phi_1^S \rightarrow \phi_2^S \mid \phi_1^S \wedge \phi_2^S \mid \phi_1^S \vee \phi_2^S \mid \bot\\
&mode := Read(BF^S) \mid Write(BF^S) \mid Trust(BF^S)\\
&RES^S := BF^S \mid mode \mid \neg RES^S\\
&\Gamma^S := \{\phi_1^S, \dots, \phi_n^S\}
\end{aligned}
$$

Every $S \in \mathcal{S}$ is a content producer which has a trustworthiness value based on its interactions with any other $S' \in \mathcal{S}$. Any $S \in \mathcal{S}$ is ordered with respect to the others by the trustworthiness order.[1] Formulas in the set BF^S express content produced by source S and they are closed under logical connectives. Functions on contents in the set *mode* refer to reading, writing and trusting formulas. Every source S is identified by the set of contents it produces, denoted by Γ^S called the profile of S. A formula expresses access from a source S to content issued by another source S' (metavariables S, S' are substituted by variables A, B):

[1] In other versions of this logic, the order between elements in $\mathcal{S}$ is differently defined, e.g. imposed by access policies, see e.g. [20,22,23].

Definition 14. *An* (un)`SecureND`*-formula* $\Gamma^A \vdash RES^B$ *says that under the content expressed by source A, some content from source B is validly accessed.*

The rule-based semantics of the calculus is given in Fig. 1. *Atom* establishes derivability of formulas from well-formed contexts and under consistency preserving extensions. We use the judgment $\Gamma : profile$ for a profile consistently construed by induction from the empty set. For brevity, we skip here the introduction and elimination rules for logical connectives, see [20] and focus only on the access rules. Differently from other versions of the same calculus, we drop here negation-completeness: a source without access to a content item from another source, will not assume access to its negation, i.e. uncertainty is admissible. *read* says that from any well-formed source profile A, formulas from a profile B can be read. *trust* says that if a content item is read and it preserves consistency when added to the reading profile, then it can be trusted. *write* says that a readable and trustable content can be written. By *distrust*, source A distrusts content ϕ^B if it induces contradiction when reading from Γ^A and A has higher trustworthiness than B. Its elimination uses →-introduction to induce *write* from the receiver profile for any content that follows a distrust operation. This allows $Write(\neg\phi^B)$ when $\neg Trust(\phi^B)$ holds. Each of the *mistrust* rules applies one different strategy from Sect. 3 for a content item ϕ^B inducing contradiction when reading from Γ^A and A has lower trustworthiness than B. By *weak mistrust*, A accepts ϕ (and removes from its own profile any conflicting information) by the simple presence of B in the set of sources with a higher reputation of A: this formulation is general enough to accommodate for the substitution of B in this condition by any other source that A considers absolutely essential (appeal to authority). *majority mistrust* requires computing the partitions of the set of sources with higher trustworthiness than A and comparing their cardinality: *any* content ϕ held by the larger partition will be kept by A (even when this reduces to an application of a *distrust* rule). In *weighted majority*, the condition is expressed by the higher average reputation of the partition. By *complete mistrust* the source A requires that every element in the set of sources with higher reputation agrees on ϕ. By the rule *write*, every trusted content can be written.

5 Evaluation

5.1 Use Case Description

In 2015, a measles outbreak took place in Disneyland, California. This event received much attention online, and a quite strongly polarised discussion followed up the news regarding this event. Public authorities and pro-vaccination sources pointed out the importance of vaccination, and some of them blamed the low vaccination rate as the main reason for this outbreak. On the other hand, the anti-vaccination movement accused the government agencies and the provaccination movement of misinforming the public, since the children involved in the outbreak were vaccinated. Two main factions are at work, the pro and the

$$\frac{\Gamma^A : \mathit{profile} \qquad \Gamma^A;\Gamma^B : \mathit{profile}}{\Gamma^A;\Gamma^B \vdash \phi^B}\ \text{Atom, for any } \phi \in \Gamma^B$$

$$\frac{}{\Gamma^A \vdash \mathit{Read}(\phi^B)}\ \mathit{read} \qquad \frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi_i^B : \mathit{profile}}{\Gamma^A \vdash \mathit{Trust}(\phi_i^B)}\ \mathit{trust}$$

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi^B \vdash \bot \qquad A <_t B}{\Gamma^A \vdash \neg \mathit{Trust}(\phi^B)}\ \mathit{distrust}$$

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi^B \vdash \bot \qquad \Delta^{B <_t A} \vdash \phi}{\Gamma'^A \vdash \mathit{Trust}(\phi^B)}\ \mathit{weak\ mistrust}, \text{ for some } \Gamma^A \supset \Gamma'^A;\phi^B \vdash wf$$

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi^B \vdash \bot \qquad \Delta^{\mathcal{T}} \vdash \phi}{\Gamma'^A \vdash \mathit{Trust}(\phi^B)}\ \mathit{majority\ mistrust}, \text{ for some } \Gamma^A \supset \Gamma'^A;\phi^B \vdash wf$$

with $\mathcal{T} \subset \mathcal{S}^{\sim}_{<_t A}$ s.t. $|\mathcal{T}| > |\mathcal{T}_\bot|$.

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi^B \vdash \bot \qquad \Delta^{\mathcal{T}} \vdash \phi}{\Gamma'^A \vdash \mathit{Trust}(\phi^B)}\ \mathit{weighted\ mistrust}, \text{ for some } \Gamma^A \supset \Gamma'^A;\phi^B \vdash wf$$

with $\mathcal{T} \subset \mathcal{S}^{\sim}_{<_t A}$ s.t. $t(\mathcal{T}) > t(\mathcal{T}_\bot)$.

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A;\phi^B \vdash \bot \qquad \Delta^{\mathcal{S}^{\sim}_{<_t A}} \vdash \phi}{\Gamma'^A \vdash \mathit{Trust}(\phi^B)}\ \mathit{complete\ mistrust}, \text{ for some } \Gamma^A \supset \Gamma'^A;\phi^B \vdash wf$$

$$\frac{\Gamma^A \vdash \mathit{Read}(\phi^B) \qquad \Gamma^A \vdash \mathit{Trust}(\phi^B)}{\Gamma^A \vdash \mathit{Write}(\phi^B)}\ \mathit{write}$$

Fig. 1. The system `(un)SecureND`: access rules.

anti vaccinations. While sources do not always identify themselves as part of one or the other, for many of them it is either clear what their stance is (e.g., when they explicitly ‘attack’ each other), or we can make safe assumptions based on our background knowledge (e.g., by assuming that authorities are pro vaccinations). We have at our disposal a set of assessments of these articles collected by means of user studies involving experts [6]. These assessments cover quality dimensions like accuracy and prediction, and present an overall quality score that is equivalent to the trustworthiness score defined here.

5.2 Data Preprocessing

We select a subset of 10 articles regarding this debate from a corpus of documents regarding the Disneyland measles outbreak[2]. The selection gives a small but diverse set of views on the topic in terms of stance (pro or anti vaccinations) and type of document (news article, official document, blog post, etc.). Provided

[2] The dataset is available online at https://goo.gl/aouDJH.

they all discuss the specific event selected, a clear network of references emerges. However, such a network is rather sparse since a large majority of these sources do not cite each other. As we are interested in capturing their polarity to compute the three trustworthiness dimensions, we reconstruct the network as follows: (1) a source criticizing another source is considered as a negative piece of evidence regarding the reputation of the source mentioned; and (2) a source citing data from another source, even in neutral terms, is considered a piece of evidence regarding the popularity of the source cited. The resulting network of references is represented in Fig. 2 and it illustrates only the relations emerging from the corpus considered, representing a partial view on the real scenario because we derive a source's trustworthiness using one or more documents published by it as a proxy; the more documents we observe from a source, the better we can assess its trustworthiness value. For example, we estimate the source knowledgeability from the number of citations of other sources. Some sources could be cited only in some articles by the source under consideration. Also, we derive a source's trustworthiness based on the references it receives from the other sources considered, but we know that the set of sources is limited, and the scenario might change when considering other sources (e.g., the number of citations of currently poorly cited sources could rise). Given these considerations, the smoothing factor added to Definitions 1, 2, and 3, helps to cope with the resulting uncertainty.

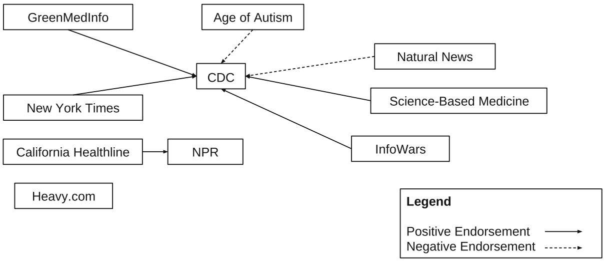

Fig. 2. Network of references resulting from the preprocessing of our corpus. Directed arrows indicate positive (continuous line) or negative (dotted line) references.

5.3 Sources Ordering

Based on the network depicted in Fig. 2, and using the formulas presented in Sect. 2, we compute the trustworthiness score for each of the sources in our sample. The trustworthiness score is computed by averaging the reputation, the knowledgeability, and the popularity of the sources, resulting in the scores reported in Table 1. Figure 3 shows a graphical representation of the resulting hierarchy of sources. Since the trustworthiness thus obtained shows a weak correlation (0.2) with the overall scores provided by the users in the user study, we explore alternative ways to aggregate the scores.

Weighted Trustworthiness. Applying weights to the trustworthiness parameters can yield a different hierarchy. Instead of applying an arbitrary weighing

Table 1. Trustworthiness scores of the sources considered for our use case. The score is computed by means of a simple average, where each component has the same weight.

Source	Reputation	Knowledgeability	Popularity	Trustworthiness
California Healthline	0.50	0.17	0.08	0.25
CDC	0.63	0.08	0.67	0.46
NYTimes	0.50	0.17	0.08	0.25
InfoWars	0.50	0.17	0.08	0.25
GreenMedInfo	0.50	0.25	0.08	0.28
Age of Autism	0.67	0.17	0.17	0.33
Science-Based Medicine	0.50	0.17	0.08	0.25
Heavy.com	0.50	0.08	0.08	0.22
Natural News	0.50	0.17	0.08	0.25
NPR	0.67	0.08	0.17	0.31

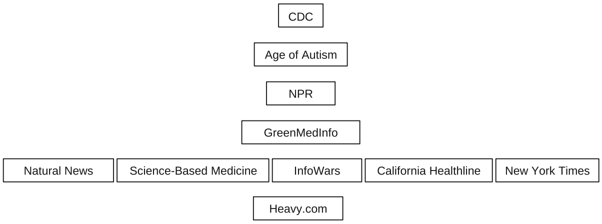

Fig. 3. Hierarchical ordering of the sources derived from the scores shown in Table 1

to the scores, we apply linear regression on the parameters, targeting the overall quality scores provided by the users in the study. Once we learn the weights for the parameters, we compute the trustworthiness scores. The resulting scores show a 0.6 correlation with those provided by the users. Moreover, we also run 3-fold cross-validation (split the dataset into 3 parts and, in round, use two parts as a training set for linear regression, and one for validation). For one item only, our model is unable to make a prediction. Excluding such item, the resulting average correlation between predicted and user-provided overall quality is −0.87 (Pearson) and −0.76 (Spearman). We consider these as promising results.

5.4 Applying Trustworthiness Selection Strategies

Here we illustrate how users could apply the selection strategies described in Sect. 3. Figure 4 shows the scenario where the trustworthiness selection strategies are applied. The sources analyzed in the previous step are now shown in white if they present a positive stance with respect to vaccinations, in grey otherwise. C is a new source with an unclear stance that joins the scenario. The stance of C (i.e., whether C *trusts* vaccines or not) will be determined by comparison with the other sources. Assume that the trustworthiness of C is higher than that of Heavy.com, but lower than the trustworthiness of all the other sources.

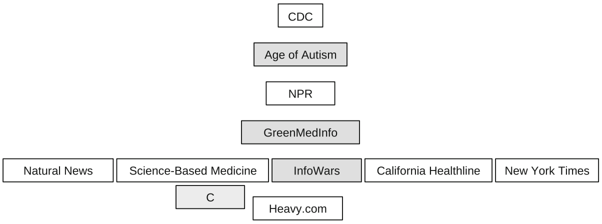

Fig. 4. Use case scenario. We adopt the same hierarchy as in Fig. 3. Sources in white trust vaccinations. Sources in grey do not. C denotes an additional source which takes part in the scenario and has not yet a clear stance.

Distrust. When C is confronted with Heavy.com and its lower trustworthiness score, following the distrust rule it will *distrust* vaccines.

Weak Trustworthiness. Let us follow up on the previous scenario. C now *distrusts* vaccines. When encountering all the other sources, if the `weak mistrust` strategy is applied, C will revise its profile: now C *trusts* vaccines because of several sources with trustworthiness higher than C *trust* ϕ. Note that `weak mistrust` requires at least one source to trust ϕ in order to follow suit.

Majority Trustworthiness. In an alternative scenario, when encountering the other sources, C can evaluate whether to trust ϕ or not based on whether the majority of the sources trusts vaccines. We partition the sources based on *vaccines* and $\neg$*vaccines*. With any strategy for determining the majority (partition cardinality, average trustworthiness of the sources in the two partitions, sum of the cardinalities in the two partitions), *trust* in vaccines prevails.

Complete Trustworthiness. When complete trustworthiness is applied, C needs all the sources to agree on vaccines to add it to its profile. Since three sources disagree, by applying this rule, we obtain that C *d*istrusts vaccines.

6 Discussion

The goal of our model is to provide means to mimic human thinking and provide a tool to systematically reason upon sources. The result of such reasoning is a relative reference system of sources. When oracles, fact-checkers, and other sources are available, such a reference system can be turned into an absolute one: if the user knows that a given set of statements is true or false, she can reason about the trustworthiness of the sources incorporating this additional information in the networks. When oracles are not available, the reference system can provide the user with a basis to coherently reason upon the sources she observes.

Frameworks like PageRank and its successors can be considered more evolved and successful alternatives to the present proposal. While PageRank can be applied to one or more networks to rank their sources, our system considers three distinct networks, aggregates them, and can be either extended with other networks or be used as reasoning support as it is. Hence we consider the present a viable complement to existing approaches.

While assessing the veracity of information is not the focal point of our system, the multidimensional approach we take shows promising robustness to possible attacks. Suppose that in an echo-chamber, sources cite each other positively in order to increase their own reputation and popularity. If their citations are limited to the sources in the echo chamber, their knowledgeability (and, thus, their trustworthiness) will necessarily be low. If to remedy this sources start citing others outside the echo chamber, their knowledgeability will rise, but they will also contribute to the popularity of these external sources. Still, vulnerability to the knowledgeability score is possible in sufficiently large echo chambers. Future developments will tackle this aspect more explicitly.

7 Related Work

Assessing the quality of information sources is a long-standing problem largely addressed in the fields of humanities, where specific guidelines and checklists have been proposed to address the issue of "source criticism" [3]. Such work has also been extended to Web sources in [6,7], where a combination of crowdsourcing and machine learning is adopted. Those works are complementary to the present contribution since they do not compare directly the references among sources. Counting links for a source as employed in this paper aims at mimicking the evaluation of the bibliography mentioned in the source criticism checklist. Another framework based on crowdsourcing is presented in [17].

Using fitness for purpose to assess information quality is a widely adopted strategy, see [12,13]. In the present work, we start from the assumption that where it is unclear or impossible for an agent to distinguish between contradictory data, source assessment based on trustworthiness is a valuable strategy. We show how such a protocol can be implemented through different selection strategies. A related topic is the one of fake news, tackled for instance in [4,25].

Research on trust in computational domains has been extensive in the last decades. Crucial aspects of the behavior of trust concern properties like propagation and blocking [8,10,14,16]. Solutions to these problems are various [2,9,11]. In the present work, we evaluate trust in information sources not on an absolute scale, but rather with varying degrees. A related approach is presented in [19], where a trust measure on agents is combined with the use of argumentation for reasoning about beliefs. Similarly, we propose a trust evaluation of sources to decide which information to maintain. The logic used in this work originates from a model designed to model trust in resource access control scenario, and to be able to block trust transitivity by design [21,23]. The logic has been applied to the Minimally Trusted Install Problem software management in [5], its negative counterpart [22], and tested to investigate optimal strategies to minimize false information diffusion [24]. For other accounts of negative trust, see [1,18].

8 Conclusion

In this paper, we presented an extension of (un)SecureND, a logic modeling trust on information, with strategies for assessing the trustworthiness of sources as a function (average or otherwise) of their knowledgeability, popularity, and reputation, possibly weighted. We evaluated this extension on a real-life case study on the trustworthiness of Web sources and applied the selection strategies to the resulting source hierarchy. We showed that a linear combination of these parameters presents a decent correlation with user-provided assessments.

We plan to extend this work in two main directions. First, we will work on the automation of the preprocessing phase. We expect to use natural language processing for this and, in particular, author attribution to systematically identify references among the sources, and textual entailment to capture the perspectives taken by the different sources. Second, we will improve the parameters considered for assessing the trustworthiness. For instance, knowledgeability will have to be assessed based on the estimated level of the truthfulness of the statements made by the source. We plan to run an exhaustive user study to guide the design of source trustworthiness assessment and selection. Lastly, we will experiment with network centrality measures as alternative indicators for these parameters.

References

1. Abdul-Rahman, A.: A framework for decentralised trust reasoning. Ph.D. thesis, Department of Computer Science, University College London (2005)
2. Abdul-Rahman, A., Hailes, S.: A distributed trust model. In: NSPW, pp. 48–60 (1997)
3. American Library Association: Evaluating information: a basic checklist (1994)
4. Bessi, A., Coletto, M., Davidescu, G., Scala, A., Caldarelli, G., Quattrociocchi, W.: Science vs conspiracy: collective narratives in the age of misinformation. PLoS One **2**, e0118093 (2015)
5. Boender, J., Primiero, G., Raimondi, F.: Minimizing transitive trust threats in software management systems. In: PST, pp. 191–198. IEEE (2015)
6. Ceolin, D., Noordegraaf, J., Aroyo, L.: Capturing the ineffable: collecting, analysing, and automating web document quality assessments. In: Blomqvist, E., Ciancarini, P., Poggi, F., Vitali, F. (eds.) EKAW 2016. LNCS (LNAI), vol. 10024, pp. 83–97. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49004-5_6
7. Ceolin, D., Noordegraaf, J., Aroyo, L., van Son, C.: Towards web documents quality assessment for digital humanities scholars. WebSci **2016**, 315–317 (2016)
8. Chakraborty, P.S., Karform, S.: Designing trust propagation algorithms based on simple multiplicative strategy for social networks. Procedia Technol. **6**, 534–539 (2012). iCCCS-2012
9. Chapin, P.C., Skalka, C., Wang, X.S.: Authorization in trust management: features and foundations. ACM Comput. Surv. **40**(3), 9 (2008)

10. Christianson, B., Harbison, W.S.: Why isn't trust transitive? In: Lomas, M. (ed.) Security Protocols 1996. LNCS, vol. 1189, pp. 171–176. Springer, Heidelberg (1997). https://doi.org/10.1007/3-540-62494-5_16
11. Clarke, S., Christianson, B., Xiao, H.: Trust*: using local guarantees to extend the reach of trust. In: Christianson, B., Malcolm, J.A., Matyáš, V., Roe, M. (eds.) Security Protocols 2009. LNCS, vol. 7028, pp. 171–178. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36213-2_21
12. Floridi, L., Illari, P. (eds.): The Philosophy of Information Quality. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07121-3
13. Illari, P.: IQ: purpose and dimensions. In: Floridi, L., Illari, P. (eds.) The Philosophy of Information Quality. SL, vol. 358, pp. 281–301. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07121-3_14
14. Jamali, M., Ester, M.: A matrix factorization technique with trust propagation for recommendation in social networks. In: RecSys, pp. 135–142. ACM (2010)
15. Jøsang, A.: Subjective Logic - A Formalism for Reasoning Under Uncertainty. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-42337-1
16. Jøsang, A., Marsh, S., Pope, S.: Exploring different types of trust propagation. In: Stølen, K., Winsborough, W.H., Martinelli, F., Massacci, F. (eds.) iTrust 2006. LNCS, vol. 3986, pp. 179–192. Springer, Heidelberg (2006). https://doi.org/10.1007/11755593_14
17. Lee, Y.W., Strong, D.M., Kahn, B.K., Wang, R.Y.: AIMQ: a methodology for information quality assessment. Inf. Manag. **40**(2), 133–146 (2002)
18. Marsh, S., Dibben, M.R.: Trust, untrust, distrust and mistrust – an exploration of the dark(er) side. In: Herrmann, P., Issarny, V., Shiu, S. (eds.) iTrust 2005. LNCS, vol. 3477, pp. 17–33. Springer, Heidelberg (2005). https://doi.org/10.1007/11429760_2
19. Parsons, S., Tang, Y., Sklar, E., McBurney, P., Cai, K.: Argumentation-based reasoning in agents with varying degrees of trust. In: AAMAS, pp. 879–886 (2011)
20. Primiero, G.: A calculus for distrust and mistrust. In: Habib, S.M.M., Vassileva, J., Mauw, S., Mühlhäuser, M. (eds.) IFIPTM 2016. IAICT, vol. 473, pp. 183–190. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-41354-9_15
21. Primiero, G., Boender, J.: Managing software uninstall with negative trust. In: Steghöfer, J.-P., Esfandiari, B. (eds.) IFIPTM 2017. IAICT, vol. 505, pp. 79–93. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59171-1_7
22. Primiero, G., Boender, J.: Negative trust for conflict resolution in software management. Web Intell. **16**(4), 251–271 (2018)
23. Primiero, G., Raimondi, F.: A typed natural deduction calculus to reason about secure trust. In: PST, pp. 379–382. IEEE (2014)
24. Primiero, G., Raimondi, F., Bottone, M., Tagliabue, J.: Trust and distrust in contradictory information transmission. Appl. Netw. Sci. **2**, 12 (2017)
25. Zhang, A.X., et al.: A structured response to misinformation: defining and annotating credibility indicators in news articles. In: WWW 18 Companion (2018)

A Fair (t, n)-Threshold Secret Sharing Scheme with Efficient Cheater Identifying

Hua Shen[1], Daijie Sun[1], Lan Zhao[1], and Mingwu Zhang[1,2](✉)

[1] School of Computer Science, Hubei University of Technology, Wuhan, China
csmwzhang@gmail.com
[2] Hubei Key Laboratory of Intelligent Geo-Information Processing,
China University of Geosciences, Wuhan, China

Abstract. The fairness of secret sharing guarantees that, if either participant obtains the secret, other participants obtain too. The fairness can be threatened by cheaters who was hidden in the participants. To efficiently and accurately identify cheaters with guaranteeing fairness, this paper proposes a fair (t, n)-threshold secret sharing scheme with an efficient cheater identifying ability. The scheme consists of three protocols which correspond to the secret distribution phase, secret reconstruction phase, and cheater identification phase respectively. The scheme's secret distribution strategy enables the secret reconstruction protocol to detect the occurrence of cheating and trigger the execution of the cheater identification protocol to accurately locate cheaters. Moreover, we prove that the scheme is fair and secure, and show that the cheater identification algorithm has higher efficiency by comparing with other schemes.

Keywords: Secret sharing · Cheater identification · Fairness · Attack model

1 Introduction

In the reconstruction phase of a (t, n)-threshold secret sharing scheme, dishonest participants can reconstruct the real secret because of receiving the valid secret shares. It's unfair for honest participants that they gain the wrong secret because of accepting the invalid secret shares [1]. To address this issue, many researchers have come up with their solutions. Laih and Lee [2] proposed a v-fair (t, n)-threshold secret sharing scheme, in which all participants do not have to show their secret shares simultaneously to recover the secret with the same probability, even if there are $v(< t/2)$ dishonest participants. [3] and [4] further improved Laih scheme [2]. In 2003, Tian [5] utilized the consistency of secret

Supported by the National Natural Science Foundation of China (61702168, 61672010), Hubei Provincial Department of Education Key Project (D20181402), the open research project of Hubei Key Laboratory of Intelligent Geo-Information Processing (KLIGIP-2017A11).

W. Meng et al. (Eds.): IFIPTM 2019, IFIP AICT 563, pp. 122–132, 2019.
https://doi.org/10.1007/978-3-030-33716-2_10

shares to detect attackers, and constructed a fair (t, n)-threshold scheme with the help of the schemes of Tompa and Woll [6]. Harn and Lin [7] also used the consistency of secret share to design an algorithm to detect cheating behavior and identify cheaters. In 2014, Harn [8] pointed out that the research on asynchronous attack in scheme [5] was incorrect. In 2015, Harn [9] proposed a scheme that can resist asynchronous attacks of external attackers and internal attackers. In 2016, Liu [10] presented a Linear (t, n)-threshold secret sharing scheme in which there is only one honest participant can detect cheaters. Lin [11] constructed a secret sharing scheme which focuses on preventing cheating behavior rather than cheating detection. With the same purpose, in 2018 Liu [12] proposed a (t, n)-threshold secret image sharing scheme. In order to improve the efficiency of the verifiable secret sharing scheme, Mashhadi [13] and Cafaro [14] put forward their schemes respectively, but none of their schemes are unconditionally safe. In 2018, Liu and Yang [16] proposed a cheating identifiable secret sharing scheme by using the symmetric bivariate polynomial, but the scheme does not achieve fairness requirement of secret sharing.

In order to not only identify deception behavior but also efficiently and accurately locate cheaters, this paper propose a fair (t, n)-threshold secret sharing scheme which realizes the fairness through *Distribution protocol* and *Reconstruction protocol*, and achieves the efficiently cheaters identification through *Cheater identification protocol*. Moreover, the presented scheme is unconditional security because of not depending on any security assumptions, and is fair and secure based on four attack models.

The remainder of this paper is organized as follows. We introduce some preliminaries, in Sect. 2. In Sect. 3, we present a fair (t, n)-threshold secret sharing scheme with an efficient cheater identifying algorithm. In Sect. 4, we describe the fairness and security of the proposed scheme, followed by the performance analysis in Sect. 5. Finally, we conclude this paper.

2 Preliminaries

In this section, we briefly recall some fundamental backgrounds which are used in our scheme and then introduce the attack models of our scheme.

2.1 Shamir's (t, N)-Secret Sharing Scheme

Shamir's (t, n)-threshold secret sharing scheme [15] is based on Lagrange interpolating polynomial, in which there are n participants $\mathcal{P}$=$\{P_1,\cdots,P_n\}$, and a mutually trusted dealer $\mathcal{D}$. The scheme consist of two algorithms:

- *Distribution Algorithm*: The dealer $\mathcal{D}$ first randomly generates a polynomial: $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$, in which the secret is s=a_0 and all the other coefficients $a_1, \cdots, a_{t-1}$ are chosen from a finite field $\mathbb{F}$, and then $\mathcal{D}$ computes the secret share $s_i = f(i)$ and sends it to the participant P_i, where $i = 1, 2, \cdots, n$.

- *Reconstruction Algorithm*: In the reconstruction phase, at least t participants submit their secret shares, the secret s can be reconstructed by calculating the Lagrangian interpolation polynomial through these secret shares.

2.2 Definitions of Consistency and Fairness

Definition 1. *(*Consistency*): In a (t, n)-threshold secret sharing scheme, suppose there are m $(m \geq t)$ participants reconstruct the secret. The m shares are consistent if any t shares in them can reconstruct the same secret.*

To check whether m shares are consistent or not, we only need to sequentially execute three steps as follows [5]. (i) Reconstruct a polynomial $g(x)$ using any t shares of the m secret shares. (ii) Check whether the degree of $g(x)$ is $t-1$ or not. (iii) Check whether the remainder $m-t$ secret shares satisfy $g(x)$ or not. If (ii) and (iii) are satisfied, we can conclude that the m shares are consistent.

Definition 2. *(*Fairness*): A (t, n)-threshold secret sharing scheme is fair if it can guarantees that either each participant who takes part in reconstructing the secret obtains the same secret, or knows nothing about the mystery.*

Not difficult to find if the m secret shares are consistent, the corresponding scheme is fair.

2.3 Attack Models

The aim of our scheme is holding the fairness and secure under the following four attack models. :

- *Non-cooperative attack with synchronisation (NCAS)*: All participants submit the secret shares simultaneously, and that there are no cooperations between dishonest parties.
- *Non-cooperative attack with asynchronisation (NCAAS)*: All participants present secret shares successfully and that there are no cooperations between dishonest parties.
- *Collusion attack with synchronisation (CAS)*: The malicious parties modify their secret shares to deceive the honest parties. We assume that all participants submit their secret shares at the same time. Under this assumption, only when the number of malicious parties is more extensive than or equal to the threshold value t, can the malicious parties successfully deceive the honest parties.
- *Collusion attack with asynchronisation (CAAS)*: The dishonest parties collaboratively modify their secret shares to deceive the honest parties. The participants asynchronously release their secret shares. The best option for dishonest participants is to submit their accordingly modified secret shares after all honest participants have submitted their secret shares.

3 Our Schemes

In this section, we introduce our fair (t, n)-threshold secret sharing scheme which consists of three algorithms: distribution algorithm, reconstruction algorithm, and cheater identification algorithm.

3.1 Distribution

The dealer $\mathcal{D}$ wants to share a secret s among n participants $\mathcal{P} = \{P_1, \cdots, P_n\}$. $\mathcal{D}$ first randomly constructs an identifier sequence $\{a_1, a_2, \cdots, a_v\}$ from $\mathbb{Z}_q$, and q is big prime integer. The sequence must satisfy: $a_1 > a_2 > \cdots > a_{l-1} > a_{l+1} > \cdots > a_v > a_l$ where $l \in [1, v]$ is randomly determined by $\mathcal{D}$, and a_l is related to finally recover s. And then, based on the sequence, $\mathcal{D}$ generates v random polynomials through which $\mathcal{D}$ calculates the secret share $s_i = (s_{i_1}, \cdots, s_{i_v})$ for the ith participant. The distribution protocol is shown as:

Distribution protocol
INPUT: the secret s, the parameter v.
OUTPUT: the secret shares $s_1, s_2, \cdots, s_n$.

1. Randomly pick an integer $l \in [1, v]$;
2. Generate $a_1 > a_2 > \cdots > a_{l-1} > a_{l+1} > \cdots > a_v > a_l$;
3. Construct v polynomials of $(t-1)$-degree, like as follows:
   $f_k(x) = a_k + a_{k,1}x + a_{k,2}x^2 + \cdots + a_{k,t-1}x^{t-1} \bmod \mathbb{Z}_q$,
   where $k = 1, \cdots, v$, and $a_{k,1}, \cdots, a_{k,t-1}$ are randomly picked from $\mathbb{Z}_q$;
4. Calculate d to satisfy: $s = a_l \cdot d$;
5. Generate the secret share of ith $(i = 1, \cdots, n)$ participant by computing $s_i = (s_{i_1}, s_{i_2}, \cdots, s_{i_v}) = (f_1(i), f_2(i), \cdots, f_v(i))$.

3.2 Reconstruction

Suppose that $m(\geq t)$ participants $\mathcal{R} = \{P_1, \cdots, P_m\}$ cooperate to reconstruct s. Denoted by $\mathcal{P}_{-i} = \mathcal{R}/P_i$. The reconstruction protocol is shown below:

Reconstruction protocol
INPUT: $m(m \geq t)$ secret shares $\{s_1, s_2, \cdots, s_m\}$.
OUTPUT: the set of cheaters $\mathcal{A}$ and the secret s.

1. 1th round: P_i sends s_{i_1} to $\mathcal{P}_{-i}$, and then performs *Receive_share*(k).
2. kth (k from 2 to v) round: If P_i receives all $(k-1)$th items of secret shares sent by $\mathcal{P}_{-i}$, then uses $\{s_{1_{k-1}}, s_{2_{k-1}}, \cdots, s_{m_{k-1}}\}$ to calculate a Lagrange interpolating polynomial $f_{k-1}(x)$. If $f_{k-1}(x)$ is $t-1$ degree,

then all participants send the kth items of their secret shares and then perform $Receive\_share(k)$. Otherwise, all participants utilize the cheater identification protocol and obtain the set $\mathcal{A}$. If $|\mathcal{P}/\mathcal{A}| \geq t$, then all participants $\in \mathcal{P}/\mathcal{A}$ send the kth items of their secret shares and performs $Receive\_share(k)$; otherwise, protocol is terminated.

Procedure $Receive\_share(k)$: Receiving the kth item of secret share

1. When P_i has received all kth items of secret shares sent by $\mathcal{P}_{-i}$, he utilizes all these items $\{s_{1_k}, s_{2_k}, \cdots, s_{m_k}\}$ to compute the Lagrange interpolating polynomial $f_k(x)$. If the degree of $f_k(x)$ is $t-1$, then P_i performs step (b). Otherwise, all participants invoke the cheater identification protocol to identify the cheaters, and put them into the cheaters' set $\mathcal{A}$. If $|\mathcal{P}/\mathcal{A}| \geq t$, then the protocol turns to step b; otherwise, it is terminated.
2. Calculate the identifier by using the secret share sent by all participants in $\mathcal{P}/\mathcal{A}$, $a_k = f_k(0)$. If $a_k > a_{k-1}$, then $\mathcal{D}$ sends d to all participants in $\mathcal{P}/\mathcal{A}$, and these participants can calculate $s = a_{k-1} \cdot d$, and then the protocol is terminated; otherwise, all participants in $\mathcal{P}/\mathcal{A}$ send the $(k+1)$-th items of secret shares.

3.3 Cheater Identification

To identify the participants who input fake shares, We use a mark vector represents a kind of choice of selecting t participants from m participants, so there are $u = \binom{m}{t}$ mark vectors, denoted by $C_1, \cdots, C_u$. Each mark vector consists of m items, of which the value is 0 or 1, denoted by $C_j = (c_{j_1}, \cdots, c_{j_m}), j = 1, 2, \cdots, u$. Therefore, each mark vector includes t $1's$ and $m - t$ $0's$.

Cheater identification protocol
Input: m, t, k, $\{s_{1_k}, s_{2_k}, \cdots, s_{m_k}\}$.
Output: the set of cheaters $\mathcal{A}$.
All the m reconstruction participants do:

1. Generate u mark vectors $C_1, C_2, \cdots, C_u$.
2. Based on the mark vector C_j $(j = 1, 2, \cdots, u)$ (that is, based on $S'_k = \{s_{i'_k} | c_{j_{i'}} = 1\}$ $(i' = 1, 2, \cdots, m)$), each participant yields the Lagrange interpolating polynomial $f_k^j(x)$. Therefor, each participant can obtain $f_k^1(x), f_k^2(x), \cdots, f_k^u(x)$.

3. According to $f_k^1(x), f_k^2(x), \cdots, f_k^u(x)$, each participant can obtain u values of the identifier a_k, that is $a_k^1 = f_k^1(0), a_k^2 = f_k^2(0), \cdots, a_k^u = f_k^u(0)$. These values might different or the same. Find the most frequently occurring value in them, the value is the value of a_k.
4. And then extract the corresponding mark vectors from $\{C_1, \cdots, C_u\}$. Use $\mathcal{C}^{succ}$ denote the set of these corresponding mark vectors.
5. Perform Logic Or operation on $\mathcal{C}^{succ}$, the participants corresponding to the items whose values are 0 in the result mark vector are cheaters, and then add these participants to $\mathcal{A}$, finally return $\mathcal{A}$.

4 Security and Correctness Analysis

Theorem 1. *In our proposed scheme, the probability that each participant successfully guesses the secret s is $1/v$.*

Proof. The dealer $\mathcal{D}$ hides the secret s into the polynomial $f_l(x)$, where $l \in [1, v]$ is randomly chosen by $\mathcal{D}$, therefore, the participants successfully guess the value of l with the probability $1/v$.

$\mathcal{P} = \{P_1, \cdots, P_m\}$ $(t \leq m \leq n)$ denotes all participants who take part in the secret reconstruction phase, $\mathcal{P}_I = \{P_{i_1}, \cdots, P_{i_\alpha}\} \subseteq \mathcal{P}$ denotes the set of cheaters in $\mathcal{P}$, $\mathcal{P}_{-I} = \mathcal{P}/\mathcal{P}_I$ denotes the set of honest participants in $\mathcal{P}$.

Theorem 2. *Under non-cooperative attack with synchronisation (NCAS), when $m > t$, our scheme is secure and fair.*

Proof. NCAS assumes that all participants present shares at the same time and that there is no cooperation between cheaters. Suppose that in the k-round reconstruction stage, the cheaters in $\mathcal{P}_I$ send invalid secret shares. Since there is no cooperation between the cheaters, their invalid secret shares can only be random numbers in $\mathbb{Z}_q$. When $m > t$, these secret shares could not pass the consistency test, and the attack is immediately detected. In order to restore s, the attackers in $\mathcal{P}_I$ need to guess in which polynomial s is hidden and which honest participants are involved. According to **Theorem** 1, the maximum successful probability is $1/v$. If v is large enough, the probability can be ignored. Therefore, under non-cooperative attack, when $m > t$, our scheme is secure and fair.

Theorem 3. *Under non-cooperative attack with asynchronisation (NCAAS), when $\{(m - \alpha < t - 1) \cap (m > t)\} \cup \{m - \alpha \geq t + 1\}$, our scheme is secure and fair.*

Proof. NCAAS assumes that all participants present shared shares successively without cooperation between attackers. A cheater' ideal attack is to show the secret share at the end, because he can obtain all the shares before others. When $m - \alpha \geq t + 1$, that is, there are no less than $t + 1$ honest participants, who show the secret shares firstly. Therefore, the attackers can reconstruct the correct polynomial $f_k(x)$ (suppose in k-round) based on t real secret shares, and then obtain the a_k. The attackers can show the real secret shares in the first l rounds and show a fake secret share in $(l+1)$th round. However, the fake secret share cannot pass the consistency test, and the attack behavior can be detected, which trigger the execution of cheater identification algorithm. The right identifier a_{l+1} can be reconstructed based on the $m-\alpha$ real secret shares, because $\binom{m-\alpha}{t} > 1$, the a_{l+1} is correct identifier which can be used to identify the attackers, therefore, the attackers could not gain d from the dealer to obtain s. When $m-\alpha < t+1$, for an attacker, even if he finally shows his secret share, he can only obtain at most $t-1$ real secret shares, so he can not reconstruct any $t-1$-degree polynomial, as a result he can not recover s. In order to detect attacks, m should greater than t. In conclusion, when $\{(m-\alpha < t-1) \cap (m > t)\} \cup \{m-\alpha \geq t+1\}$, the proposed scheme is secure and fair.

Theorem 4. *Under collusion attack with synchronisation (CAS), when* $\{(\alpha < t) \cap (m > t)\} \cup \{(\alpha \geq t) \cap (m-\alpha > \alpha+t-1)\}$*, our scheme is secure and fair.*

Proof. CAS assumes that all participants present secret shares simultaneously and that multiple attackers conspire to attack the scheme. Suppose there are α cheaters in k-round. (i) When $\alpha \geq t$, if the number of honest participants is less than t, that is, $m-\alpha < t$, then cheaters can cooperate to forge a set of invalid secret shares which can pass consistency detection. The specific process is as follows: Cheaters first use their secret shares to recover an interpolation polynomial, then utilize the polynomial to calculate the secret shares held by other honest participants, and then generate their false secret shares based on the secret shares of other honest participants. For example, $\alpha = t$, $m-\alpha = t-1$, $m = 2t-1$, use $\{P_1, \cdots, P_{t-1}\}$ denote honest participants, use $\{P_t, P_{t+1}, \cdots, P_{2t-1}\}$ denote cheaters. Cheaters can use their true secret share $\{s_{t_k}, s_{t+1_k}, \cdots, s_{2t-1_k}\}$ to calculate the interpolation polynomial $f_k(x)$, so they can show the true secret shares in the first l rounds, and in $(l+1)$th round, they can use $f_{l+1}(x)$ to obtain other honest participants' secret shares $\{s_{1_{l+1}}, \cdots, s_{t-1_{l+1}}\}$, and calculate another $(t-1)$-degree polynomial $f'_{l+1}(x)$ by using secret shares $\{s_{1_{l+1}}, s_{2_{l+1}}, \cdots, s_{t-1_{l+1}}\}$ and a random value $s'_{t_{l+1}}$. And then, cheaters use $f'_{l+1}(x)$ to calculate $t-1$ invalid secret shares $\{s'_{t_{l+1}}, s'_{t+1_{l+1}}, \cdots, s'_{2t-1_{l+1}}\}$. Finally, the secret shares shown by all participants as follows: $\{s_{1_{l+1}}, s_{2_{l+1}}, \cdots, s_{t-1_{l+1}}, s'_{t_{l+1}}, s'_{t+1_{l+1}}, \cdots, s'_{2t-1_{l+1}}\}$. These m secret shares can pass consistency detection when $m-\alpha \geq t$. The secret shares forged by the above method in $(l+1)$th round cannot pass consistency detection. By executing the identification algorithm, m real secret shares can used to reconstruct the correct identifier a_{l+1} at $\binom{m-\alpha}{t}$ times, while $t-1$ real secret shares and an invalid secret share can be utilized to reconstruct a wrong identifier a'_{l+1} at $\binom{\alpha+t-1}{t}$ times. Therefore, we have $\binom{m-\alpha}{t} > \binom{\alpha+t-1}{t}$. That is, $m-\alpha > \alpha+t-1$, under this condition, the invalid secret shares can be detected, and cheaters cannot obtain d from the dealer and recover s. But the honest participants can gain d and reconstruct s. (ii) If $\alpha < t$, these α cheaters can not use their real secret shares to forge the invalid secret shares that can pass the consistency detection. When $m > t$, this attack can not pass the consistency detection. If cheaters want to reconstruct s, they can only guess the value of l, the probability of successfully guessing is only $1/v$. From what has been discussed above, when $\{(\alpha < t) \cap (m > t)\} \cup \{(\alpha \geq t) \cap (m - \alpha > \alpha + t - 1)\}$, our scheme is secure and fair.

Theorem 5. *Under collusion attack with asynchronisation (CAAS), when* $m - \alpha > \alpha + t - 1$*, our scheme is secure and fair.*

Proof. CAAS assumes that all participants present secret shares successively and that multiple cheaters conspire to attack the scheme. For cheaters, the ideal mode of attack is to present the secret shares at the end, so that they can obtain the real secret shares presented by previous honest participants. When $m - \alpha \geq t$, there are not less than t honest participants, who first show the secret shares. Attackers use $t - 1$ real secret shares (according to the method of **Theorem** 4) to forge α invalid secret shares. Because $m - \alpha \geq t$, these invalid secret shares cannot pass consistency detection. By executing the identification algorithm, $m - \alpha$ real secret shares can be used to recover the correct identifier a_{l+1} $\binom{m-\alpha}{t}$ times, while $t - 1$ real secret shares and an invalid secret share can be utilized to reconstruct a wrong identifier a'_{l+1} $\binom{\alpha+t-1}{t}$ times. Therefore, we have $\binom{m-\alpha}{t} > \binom{\alpha+t-1}{t}$. Concretely, under $m - \alpha > \alpha + t - 1$, these invalid secret shares can be detected, and cheaters cannot gain d from the dealer and reconstruct s. But the honest participants can obtain d and recover s. Therefore, when $m - \alpha > \alpha + t - 1$, the proposed scheme is secure and fair.

Theorem 6. *Under the conditions mentioned above, our cheater identification algorithm is correct.*

Proof. The key to prove the correctness of the cheater identification protocol is to prove the most frequently occurring value in $\{a_k^1 = f_k^1(0), \cdots, a_k^u = f_k^u(0)\}$ is the correct value of a_k. In the cheater identification protocol, interpolating polynomials are reconstructed only based on t secret shares, therefore, only when the t secret shares are real can the correct value of a_k be recovered. To guarantee the most frequently occurring value in $\{a_k^1 = f_k^1(0), \cdots, a_k^u = f_k^u(0)\}$ is the correct value of a_k, the following condition must be satisfied:

$$\binom{m-\alpha}{t} > \frac{1}{2}\binom{m}{t}.$$

We have,

$$\begin{aligned}
&\frac{(m-\alpha)!}{(m-\alpha-t)!t!} > \frac{1}{2}\cdot\frac{m!}{(m-t)!t!} = \frac{1}{2}\cdot\frac{(m-\alpha)!\alpha!}{(m-t)!t!}\\
\Rightarrow &\frac{(m-\alpha)!}{(m-\alpha-t)!} > \frac{1}{2}\cdot\frac{(m-\alpha)!\alpha!}{(m-t)!} = \frac{1}{2}\cdot\frac{(m-\alpha)!}{(m-\alpha-t)!}
\end{aligned}$$

Since the inequality is always true, our cheater identification algorithm is correct.

5 Performance

The following two examples are given to respectively calculate the maximum number of attackers α_{max} under the four types of attack models. Taking (7, n) threshold scheme as an example, assuming $m = 9$ and $m = 11$, where m is the number of participants who take part in the secret reconstruction phase. Under NCAS, according to **Theorem** 2, when $m > t$ our scheme is secure and fair, so $\alpha_{max} = 9$. Similarly, under NCAAS, according to **Theorem** 3, when $\{(m - \alpha < t - 1)\cap(m > t)\}\cup\{m - \alpha\geq t + 1\}$ our scheme is secure and fair, which means $\alpha_{max} = 9$. From the analysis of **Theorem** 4, Under CAS, when $\{(\alpha < t)\cap(m > t)\}\cup\{(\alpha \geq t)\cap(m-\alpha > \alpha+t-1)\}$ the proposed scheme is safe and fair, so $\alpha_{max} = 6$. According to the analysis of **Theorem** 5, Under CAAS, our scheme can defend at most 1 cheaters, as shown Table 1. Based on a similar analysis process, when $m = 11$, the values of α_{max} are shown as in Table 1.

Table 1. (7,n)-threshold scheme, $m = 9$ or $m = 11$

Attack model	Conditions	$\alpha_{max}(m = 9)$	$\alpha_{max}(m = 11)$
NCAS	$m > t$	9	11
NCAAS	$\{(m - \alpha < t - 1)\cap(m > t)\}\cup\{m - \alpha\geq t + 1\}$	9	11
CAS	$\{(\alpha < t) \cap (m > t)\} \cup \{(\alpha \geq t) \cap (m - \alpha > \alpha + t - 1)\}$	6	6
CAAS	$m - \alpha > \alpha + t - 1$	1	2

Different from Tian and Peng's [17] scheme, our scheme does not depend on any security assumptions, it is a unconditional security scheme. Compared to Tian's [5], Harn's [8], Harn-Lin's [7] and Liu-Yang's [16] secret sharing schemes, our scheme achieves fairness but they do not have, as shown in Table 2.

Table 2. Security comparison

Scheme	Tian [5]	Harn-Lin [7]	Liu-Yang [16]	Tian-Peng [17]	ours
Security assumption	no	no	no	ECDLP	no
Fairness	no	no	no	no	yes

In [7], Harn and Lin proposed a secret sharing scheme that can identify cheaters. In their scheme, the correct secret needs to be confirmed and the secret share of each participant needs to be verified. In our scheme, we removed the process of validating each participant's secret share but achieves the same function of [7]. Therefore, our scheme has higher operating efficiency than [7].

6 Conclusion

In this paper, we study the cheater identification issue and the fairness problem in the reconstruction phase of secret sharing, and propose a fair (t, n) secret sharing scheme including a efficient cheater identification algorithm. By comparing with the existing verifiable secret sharing schemes, it can be found that our scheme achieves fairness. Compared with the fair secret sharing scheme, our cheater identification algorithm has a lower computational complexity. Moreover, we analyzed the security of our proposed scheme under four different attack models.

References

1. Zhang, M., Zhang, Y., Jiang, Y., Shen, J.: Obfuscating EVES algorithm and its application in fair electronic transactions in public cloud systems. IEEE Syst. J. **13**(2), 1478–1486 (2019)
2. Laih, C.S., Lee, Y.C.: V-fairness (t, n) secret sharing scheme. IEEE Proc.-Comput. Digital Tech. **144**(4), 245–248 (1997)
3. Lee, Y.-C.: A Simple $(v,\ t,\ n)$-fairness secret sharing scheme with one shadow for each participant. In: Gong, Z., Luo, X., Chen, J., Lei, J., Wang, F.L. (eds.) WISM 2011. LNCS, vol. 6987, pp. 384–389. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23971-7_48
4. Yang J.H., Chang C.C., Wang C.H.: An efficient v-fairness (t, n) threshold secret sharing scheme. In: 2011 Fifth International Conference on Genetic and Evolutionary Computing, pp. 180–183. IEEE (2011)
5. Tian, Y., Ma, J., Peng, C., Jiang, Q.: Fair (t, n) threshold secret sharing scheme. IET Inf. Secur. **7**(2), 106–112 (2013)
6. Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptol. **1**(3), 133–138 (1989)
7. Harn, L., Lin, C.: Detection and identification of cheaters in (t, n) secret sharing scheme. Des. Codes Crypt. **52**(1), 15–24 (2009)
8. Harn, L.: Comments on'fair (t, n) threshold secret sharing scheme. IET Inf. Secur. **8**(6), 303–304 (2014)
9. Harn, L., Lin, C., Li, Y.: Fair secret reconstruction in (t, n) secret sharing. J. Inf. Secur. Appl. **23**, 1–7 (2015)
10. Liu, Y.: Linear (k, n) secret sharing scheme with cheating detection. Secur. Commun. Netw. **9**(13), 2115–2121 (2016)
11. Lin, P.: Distributed secret sharing approach with cheater prevention based on qr code. IEEE Trans. Ind. Inform. **12**(1), 384–392 (2016)
12. Liu, Y., Sun, Q., Yang, C.: (k, n) secret image sharing scheme capable of cheating detection. EURASIP J. Wireless Commun. Netw. **1**, 72 (2018)

13. Mashhadi, S., Dehkordi, M.H., Kiamari, N.: Provably secure verifiable multi-stage secret sharing scheme based on monotone span program. IET Inf. Secur. **11**(6), 326–331 (2017)
14. Cafaro, M., Pelle, P.: Space-efficient verifiable secret sharing using polynomial interpolation. IEEE Trans. Cloud Comput. **6**(2), 453–463 (2018)
15. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
16. Liu, Y., Yang, C., Wang, Y., Zhu, L., Ji, W.: Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. Inf. Sci. **453**, 21–29 (2018)
17. Tian Y., Peng C., Zhang R., Chen Y.: A practical publicly verifiable secret sharing scheme based on bilinear pairing. In: International Conference on Anti-counterfeiting, pp. 71–75. IEEE (2008)