Modeling Reactive Trust Acquisition Using State Transition Systems

Sergiy Gladysh, Peter Herrmann

Modeling Reactive Trust Acquisition using State Transition Systems

Sergiy Gladysh and Peter Herrmann

Department of Telematics
Norwegian University of Science and Technology (NTNU)
Trondheim, Norway
{sg, herrmann}@item.ntnu.no

Abstract. In this work-in-progress article, we propose the use of state transition systems to model and specify non-trivial real-life trust acquisition strategies, which are stateful and may dynamically adapt, depending on the particular context/situation of a truster, a trustee or an environment. The approach is exemplified with an oral examination scenario in which the kind of questions and, hence, the trust acquisition strategy can be automatically adjusted according to the performance of the examinee. We define a discrete trust metric (a "*state of trust*"), built on top of a continuous trust representation (Jøsang's subjective logic in our example). To specify the according trust acquisition policy as a state-transition system, we use the temporal logic cTLA.

1 Introduction

One major driving force in the trust management field is to make the human trust handling process realizable on computers. This seems to be of highly practical relevance since more and more people use computer devices for the interaction with others, particularly, in social networks. Thus, in spite of the spacial distance to the cooperation partners, these media should basically allow the same use of trust in the interaction with others as traditional face-to-face communication. This holds particularly for trust-based decisions, for instance, when the trust to a "friend" in a social network is used to decide if documents can be exchanged with her/him. McKnight and Chervany defined such *decision trust* as *"the willingness to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible"* [1].

In the last two decades significant efforts were made to realize the handling of decision trust on computer devices. Interestingly, however, the existing methods enable only stateless trust acquisition based on experience, i.e., do neither consider the particular situation, in which a person acquires trust, nor the order in which varying experience is made. Yet, many trust building (and also trust-based decision) contexts call for taking these aspects into consideration, which should also be realizable on a computer.

To address this problem, we propose the use of state transition systems to model the process of gaining trust based on experience. In theses systems, the

states are used to represent both, the representation of trust and the current situation of the truster. The transitions model the various kinds of experience which lead the truster to adapt the trust representation and might also change her/his situation. State transition systems are relatively easy to specify and, as long as the state space is finite, can be quite directly transformed into programming code (see [2]). Further, as pointed out in [3], they can be easily combined to implement a whole trust-based decision process and important properties can be highly automatically proved by model checking.

2 Trust Modeling Mechanisms

A first step in realizing trust on computers is to create a decent representation of the current trust of a truster in a trustee which is usually referred as *trust value*. The trust values can be binary and classify only if somebody is "trusted" or "distrusted". Since trust is usually more complex than that, one can also use discrete representations with more than two values like "strong trust", "weak trust", "weak distrust" or "strong distrust" [4] resp. the 12 different stars expressing the difference of positive and negative ratings somebody gained from sales partners in eBay.[1] Or we can use continuous trust values which often are intervals of real numbers reaching, e.g., from 0 to 1, where the former describes complete full distrust and the latter full trust [5, 6]. In the subjective logic [7], Jøsang uses so-called *opinion triangles* which besides of trust and distrust also enable to model uncertainty. That means, a trust value is represented by the three variables b (*belief*, i.e., trust), d (*disbelief*, i.e., distrust) and u (*uncertainty*). All three variables are real numbers in the interval $[0, 1]$ which must add up to 1. This allows to distinguish if missing trust is caused by a high degree of disbelief in or by missing knowledge about a trustee.

For discrete trust values, one can simply define mappings linking a certain trust value to a policy to be enforced (e.g., buy only from sellers in eBay that have at least a purple star). When one uses continuous values in an interval, sub-intervals (e.g., $[0.9, 1]$) can be defined and all their trust values assigned to certain policies. Likewise, one can define areas in an opinion triangle and map all trust values in an area to a certain policy [8].

With respect to trust building based on recommendations, i.e., scenarios like Alice acquires trust on David based on the recommendations of Bruce and Charlotte, one can, for example, use the *discounting* and *consensus* operators of the subjective logic [7]. If Alice has certain trust in the quality of Bruce's recommendations about other people, and Bruce has direct trust in David which both are expressed by opinion triangles, the discounting operator can be used to compute the trust Alice should have in David based on Bruce's recommendation. Further, if there are trust values of Alice's trust in David based on both, Bruce's and Charlotte's recommendations, one can use the consensus operator to bring the two opinion triangles together to one trust value showing the overall trust Alice should have in David based on both recommendations together.

[1] `http://pages.ebay.com/help/feedback/questions/star.html`

Most of the work done in trust acquisition based on experience, comprises the computation of trust values from positive and negative experience. With respect to discrete trust values, one can, for example, use the difference of positive and negative experience reports and map the result to a certain trust value. This is done by eBay to assign stars to traders. Another way is to allow several ratings, often ranging from one to five stars and to represent the trust value as an average of the ratings which, despite its primitiveness and roughness, is transparent and intuitively understood by many end-users. The scores can be either equally weighted or being discriminated (i.e., multiplied by coefficients) depending on their importance, reputation, age, freshness, location, etc. The latter is used, for instance, in epinions and Amazon.[2]

Trust and reputation acquisition metrics producing continuous trust values were developed for relevant application domains like social networks [6, 9] and web search [10]. Some of these techniques, i.e., the one used by Advogato,[3] are designed to be robust and resistant against security attacks, e.g., reducing somebody's reputation by defamation.

The Subjective Logic [7] enables trust computation based on Bayesian probabilistic methods [7]. A closely related metric to compute continuous trust values is the one of Jøsang and Knapskog [11] that allows to compose opinion triangles from positive (p) and negative (n) ratings according to the following formulas:

$$b = \frac{p}{p+n+k} \qquad d = \frac{n}{p+n+k} \qquad u = \frac{k}{p+n+k}$$

By the constant k, for which often the values 1 or 2 are used, one can define how prompt certainty about a trustee is built. Variants of this metric allow to deduce older experiences with a forgetting factor [12, 3] or to express various degrees of positive and negative experience reports like the five stars mentioned above [13]. An alternative is the application of fuzzy logic to compute continuous trust and belief values. This is proposed by Flaminio et al. [14].

Our main observation, after having analyzed these trust acquisition methods, is that these functions are pure information transformation algorithms that do not allow reacting on changing situations. Thus, trust building is mostly stateless and the resulting trust values depend neither on the dynamic context of the situation nor on the logical ordering of the outcomes. In contrast, we are targeting to model reactive, dynamic, stateful and context-aware trust acquisition.

3 An Oral Examination Scenario

Exams of university courses are a typical example of building decision trust based on experience since one cannot fully examine the whole content of a course within the 30 or 45 minutes, an oral exam usually lasts. Instead, an examiner asks relatively few well-directed questions to get a realistic belief in the examinee's

[2] `http://www.epinions.com`, `http://www.amazon.com`
[3] `http://www.advogato.org`

knowledge and ability to work with the contents of the course. Based on this belief, the degree of the examinee is decided.

In our scenario, we use some simplifications. We assume that, in the beginning, the examiner has no knowledge about the student's abilities. Further, we suppose only correct or wrong answers but not partially correct ones. Taking this into account, Jøsang's opinion triangles seem to be adequate representations to describe the current belief of the examiner in the examinee. The exam starts with the uncertainty value u being 1 and by giving correct or wrong answers, the belief resp. disbelief values b and d are increasing until the examiner has a sufficient certainty to grade the examinee.

In contrast, due to its hyperbolic way to get certainty, i.e, the uncertainty value decreases strongly in the beginning and mitigates later on, we consider the metric of Jøsang and Knapskog [11] less appropriate. Albeit we agree, that an experienced examiner can often make a good guess about the later outcome from the ways the first questions are answered, in the end, the different parts of the course content are asked in subsequent questions such that a linear growing of certainty seems more adequate.

Moreover, the examiner has the possibility to react on the performance of the examinee by adapting the complexity of the questions. For instance, if the student starts with convincing responses, the examiner might conclude at a certain point that she/he is quite mature and starts to ask tougher questions to find out more about the examinee's grade of excellence. Likewise, a meager start leads to simpler questions to check if the student meets at least the minimum requirements to pass the course. Thus, the examiner might change the originally neutral bias to a positive or negative one and, in consequence, adapt the way to continue the examination.

Changing the bias is considered in the policy of our scenario:

- The examination starts with a neutral bias and it is planned to ask 12 to 13 questions. Accordingly, correct and wrong answers lead to a linear increase of the b resp. d values.
- If at least seven of the first eight questions were answered correctly, the examiner gets a positive bias and starts to ask more difficult questions. In consequence, positive answers lead to a stronger growth of the b value while wrong ones increase the d value less than in the neutral case. Further, the student is guaranteed at least a very good grading.
- If at least four of the first eight questions were not correctly answered, the bias of the examiner is getting negative and the subsequent questions are simpler. Correct answers lead to a slower increase of the b value while wrong ones to a stronger growing of the d value. The student may reach a satisfactory grade at maximum.

4 State Transition Systems

As mentioned in the introduction, we like to model trust building strategies like the one sketched above by state transition systems. Here, the states express the

current trust values as well as additional situation information (e.g., the current bias of an examiner) and the transitions model changes of the trust values and situation according to new experience. This allows clearly arranged specifications of complex trust building policies and the formal nature of the models enables to prove properties by, e.g., model checkers. While there are state transition system techniques that enable to specify infinitely many states, the applicability of model checkers restrict them to finite subsets. Further, only state transition systems with final states can be realized on computers. In consequence, the modeled trust values have to be discrete which contradicts with Jøsang's claim that discrete models are *theoretically misguided* [4]. From a theoretical point of view, we agree with him since, for instance, only continuous models offer the unlimited granularity to model all thinkable trust scenarios. From a practical viewpoint, however, also discrete trust values should be able to reflect most relevant scenarios if they are sufficiently fine-grained. So, we have been challenged to find a granularity that is detailed enough to model nearly all kinds of building trust but sufficiently small to enable the use of model checkers.

As trust representation, we apply the opinion triangles [7] introduced in Sect. 2 since their ability to distinguish uncertainty from disbelief makes them superior to other techniques. To reach a finite subset of trust values, however, the three variables b, d and u had to be discretized. Due to our experience, we decided to use intervals of 0.01 between two discrete values which enables 101 different values for each of the three variables and leads to 5050 different possible trust values. That is a number that state-of-the-art model checkers can easily manage. For convenience, we use integer values between 0 and 100 for each of the three variables which have to add up to 100.

To model the trust building scenario for oral examinations introduced in Sect. 3, we use the specification technique *compositional Temporal Logic of Actions* (cTLA) [15] that is based on Lamport's *Temporal Logic of Actions* (TLA) [16]. This style allows comprehensible specifications of complex behavioral properties which can be directly proved by the model checker TLC [17].

Fig. 1 depicts the cTLA model of our trust building scenario. In cTLA, states are modeled by variables which are declared in the area VARIABLES. The current trust value is represented by the variables bf and db which both range from 0 to 100 and model the belief resp. disbelief values of the discretized opinion triangle. The uncertainty variable does not need to be represented by a variable since it is always $100 - bf - db$. Further, the variable *bias* specifies the current bias of the examiner that can be neutral, positive or negative as described by the type *Biases* defined in the area CONSTANTS. In the area INIT, the variable setting in the initial state is defined. Assuming uncertainty at the beginning of an exam, both variables bf and db are set to 0 while the initial bias is neutral.

Transitions are modeled by actions which are pairs of states, i.e., the state before and the one after carrying out an action. Here, variable identifiers without an add-on (e.g., bf) refer to the state before execution while identifiers with a prime (e.g., bf') mark the state reached afterwards. In the area ACTIONS, we defined two actions modeling the development of the trust values and bias after

MODULE *Oral Exam Trust Building*

CONSTANTS
$Biases \triangleq \{\text{“neutral”}, \text{“positive”}, \text{“negative”}\};$

FUNCTIONS
$New\_Bias(b, d : 0 \ldots 100, bi : Biases) : Biases \triangleq$
IF $(b + d \geq 64 \wedge d \leq 8) \vee bi = \text{“positive”}$
THEN “positive”
ELSE IF $(b + d \geq 64 \wedge d \geq 32) \vee bi = \text{“negative”}$ THEN “negative”
ELSE “neutral”;

VARIABLES
$bf, db : 0 \ldots 100;\ bias : Biases;$

INIT
$bf = 0 \wedge db = 0 \wedge bias = \text{“neutral”};$

ACTIONS
$correct\_answer(b, d, u : 0 \ldots 100, bi : Biases) \triangleq$
$b = min(100 - db,$
$bf +$ IF $bias = \text{“neutral”}$ THEN 8
ELSE IF $bias = \text{“positive”}$ THEN 12
ELSE 4)
$\wedge\ d = db \wedge u = 100 - b - d \wedge bi = New\_Bias(b, d, bias)$
$\wedge\ bf' = b \wedge db' = d \wedge bias' = bi;$
$wrong\_answer(b, d, u : 0 \ldots 100, bi : Biases) \triangleq$
$d = min(100 - bf,$
$db +$ IF $bias = \text{“neutral”}$ THEN 8
ELSE IF $bias = \text{“negative”}$ THEN 12
ELSE 4)
$\wedge\ b = bf \wedge u = 100 - b - d \wedge bi = New\_Bias(b, d, bias)$
$\wedge\ bf' = b \wedge db' = d \wedge bias' = bi;$

Fig. 1. State Transition System for Adapted Trust Building in Oral Exams

a correct resp. a wrong answer. Both actions offer the elements b, d and u of the trust value achieved by considering the answer as well as the new bias bi as parameters. So, they can be composed with actions of other modules (see [15]) modeling for instance the grading policy or the use of the consensus operator combining the trust values of different examiners (see [3]).

The first conjunct of action *correct_answer* models the computation of the new belief value, i.e., the parameter b. Following the policy mentioned above, the belief is increased by 8 if the examiner has a neutral bias, 12 with an positive bias reflecting that the questions are more difficult in this case, and 4 with a negative bias since the questions are now simpler. Further, we assure by using the function *min* (minimum) that the sum of the belief and disbelief values never gets larger than 100. By the conjuncts in the next line, we state that the disbelief is not changed by the positive answer and that the uncertainty is indeed

the difference of the belief and disbelief values to 100. Further, we model the new bias of the examiner which is expressed by the function *New_Bias* declared in the area FUNCTIONS. It follows our policy since the bias will be positive if either at least eight questions were asked ($b + d \geq 64$) of which at most one was answered wrongly ($d \leq 8$) or the bias already is positive. A negative bias is reached if at least four of the first eight questions were negative ($d \geq 32$) or the examiner is already in a negative bias. In all other cases, the bias remains neutral. Finally, the conjuncts on the last line of the action specify that the variables bf, db and *bias* carry the new values after executing it. The action *wrong_answer* is modeled in a similar way.

Using the model checker TLC [17], we proved some interesting properties. The most basic constraint is that the sum of the three variables of a discretized opinion triangle never exceeds 100 which is specified by the invariant property $bf + db \leq 100$. Moreover, we verified the general trust building property that new experience cannot increase the uncertainty by checking for both actions that they fulfill $bf' + db' \geq bf + db$. Finally, we proved that the examiner remains in a positive resp. negative bias in order to guarantee fairness towards the examinees, i.e., to prevent that, first, the positive bias is reached which leads to complex questions, but than returns to normal such that the student is not guaranteed a very good grade anymore. Of course, in models that are so simple as the one shown in Fig. 1, the fulfillment of these properties can be easily observed by walking through the definitions but for more complex trust building strategies, the verification with model checkers is surely helpful. TLC needed only a few seconds to detect 222 different reachable states that all fulfilled the properties mentioned above.

5 Discussion

State transition systems give us a theoretically sound foundation and are a highly powerful way to model, analyze and develop dynamic trust management systems. A core advantage of our approach is that discrete formal methods like finite automata, state-machines and temporal logic can allow us to put trust management "on the shoulders of (the) giants" of theoretical computer science. Our research hypothesis is the following: for quite an extensive class of trust management scenarios, the "*digital*" discrete methods will give more fruitful and appropriate results than the "*analogous*" continuous trust acquisition techniques. Further, we assume that situation-aware trust acquisition enables to build stronger ties between trust management and information security, in particular in the area of access control models and formal security policies.

As the next steps within this research direction we envision to prove our claims by going more deeply into the development of reactive state transition-based trust acquisition models. Moreover, we want to investigate the method for combining the state transition trust systems with the formal models of access control and security policies. With respect to tool support, we want to combine our method with the model-based system engineering technique SPACE [18] that

was already used in trust management [2]. As an interesting application domain for our work, we see access control based on reactive trust acquisition in the Future Internet and, in particular, in social networks.

References

1. McKnight, D.H., Chervany, N.L.: The Meanings of Trust. Working Paper Series 96–04, University of Minnesota — Carlson School of Management (1996)
2. Herrmann, P., Kraemer, F.A.: Design of Trusted Systems with Reusable Collaboration Models. In: Proceedings of the Joint iTrust and PST Conferences on Privacy, Trust Management and Security (IFIPTM07). IFIP AICT 238, Moncton, Springer-Verlag (July/August 2007) 317–332
3. Herrmann, P.: Temporal Logic-Based Specification and Verification of Trust Models. In: Proceedings of the 4th International Conference on Trust Management (iTrust 2006). LNCS 3986, Pisa, Springer–Verlag (May 2006) 105–119
4. Jøsang, A.: Trust and Reputation Systems. Tutorial at IFIPTM 2009, Purdue (June 2009)
5. Ni, Q., Bertino, E., Lobo, J.: Risk-based access control systems built on fuzzy inferences. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ASIACCS '10, New York, ACM (2010) 250–260
6. Golbeck, J.: Computing with Social Trust. Springer (December 2010)
7. Jøsang, A.: A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems **9**(3) (June 2001) 279–311
8. Herrmann, P.: Trust-Based Protection of Software Component Users and Designers. In Nixon, P., Terzis, S., eds.: Proceedings of the 1st International Conference on Trust Management. LNCS 2692, Heraklion, Springer-Verlag (May 2003) 75–90
9. Carminati, B., Ferrari, E., Perego, A.: Enforcing access control in web-based social networks. ACM Trans. Inf. Syst. Secur. **13**(1) (November 2009) 6:1–6:38
10. Page, L., Brin, S., Motwani, R., Winograd, T.: The PageRank Citation Ranking: Bringing Order to the Web. Technical report, Stanford Digital Library Technologies Project (1998)
11. Jøsang, A., Knapskog, S.J.: A metric for trusted systems. In: Proceedings of the 21st National Security Conference, NSA (1998)
12. Jøsang, A., Ismail, R.: The Beta Reputation System. In: Proceedings of the 15th Bled Electronic Commerce Conference. (June 2002)
13. Tavakolifard, M., Herrmann, P., Knapskog, S.: Inferring Trust based on Similarity with TILLIT. In: Proceedings of the 3rd IFIP WG 11.11 International Conference on Trust Management (IFIPTM09). IFIP AICT 300, West Lafayette, Springer-Verlag (June 2009) 133–148
14. Flaminio, T., Pinna, G.M., Tiezzi, E.B.: A complete fuzzy logical system to deal with trust management systems. Fuzzy Sets and Systems **159**(2008) 1191–1207
15. Herrmann, P., Krumm, H.: A Framework for Modeling Transfer Protocols. Computer Networks **34**(2) (2000) 317–337
16. Lamport, L.: Specifying Systems. Addison-Wesley (2002)
17. Yu, Y., Manolios, P., Lamport, L.: Model Checking TLA+ Specifications. In Pierre, L., Kropf, T., eds.: Correct Hardware Design and Verification Methods (CHARME '99). Lecture Notes in Computer Science 1703, Springer-Verlag (1999) 54–66
18. Kraemer, F., Slåtten, V., Herrmann, P.: Tool Support for the Rapid Composition, Analysis and Implementation of Reactive Services. Journal of Systems and Software **82** (2009) 2068–2080