

Understanding and learning trust: a review, characterization and tool

S. Bottitta

Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Italy

M. Felici

School of Informatics, The University of Edinburgh, UK

ABSTRACT: This paper reviews works and studies concerning the concept of trust. The review highlights multidisciplinary aspects of the concept of trust and its use. The *Prisoners' Dilemma* provides a characterization of trust. *Trust games* extend the prisoners' dilemma in order to overcome some of its practical limitations. Trust games allow us to study and analyze dynamics of trust. Furthermore, trust games represent those situations where cooperation (or competition) between two entities might emerge eventually. It is necessary to investigate different strategies and their interactions in order to understand trust dynamics (e.g., trust formation). We have implemented a tool, which, accordingly to learning-by-experience approaches, supports exploratory trust games. A graphical interface allows us to understand easily the results. Scenarios of use validate some functionalities of the tool.

1 INTRODUCTION

What is *Trust*? Trust affects diverse relationships or interactions between diverse entities (e.g., trust in people, trust in technology). Trust is critical in those situations of uncertainty. System failures often undermine our trust in technology. Trust relates to the risk associated with technology in presence of uncertainty. This paper reviews works and studies concerning the concept of trust. The review highlights multidisciplinary aspects of the concept of trust and its use. Many diverse models represent aspects of trust. However, there has been little attention about dynamic aspects (e.g., evolution and construction) of trust. The social aspects of trust and risk perception highlight the interaction between trust, risk and knowledge (Douglas and Wildavsky 1982). The different relationships between trust, risk and knowledge affect individual behaviors (e.g., cooperation or competition). These relationships are relevant to the social aspects of technology (Douglas and Wildavsky 1982; MacKenzie and Waicman 1999).

This paper is organized as follows. Section 2 reviews different models of trust. Models capture different trust aspects (e.g., trust dimensions, trust measurements and trust dynamics). Section 3 introduces the prisoner's dilemma as a characterization of trust. Although real scenarios expose the limitations of the prisoners' dilemma, it is still useful to capture basic trust dynamics (e.g., trust strategies, trust evolution, interactions, etc.). *Trust games* extend the prisoners' dilemma in order to overcome some of its

practical limitations. Trust games allow us to study and analyze dynamics of trust. Section 4 describes a tool for trust games. Section 5 validates some tool functionalities on scenarios of use. Section 6, finally, draws conclusions.

2 MODELS OF TRUST

This section introduces the concept of *Trust*. The lack of a generally accepted definition of trust and its multidisciplinary nature emphasize the difficulty in understanding the concept of trust. The characterization of trust dimensions allows us to analyze different aspects (e.g., distribution, dynamic, quantitative, etc.) of trust. Although many different models have been proposed, practical aspects regarding trust expose the limitations of trust models. In particular, models capture to some extent trust dynamics. The review of various models and aspects of trust highlights the complexity of the concept of trust.

2.1 *Trust dimensions*

Trust regards many different socio-technical contexts that characterize the modern *Information Society*. In order to understand the meaning of trust in such contexts, it is necessary an analysis of trust itself and a characterization of trust that captures various socio-technical aspects of trust (McKnight and Chervany 2000). McKnight and Chervany propose an interdisciplinary model, which identifies various

aspects and mechanisms of trust (McKnight and Chervany 1996; McKnight and Chervany 2000). The proposed model derives from a vast literature review that refers to the definition of trust. The proposed model consists of two typologies: a *classification system* for different types of trust; a definition of six different types of *trust constructs*, drawn from the analysis of the classification system, forming the model of trust. A classification system allows us to differentiate among conceptual types. The definition of six different types of trust identifies a set of constructs (or mechanisms) that are conceptually distinguishable, but related on one another. The definition of these six constructs reflects meanings of trust commonly used. The six trust constructs are: *Trusting Intention*, *Trusting Behavior*, *Trusting Beliefs*, *System Trust*, *Dispositional Trust* and *Situational Decision to Trust*. Figure 1 shows the typology of trust and the relationships between the trust constructs (McKnight and Chervany 1996). Table 1 describes the trust constructs.

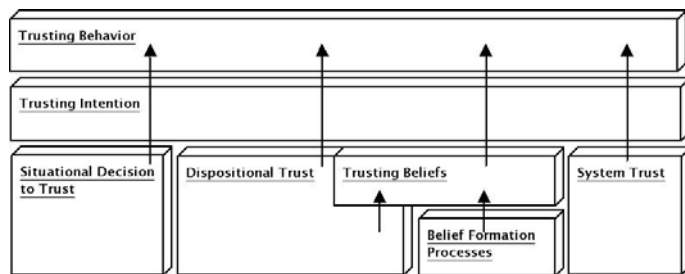


Figure 1. A typology of trust.

Table 1. Trust constructs.

Construct	Definition
Trusting Intention	The extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible.
Trusting Behavior	The extent to which one person voluntarily depends on another person in a specific situation with a feeling of relative security, even though negative consequences are possible.
Trusting Beliefs	The extent to which one believes (and feels confident in believing) that another person is trustworthy in the situation.
System Trust	The extent to which one believes that proper impersonal structures are in place to enable one to anticipate a successful future endeavor.
Dispositional Trust	The recognition that people develop, over the course of their lives, generalized expectations about the trustworthiness of other people.
Situational Decision to Trust	The extent to which one intends to depend on a non-specific other party in a given situation.

The typology of trust (McKnight and Chervany 1996) characterizes trust in terms of relationships. These relationships, or constructs, allow us to analyze trust in different situational contexts. The analysis of trust in different situational contexts allows the identification of different practical characteristics of trust (McKnight and Chervany 2001b).

The identification of such characteristics helps to use the concept of trust (or its characteristics) consistently. The different meanings of trust have origins in different disciplines (e.g., Sociology, Psychology and Economy) characterizing the complexity and multidisciplinary of trust. The analysis of different usages of trust identifies two main groups of definitions: *conceptual* and *referent types*. The first group, i.e., conceptual types, forms the foundations of the typology that identifies the basic trust constructs (McKnight and Chervany 1996). The second group identifies the characteristics of trust related to its usage. Trust is therefore defined according to its usage. Hence, trust identifies specific situations, for instance, *trust in something* (e.g., trust in system reliability) or *trust in someone* (e.g., trust in someone honesty). It is possible to identify sixteen different characteristics grouped into five categories: *Competence*, *Predictability*, *Benevolence*, *Integrity* and others. The typology of trust and its characteristics allow the comparison of different situations or experiments involving the concept of trust. For instance, the typology of trust and its characteristics have been tailored to e-commerce (McKnight and Chervany 2001a). The contextualization of trust in specific scenarios of use, e.g., e-commerce or Internet applications, allows us to identify relationships (e.g., privacy, quality of service, etc.) occurring in remote interactions with respect to the constructs of trust (Grabner-Kräuter and Kalascha 2003; Grandison and Sloman 2000; McKnight and Chervany 2001a). Similarly, the extension of the typology of trust to those situations in which a lack of trust emerges allows us to characterize the concept of *mistrust* (McKnight and Chervany 2001). The typology of mistrust consists of similar, but dual, constructs of the typology of trust. This reflects the use of trust and mistrust as opposite. Note that the typologies define trust and mistrust as two opposite concepts. Thus, it is possible to distinguish them.

Other empirical models, e.g., (Uggirala et al. 2004; Dassonville et al. 1996), identify similar structural models of trust. Barber (Barber 1983) defines trust according to three main characteristics: *Persistence*, *Technical Competence* and *Fiduciary Responsibility*. In contrast, a hierarchical model identifies different levels of trust (Rempel et al. 1985). Each level of trust depends on the previous level. According to the various trust levels, predictability (of system behavior) is a critical characteristic in human-computer interaction, followed by reliability and trust. This model stresses that people judge the predictability of a computer system and assess its behavior. This assumption of predictability relies on three main hypotheses: current system behavior, human ability in assessing computer systems and environmental stability. This means that any variation in system behavior may affect its predictability, hence, affect trust in it. Trust or mistrust in system

behavior affects the overall system performance (Moray et al. 1995; Muir 1994, Muir and Moray 1996). Modeling trust allows the assessment of the impact of trust in automation on human performance (Uggirala et al. 2004).

2.2 Trust measurements

The different trust dimensions highlight the complexity of trust and its different aspects. Measuring trust, therefore, results to be a difficult objective in practice. Such difficulty is due to the multidimensional and multidisciplinary aspects of trust. The relationship between trust and reliability of human-machine interactions justifies the interest on measuring trust. Several studies (Moray et al. 1995; Muir 1994; Muir and Moray 1996) highlight the relationship between system reliability and trust in the system. A lack of trust in system performance is often due to the limited system reliability or predictability.

One of the main issue in measuring trust is due to *uncertainty*. Any trust relationship involves a level of uncertainty. It is necessary to understand the relationship between system properties and operator perception (Uggirala et al. 2004). Uncertainty, differently than trust, can be quantified and related to system properties (Uggirala et al. 2004). Mapping system properties to operator perceptions identifies quantifiable dimensions referred to as uncertainty. Measuring uncertainty shows that the overall trust in the system has an inverse relationship with uncertainty. Hence, decreasing uncertainty would improve the overall system performance (Uggirala et al. 2004).

Although empirical results encourage measuring trust, there are still many issues related to quantitative aspects of trust. Firstly, system measures are often subjective and error-prone. Although quantitative approaches, e.g., Software Metrics (Fenton and Pfleeger 1996), allow the assessment of system features (e.g., reliability), the extension to human factors expose the limitation of measurement practices (Pasquini et al. 2001). Secondly, human perception may affect measurement. Finally, self-confidence or self-trust often affects the perception of system behavior. Although trust in automation affects the overall system performance, perception of system properties is indirectly related to trust. Empirical results show that the main existing relationship is between system uncertainty and competence (as trust dimension) (Uggirala et al. 2004).

2.3 Trust dynamics

In order to understand the meanings of trust and their usages, different models formalize aspects of trust (Carbone et al. 2003; Falcone and Castelfranchi 2001; Nielsen and Krukow 2003). A formal model intends to characterize trust in dynamic networks

(Carbone et al. 2003). The formal model relies on *Global Computing* scenarios, which highlight the aspects of *trust formation, evolution* and *propagation*. A Global Computing environment consists of autonomous, decentralized, mobile and dynamically configurable entities. Global Computing systems become very complex and require security mechanisms. The features of Global Computing systems expose the limitations of traditional security mechanisms (Anderson 2001). Formal notions of trust, as alternative approaches, extend traditional security mechanisms in Global Computing environments. Note that formal models of trust partially capture the typology of trust (McKnight and Chervany 1996). Although it is difficult to capture formally the meanings of trust, it is still possible to identify some general features of trust modeling. In particular, a suitable model of computational trust should be able to express trust dependencies over time and trust dynamics (e.g., evolution of trust). A computational model of trust intends to support a *trust management system* (Carbone et al. 2003). A trust management system consists of a *trust engine* and a *risk engine*, which together form a *principal*. The trust engine is responsible for updating the information on trust according to, direct or indirect, observations. The risk engine then takes and feedbacks the trust information to the trust engine. Note that a trust management system is mainly concerned with the formation, evolution and propagation of trust. A trust management system is, therefore, a suitable instrument for the development of systems that need to comply with stringent privacy requirements (Blaze et al. 1996). Trust management systems exhibit similar features: unified mechanisms, flexibility, locality and differentiation between trust and policy mechanisms.

Trust, as a social phenomenon, exhibits an evolutionary behavior. This aspect exposes the limitations of trust management systems, although they provide mechanisms for implementing trust. Trust emerges and evolves over time. For instance, an entity *A* has trust in *B* according to past experiences (Falcone and Castelfranchi 2001). Trust changes over time. Therefore, it is necessary further to understand trust dynamics. In particular, the relationship between trust and risk perception affects trust dynamics (Corritore et al. 2003; Gefen et al. 2003).

3 A CHARACTERIZATION OF TRUST

3.1 The prisoners' dilemma

The *Prisoners' Dilemma* provides a characterization of trust (Axelrod 1990; Dixit and Nalebuff 1991; Nalebuff and Brandenburger 1996). The prisoners' dilemma captures those situations where cooperation

or competition may arise. It is necessary to find out different strategies and their interactions in order to understand how trust (mistrust) emerges. The dilemma involves two prisoners, who are placed in separate cells. Both prisoners care much more about their personal freedom than about the welfare of their accomplice. They may choose to confess or remain silent. If they both confess, they will receive reduced convictions (i.e., reward for mutual cooperation). If they both remain silent, they will receive minimal convictions (i.e., punishment for mutual defection). However, if they disagree (i.e., a prisoner confesses and the other remains silent, and vice versa), the silent one will receive the full conviction. Whereas the one who confessed will be freed, the dilemma here is that, whatever the other does, each is better off confessing than remaining silent. But the outcome obtained when both confess is worse for each than the outcome they would have obtained had both remained silent. Figure 1 shows a matrix representation of the prisoners' dilemma. Note that there exist a relationship that specifies the order of the four pay-offs: from best $T > R > P > S$ to worst (Axelrod 1990). Different matrices and different rules identify different games (e.g., symmetric, asymmetric, iterative, etc.).

		Column Player	
		Cooperate	Defect
Row Player	Cooperate	R=3, R=3 Reward for mutual cooperation	S=0, T=5 Sucker's payoff and temptation to defeat
	Defect	T=5, S=0 Sucker's payoff and temptation to defeat	P=1, P=1 Punishment for mutual defection

Figure 1. The prisoners' dilemma.

The prisoners' dilemma captures those situations in which two players have conflicting interests. Although the two players have their own interests in winning the game, the better strategy corresponds to cooperation (Axelrod 1990). It is possible to identify different heuristics depending on whether or not *dominant strategies* (Dixit and Nalebuff 1991). Therefore, the prisoner's dilemma captures those situations that may result in cooperation or competition, i.e., *co-opetition* (Nalebuff and Brandenburger 1996). The prisoners' dilemma captures trust between individuals (or groups of individuals). People have to collaborate in order to improve their situations. If they trust each other, they have a cooperative strategy.

Several studies investigate different strategies (e.g., always cooperates, always defects, tit-for-tat¹, mistrust², etc.). Two main approaches exist in order to assess different strategies. The first one is a simple *round-robin tournament*. All strategies are compared according to their scores in each confrontation. The final score, i.e., the sum of all scores, allows the ranking of all strategies according to their performances. The second one is a simulated *ecological evolution*. There initial fixed population of individuals plays round-robin tournaments until their preferences (over the winning strategy) are stable. After every tournament the population of bad strategies is decreased, whereas good strategies obtain new elements. Tournaments are played until the population has been stabilized (the population does not change any more).

3.2 Trust games

Several studies use the prisoners' dilemma in order to characterize trust. In particular, studies evaluate trust in computer-mediated communications (Riegelsberger et al. 2003). Trust in computer-mediated communications is a critical aspect. Mediated communications carry an increased risk. Moreover, they inhibit trust development. Unfortunately, social connectivity (MacKenzie 2004) exposes the limitations of interpreting the rate of cooperation (measured in terms of collective pay-off) as the level of trust in computer-mediated communications (Riegelsberger et al. 2003). Characterizations of trust based on the basic prisoners' dilemma partially capture trust complexity. *Trust games* extend the prisoners' dilemma in order to overcome some of its practical limitations (Riegelsberger et al. 2003). Trust games capture real scenarios that exhibit asynchronous and asymmetric properties, which expose the limitations of the prisoners' dilemma (Riegelsberger et al. 2003). Trust games allow the players to act on different payoff matrixes. Moreover, in a trust game, the players first decide whether to trust or not. Thus, decisions are taken asynchronously.

4 A TOOL FOR TRUST GAMES

This section introduces a tool for trust games. The main objective, according to learning-by-experience, is to support the learning of basic aspects of trust. The tool allows the simulation of trust games drawn as extensions of the prisoners' dilemma. The tool stresses the evolutionary aspects of games (e.g., strategy interactions, player matrixes, etc.). The level of trust between the two players depends on the final score of each game. Measuring trust as collec-

¹ Cooperates, then plays opponent's move.

² Defects, then plays opponent's move.

tive payoff exhibits some limitations in prisoners' dilemma games (Riegelsberger et al. 2003). However, it allows the players to understand and perceive the dependencies between payoff matrixes and strategies. Although collective payoffs provide limited account of the level of trust (cooperation or competition) between the players, differences between scores highlight the combined contributions of payoff matrixes and strategies.

The tool allows the simulation of asymmetric trust games, i.e., two players playing with different payoff matrixes. The interactivity of the tool supports the easy learning of some general aspects of trust (e.g., trust strategies, payoff matrix dependency, evolution, etc.). A graphical interface shows a representation of trust games in terms of decision trees. This supports the understanding of the results. Some scenarios have been analyzed in order to test our tool.

4.1 Tool's architecture

We have implemented a tool, which uses existing Java libraries for the simulation of the prisoner's dilemma. In order to simulate the iterate prisoner's dilemma, the tool uses the Java libraries of the PRISON project³: `fr.lifl.prison` contains the main classes, `fr.lifl.prison.strategies`, implements the main strategies and `fr.lifl.prison.util` provides several utilities for data handling. The tool implements additional classes, which support different functionalities. For instance, it is possible to define and input new strategies. This allows the easy interaction with the prisoner's libraries in order to run several experiments interactively. It is already possible to save game matrixes as XML files. Future implementation will extend this functionality to games, that is, saving games a structured XML files. This would support game and strategy analysis. The tool allows us to use the basic strategies implemented by the `BasicStrategies` class of the prisoner's libraries. Figure 2 shows the tool's architecture.

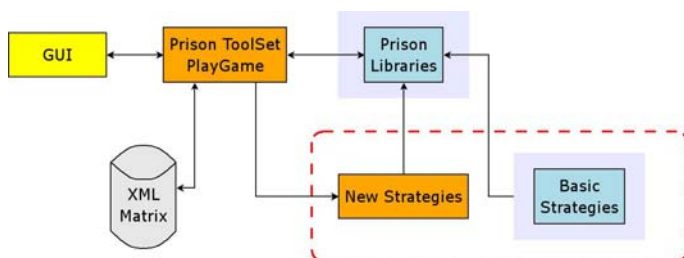


Figure 2. The tool's architecture.

5 SCENARIOS OF USE

Trust games, as extensions of the prisoners' dilemma, allow us to study and analyze different aspects (e.g., interaction, evolution, etc.). Furthermore, trust games represent those situations where cooperation or competition between two entities may emerge. Trust games allow a characterization of the interaction between trust, risk and knowledge. The characterization of trust and risk stresses that the underlying mechanisms of trust and risk perception interact each other.

5.1 Cooperation and competition

The prisoners' dilemma captures those situations in which cooperation or competition (i.e., co-opetition) emerges (Nalebuff and Brandenburger 1996). Let us consider, for instance, the commercial competition between two countries, e.g., USA and Japan, for the development of high-resolution TV. Let us assume that USA has an innovative knowledge, but limited financial resources. Japan could try to exploit this situation in order to gain market shares. USA and Japan, therefore, would engage a strategic decision-making in order to maximize their presence in the market and optimize investment strategies. Their decisions will affect each other strategies. A game, based on the prisoners' dilemma, can easily capture this situation. Each country can decide over two different strategies: *Low* (i.e., investing in low-resolution TV) or *High* (i.e., investing in high-resolution TV). Figure 3 shows the payoff matrix for the game.

		Japan	
		Low	High
USA	Low	4,3	2,4
	High	3,2	1,1

Figure 3. Matrix of the payoffs for USA and Japan.

Figure 4 shows the *decision tree* corresponding to the payoff matrix of Figure 3. The tool captures the decision tree of the game. Figure 5 shows the different options for Player 1 (i.e., USA) and Player 2 (i.e., Japan). Note that the payoff for mutual cooperation corresponds to the strategies of both countries investing for low-resolution TV. This interpretation creates a correspondence between the game and the tool matrixes.

³ <http://www.lifl.fr/IPD/>

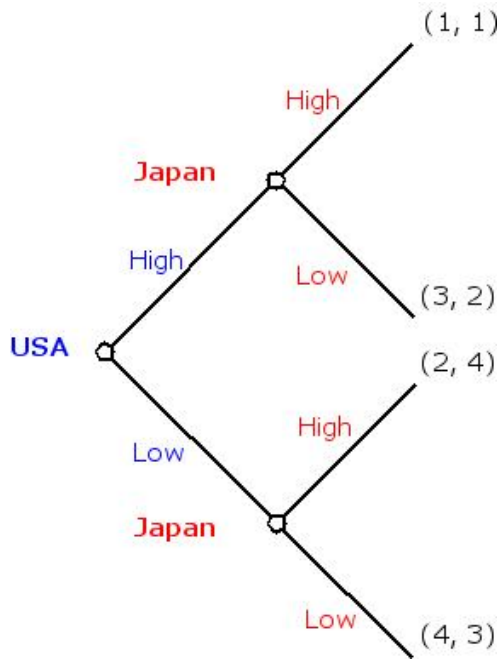
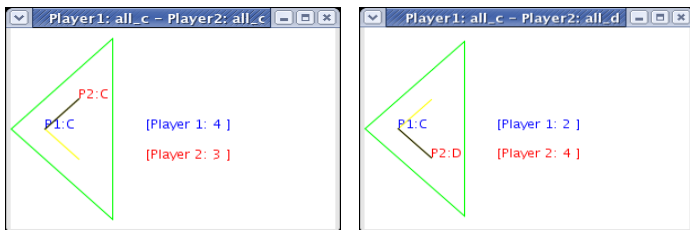


Figure 4. Decision tree.

The tool allows us to play asymmetric games, that is, games relying on different payoff matrixes. These games capture when the two players have different game conditions (e.g., different gains in engaging the game), different risk perceptions or different knowledge (about the game).

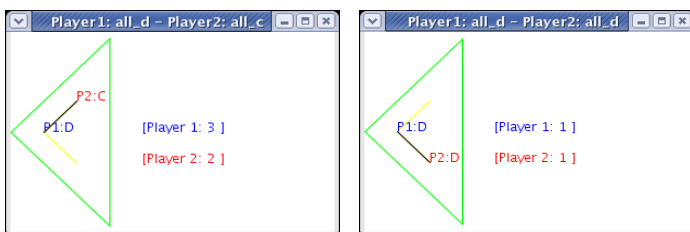
5.2 Comparison of technologies

The prisoners' dilemma can characterize dynamics of trust formation in different communication media (e.g., no communication, textual chat, combination of textual chat and voice communication, and voice communication) (Jensen et al. 2000). The assessment shows how different communication media support formation of trust in people. The experiment consists on letting people to play the prisoners' dilemma. Players can communicate each other by different means. The players fall in different categories according to the means of communication used in the game. This supports the evaluation of trust in different communication media. Figure 7 shows the payoff matrixes for the prisoners' dilemma. The two players have 10 available points. They can distribute between 0 and 10 points to their partner (i.e., opponent player in the game). The given points are doubled and allocated as partner's score. Each player can obtain the maximum score if receives all 10 points from the partner. In this case the score is 30. If both players defeat (i.e., non-cooperate), they receive only 10 points. If they both cooperate, they receive 20 points.



(a): Player 1 and Player 2 cooperate (CC).

(b): Player 1 cooperates and Player 2 defects (CD)



(c): Player 1 defects and Player 2 cooperates (DC)

(d): Player 1 and Player 2 defect (DD)

Figure 5: Decision options for Player 1 and Player 2.

Figure 6 shows the main Tool GUI with the two matrixes of the game.

	Cooperate	Non-cooperate
Cooperate	R = 20; R = 20	S = 0; T = 30
Non-cooperate	T = 30; S = 0	P = 10; P = 10

Figure 7. Payoff matrixes.



Figure 6. Payoff matrixes.

The tool allows us to simulate simple instances of the prisoner's dilemma. Figure 8 shows the decision tree resulting from a simulation of the game. The graphical representation supports ease understanding of the strategies. It is also possible to change strategies easily. This allows exploratory approaches to strategies. Therefore, the tool supports learning-by-experience approaches in order to learn and understand the concept of trust.

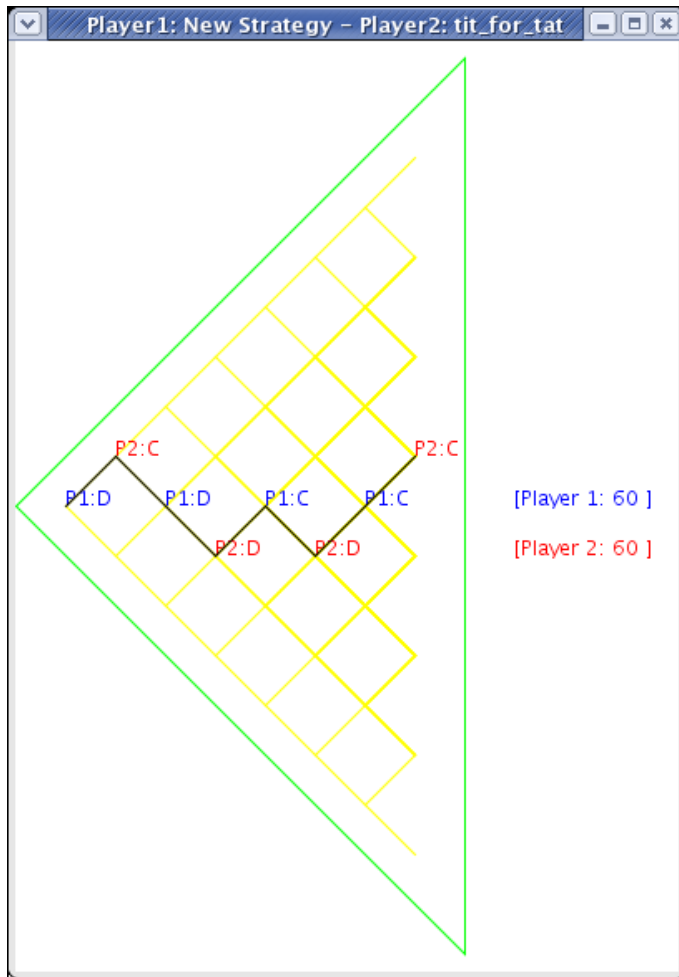


Figure 8. A decision tree.

6 CONCLUSIONS

This paper reviews diverse models of trust. The review highlights the complexity and multidisciplinary of trust. Although different models capture to some extent the concept of trust, it is necessary further to understand trust dynamics (e.g., trust formation and evolution). The prisoner's dilemma provides a characterization of trust. Trust games extending the prisoner's dilemma allow us to understand and experience different trust aspects (e.g., strategies).

The paper introduces a software tool for the simulation of trust games. Although the tool implements simple functionalities, it already allows us to adopt exploratory learning-by-experience approaches to trust. The simulations of practical scenarios highlight how the tool captures trust games where cooperation (or competition) emerges. The tool supports the understanding of trust dynamics (e.g., trust strategies, interactions, payoff matrixes and trust evolution). In particular, the tool allows us to play asymmetric trust games. These games highlight trust as depending on the interaction between payoff matrixes and strategies. This emphasizes trust dependencies and dynamics. Therefore, the tool is a valuable support for learning and understanding trust.

ACKNOWLEDGEMENTS

The authors would like to thank Stuart Anderson and Domenico Cantone for their support.

REFERENCES

- Anderson, R. 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons.
- Axelrod, R. 1990. *The Evolution of Cooperation*. Penguin Books.
- Barber, B. 1983. *The Logic and Limits of Trust*. Rutgers University Press, New Brunswick, NJ.
- Blaze, M., Feigenbaum, J. & Lacy, J. 1996. Decentralized trust management. In *Proceedings of the IEEE Conference on Security and Privacy*.
- Carbone, M., Nielsen, M. & Sassone, V. 2003. A formal model of trust in dynamic networks. In *Proceedings of the First International Conference on Software Engineering and Formal Methods (SEFM'03)*. IEEE Computer Society.
- Corritore, C.L., Kracher, B., & Wiedenbeck, S. 2003. On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies* 58, 737–758.
- Dassonville, I., Jolly, D. & Desodt, A.M. 1996. Trust between man and machine in a teleoperation system. *Reliability Engineering & System Safety* 53, 319–325.
- Dixit, A.K. & Nalebuff, B.J. 1991. *Thinking Strategically: The Competitive Edge in Business, Politics, and Everyday Life*. W.W. Norton & Company.
- Douglas, M. & Wildavsky, A. 1982. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers*. University of California Press.
- Falcone, R. & Castelfranchi, C. 2001. The socio-cognitive dynamics of trust: Does trust create trust? In Falcone, R., Singh, M. & Tan, Y.-H. (Eds.), *Trust in Cyber-societies*, Number 2246 in LNAI, pp. 55–72. Springer-Verlag.
- Fenton, N.E. & Pfleeger, S.L. 1996. *Software Metrics: A Rigorous and Practical Approach (Second Edition)*. International Thomson Computer Press.
- Gefen, D., Rao, V.S. & Tractinsky, N. 2003. The conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. In *Proceedings of the 36th Hawaii International Conference on Systems Sciences (HICSS'03)*. IEEE.
- Grabner-Kräuter, S. & Kalascha, E.A. 2003. Empirical research in on-line trust: a review and critical assessment. *International Journal of Human-Computer Studies* 58(6), 783–812.
- Grandison, T. & Sloman, M. 2000. A survey of trust in internet application. *IEEE Communications Surveys & Tutorials* 3(4).
- Jensen, C., Farnham, S.D., Drucker, S.M. & Kollock, P. 2000. The effect of communication modality on cooperation in online environments. In *Proceedings of CHI 2000*, pp. 470–477. ACM.
- MacKenzie, D. 2004. Social connectivities in global financial markets. *Environment and Planning D: Society and Space* 22, 83–101.
- MacKenzie, D.A. & Wajcman, J. (Eds.) 1999. *The Social Shaping of Technology* (2nd ed.). Open University Press.
- McKnight, D.H. & Chervany, N.L. 1996. The meanings of trust. Technical Report 96-04, University of Minnesota.
- McKnight, D.H. & Chervany, N.L. 1996. The meanings of trust. Technical Report 96-04, University of Minnesota.
- McKnight, D.H. & Chervany, N.L. 2000. What is trust? a conceptual analysis and an interdisciplinary model. In *Proceed-*

- ings of the Americas Conference on Information Systems, pp. 827–833.
- McKnight, D.H. & Chervany, N.L. 2001a. Conceptualizing trust: A typology and ecommerce customer relationships model. In *Proceedings of the 34th Hawaii International Conference on System Sciences*, pp. 1–9. IEEE.
- McKnight, D.H. & Chervany, N.L. 2001b. Trust and distrust definitions: One bite at a time. In Falcone, R., Singh, M. & Tan, Y.-H. (Eds.), *Trust in Cyber-societies*, Number 2246 in LNAI, pp. 27–54. Springer-Verlag.
- Moray, N., Hiskes, D., Lee, J. & Muir, B.M. 1995. Trust and human intervention in automated systems. In Hoc, J.-M. Cacciabue, P.C. & Hollnagel, E. (Eds.), *Expertise and Technology: Cognition & Human-Computer Cooperation*, pp. 183–194. Lawrence Erlbaum Associates.
- Muir, B. 1994. Trust in automation: part I. Theoretical issues in the study of trust and human intervention in automated system. *Ergonomics* 37, 1905–1922.
- Muir, B. & Moray, N. 1996. Trust in automation: part II. Experimental studies of trust and human intervention in a process control simulation. *Ergonomics* 39, 429–460.
- Nalebuff, B.J. & Brandenburger, A.M. 1996. *Co-opetition*. HarperCollinsBusiness.
- Nielsen, M. & Krukow, K. 2003. Towards a formal notion of trust. In *Proceedings of PPD'03*. ACM.
- Pasquini, A., Pistolesi, G. & Rizzo, A. 2001. Reliability analysis of systems based on software and human resources. *IEEE Transactions on Reliability* 50(4), 337–345.
- Rempel, J.K., Holmes, J.G. & Zanna, M.P. 1985. Trust in close relationships. *Journal of Personality and Social Psychology* 49(1), 95–112.
- Riegelsberger, J., Sasse, M.A. & McCarthy, J.D. 2003. The researcher's dilemma: evaluating trust in computer-mediated communication. *International Journal of Human-Computer Studies* 58(6), 759–781.
- Uggirala, A., Gramopadhye, A.K., Melloy, N.J. & Toler, J.E. 2004. Measurement of trust in complex and dynamic systems using a quantitative approach. *International Journal of Industrial Ergonomics* 34(3), 175–186.