



UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Enhancing Trustability in MMOGs Environments

Rui João Morais de Almeida Costa Cardoso

Tese para a obtenção do Grau de Doutor em
Engenharia Informática
(3º Ciclo de Estudos)

Orientador: Prof. Dr. Abel João Padrão Gomes (Universidade da Beira Interior)
Co-orientador: Prof. Dr. Mário Marques Freire (Universidade da Beira Interior)

Covilhã, Janeiro 2017

This thesis was conducted under Professor Abel João Padrão Gomes supervision with Professor Mário Marques Freire as co-supervisor. The research work that sustain this doctoral dissertation was developed within the NAP-Cv (Network Architectures and Protocols - Covilhã) at *Institute of Telecommunications* (Instituto de Telecomunicações), University of Beira Interior, Portugal.



instituto de
telecomunicações



UNIVERSIDADE DA BEIRA INTERIOR
Covilhã | Portugal

The thesis was financed by the Portuguese Research Agency, *Foundation for Science and Technology* (*Fundação para a Ciência e a Tecnologia*) through grant contract SFRH /BD /79567 /2011 under the Human Potential Operational Program Type 4.1 Advanced Training POPH (Programa Operacional Potencial Humano), within the National Strategic Reference Framework QREN (Quadro de Referência Estratégico Nacional), co-funded by the European Social Fund and by national funds from the Portuguese Education and Science Minister (Ministério da Educação e Ciência).



Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA



QUALIFICAR É CRESCER.



QUADRO
DE REFERÊNCIA
ESTRATÉGICO
NACIONAL
PORTUGAL 2007-2013



Governo da República
Portuguesa



UNIÃO EUROPEIA
Fundo Social Europeu

*Eu quero dedicar esta tese à Luz, ao Afonso e à Céu.
Em suma, à minha família, a principal prejudicada pela
minha “ausência” durante estes anos.*

I want to dedicate this thesis to Luz, Afonso and Céu.

Acknowledgments

First and foremost, I would like to thank my thesis supervisor Professor Abel João Padrão Gomes. It was due to him that I started this dissertation endeavor. I would never have been able to finish this thesis without his invaluable and permanent support. Always enthusiastic and supportive, encouraging me in every step of the way. Always available to tackle every bottleneck. His thorough and careful reviewing skills contributed decisively to the quality of the papers produced.

I would like also, to give my appreciation to Professor Mário Freire for agreeing to be my thesis co-supervisor and for his insightful feedback in reviewing my papers.

Special thanks to João, Carlos and Rui, for their friendship. In many occasions, our fruitful discussions, contributed to kept me focus in the final goal.

I would like to thank to the Portuguese Research Agency, *Foundation for Science and Technology (Fundação para a Ciência e a Tecnologia)* for funding this research.

I also must acknowledge and thank the *Institute of Telecommunications* (Instituto de Telecomunicações) for providing the facilities for the research at *Communications and Multimedia Laboratory in IT Covilhã*.

Thanks also extended to the University of Beira Interior and its Informatics Center for hosting the rack servers used in the research work.

Finally, and most importantly, I would like to thank my family. Specially to my wife Céu, my son Afonso and daughter Luz for their unconditional love and support. Also to my father João thank you, for everything. And finally, to my sister Sandra, for making me believe that I could finish this.

Foreword

This thesis is submitted to the University of Beira Interior (UBI) for the fulfillment of requirements for the degree of Doctor of Philosophy in Informatics Engineering to be present in a public dissertation examination session.

The research work reproduced in this thesis is the result of an independent work developed by Rui Costa Cardoso.

The research was performed at IT Covilhã, University of Beira Interior, Portugal.

List of Publications

List of publications produced during the doctoral research program that are included in the thesis.

- P1** Cardoso, R. C. and Gomes, A. *Security Issues in Massively Multiplayer Online Games*. In M. Cruz-Cunha (Ed.), *Handbook of Research on Serious Games as Educational, Business and Research Tools: Development and Design*, IGI Global, pp. 290-314, February, 2012.
doi:10.4018/978-1-4666-0149-9.ch016
- P2** Rui Costa Cardoso and Abel Gomes. *Towards a trust framework for multi-user virtual environments*. In Beniamino Murgante, Sanjay Misra, Ana Maria A. C. Rocha, Carmelo Torre, Jorge Gustavo Rocha, Maria Irene Falcão, David Taniar, Bernady O. Apduhan, and Osvaldo Gervasi (Eds.), *Computational Science and Its Applications (ICCSA'2014)*, *Lecture Notes in Computer Science*, Vol. 8579, pp. 754-768, Springer-Verlag, 2014.
doi:10.1007/978-3-319-09144-0-52
- P3** R. C. Cardoso; A. J. P. Gomes; M. M. Freire, *A User Trust System for Online Games - Part I: An Activity Theory Approach for Trust Representation*, *IEEE Transactions on Computational Intelligence and AI in Games* (published first online on July 19, 2016).
doi:10.1109/TCIAIG.2016.2592965
- P4** R. C. Cardoso, A. Gomes, and M. Freire, *A User Trust System for Online Games - Part II: A Subjective Logic Approach for Trust Inference*, *IEEE Transactions on Computational Intelligence and AI in Games* (published first online on July 19, 2016).
doi:10.1109/TCIAIG.2016.2593000
- P5** Cardoso, Rui Costa, and Gomes, Abel, and Freire, Mário. *Trust models for massively multiuser virtual environments: a comparative approach* (to be submitted for publication).

Resumo

MMOGs (Massively Multiplayer Online Games, como por exemplo, World of Warcraft), mundos virtuais (VW, como por exemplo, o Second Life) e redes sociais (como por exemplo, Facebook) necessitam de mecanismos de confiança mais autónomos, capazes de assegurar a segurança e a confiança de uma forma semelhante à que os seres humanos utilizam na vida real. Como se sabe, esta não é uma questão fácil. Porque confiar em seres humanos e ou organizações depende da percepção e da experiência de cada indivíduo, o que é difícil de quantificar ou medir à partida. Na verdade, esses ambientes sociais carecem dos mecanismos de confiança presentes em interacções humanas presenciais. Além disso, as interacções mediadas por dispositivos computacionais estão em constante evolução, necessitando de mecanismos de confiança adequados ao ritmo da evolução para avaliar situações de risco.

Em VW/MMOGs, é amplamente reconhecido que os utilizadores desenvolvem relações de confiança a partir das suas interacções no mundo com outros. No entanto, essas relações de confiança acabam por não ser representadas nas estruturas de dados (ou bases de dados) do VW/MMOG específico, embora às vezes apareçam associados à reputação e a sistemas de reputação. Além disso, tanto quanto sabemos, ao utilizador não lhe é facultado nenhum mecanismo que suporte uma ferramenta de confiança individual para sustentar o seu processo de tomada de decisão, enquanto ele interage com outros utilizadores no mundo virtual ou jogo. A fim de resolver este problema, bem como os mencionados acima, propomos nesta tese uma representação formal para essas relações de confiança pessoal, baseada em interacções avatar-avatar. A ideia principal é fornecer a cada jogador representado por um avatar uma ferramenta de confiança pessoal que segue um modelo de confiança distribuída, ou seja, os dados de confiança são distribuídos através da rede social de um determinado VW/MMOG.

Representar, manipular e inferir a confiança do ponto de utilizador/jogador, é certamente um grande desafio. Quando alguém encontra um indivíduo desconhecido, a pergunta é “Posso confiar ou não nele?”. É claro que isto requer que o utilizador tenha acesso a uma representação de confiança sobre os outros, mas, a menos que possamos usar uma plataforma VW/MMOG de código aberto, é difícil – para não dizer impossível – obter acesso aos dados gerados pelos utilizadores. Mesmo em sistemas de código aberto, um número de utilizadores pode recusar partilhar informações sobre seus amigos, conhecidos, ou sobre outros. Ao juntar seus próprios dados com os dados obtidos de outros, o utilizador/jogador representado por um avatar deve ser capaz de produzir uma avaliação de confiança sobre o utilizador/jogador com o qual se encontra a interagir. Relativamente ao método de avaliação de confiança empregue nesta tese, utilizamos lógica subjectiva para a representação da confiança, e também operadores lógicos da lógica subjectiva juntamente com algoritmos de procura em grafos para empreender o processo de inferência da confiança relativamente a outro utilizador. O sistema de inferência de confiança proposto foi validado através de um número de cenários Open-

Enhancing Trustability in MMOGs Environments

Simulator (opensimulator.org), que mostrou um aumento na precisão na avaliação da confiança de avatares.

Resumindo, a nossa proposta visa, assim, introduzir uma teoria de confiança para mundos virtuais, conjuntamente com métricas de avaliação de confiança (por exemplo, a lógica subjectiva) e em métodos de procura de caminhos de confiança (com por exemplo, através de métodos de pesquisa em grafos), partindo de uma base individual, em vez de se basear em sistemas habituais de reputação centralizados. Em particular, e ao contrário de outros métodos de determinação do grau de confiança, os nossos métodos são executados em tempo real.

Palavras-chave

Confiança,
Interacções,
Jogos Online Massivos Multi-jogador,
Lógica Subjectiva,
Modelos de Confiança,
Mundos Virtuais,
Pesquisa em Grafos.

Abstract

Massively Multiplayer Online Games (MMOGs; e.g., World of Warcraft), virtual worlds (VW; e.g., Second Life), social networks (e.g., Facebook) strongly demand for more autonomic, security, and trust mechanisms in a way similar to humans do in the real life world. As known, this is a difficult matter because trusting in humans and organizations depends on the perception and experience of each individual, which is difficult to quantify or measure. In fact, these societal environments lack trust mechanisms similar to those involved in humans-to-human interactions. Besides, interactions mediated by compute devices are constantly evolving, requiring trust mechanisms that keep the pace with the developments and assess risk situations.

In VW/MMOGs, it is widely recognized that users develop trust relationships from their in-world interactions with others. However, these trust relationships end up not being represented in the data structures (or databases) of such virtual worlds, though they sometimes appear associated to reputation and recommendation systems. In addition, as far as we know, the user is not provided with a personal trust tool to sustain his/her decision making while he/she interacts with other users in the virtual or game world. In order to solve this problem, as well as those mentioned above, we propose herein a formal representation of these personal trust relationships, which are based on avatar-avatar interactions. The leading idea is to provide each avatar-impersonated player with a personal trust tool that follows a distributed trust model, i.e., the trust data is distributed over the societal network of a given VW/MMOG.

Representing, manipulating, and inferring trust from the user/player point of view certainly is a grand challenge. When someone meets an unknown individual, the question is “Can I trust him/her or not?”. It is clear that this requires the user to have access to a representation of trust about others, but, unless we are using an open source VW/MMOG, it is difficult —not to say unfeasible— to get access to such data. Even, in an open source system, a number of users may refuse to pass information about its friends, acquaintances, or others. Putting together its own data and gathered data obtained from others, the avatar-impersonated player should be able to come across a trust result about its current trustee. For the trust assessment method used in this thesis, we use subjective logic operators and graph search algorithms to undertake such trust inference about the trustee. The proposed trust inference system has been validated using a number of OpenSimulator (opensimulator.org) scenarios, which showed an accuracy increase in evaluating trustability of avatars.

Summing up, our proposal aims thus to introduce a trust theory for virtual worlds, its trust assessment metrics (e.g., subjective logic) and trust discovery methods (e.g., graph search methods), on an individual basis, rather than based on usual centralized reputation systems. In particular, and unlike other trust discovery methods, our methods run at interactive rates.

Keywords

Interactions,
Graph Search,
Massive Multiplayer Online Games,
Subjective Logic,
Trust,
Trust Models,
Virtual Worlds.

Contents

Dedictory	v
Acknowledgments	vii
Foreword	ix
List of publications	xi
Resumo	xiii
Abstract	xv
List of Figures	xxi
List of Tables	xxii
Acronyms	xxiii
Terminology	xxv
1 Introduction	1
1.1 Motivation	1
1.2 Problem Outline	2
1.3 Thesis Statement	3
1.4 Research Objectives	3
1.5 Contributions	5
1.6 Publications	6
1.7 Thesis Structure	8
2 Security Issues	11
2.1 Introduction	11
2.2 Related Work	12
2.3 Massively Multiplayer Online Games	13
2.4 Architecture	15
2.5 Threats and Vulnerabilities	16
2.5.1 Game Economy	16
2.5.2 Strong Social Interaction	16
2.5.3 Real Time Interaction	16
2.5.4 Poor Law Enforcement Schemes	17
2.5.5 Game Design and Development	17
2.6 Risk Assessment	17
2.7 Security	18
2.8 Security Dimensions	19
2.8.1 Game Client	19
2.8.2 Game Communications	20

Enhancing Trustability in MMOGs Environments

2.8.3	Game Virtual Environment	21
2.8.4	Game Server	24
2.8.5	Player	25
2.9	Security Evaluation	26
2.9.1	Asset identification	27
2.9.2	Threat classification	30
2.10	Security Framework	34
2.11	Summary	36
3	Trust in Virtual Worlds	37
3.1	Introduction	37
3.1.1	Trust in VW/MMOGs	37
3.1.2	Trust Approaches	38
3.1.3	Other Surveys	38
3.1.4	Outline	40
3.2	Trust Studies	41
3.2.1	Historical Notes	42
3.2.2	Trust in Social Sciences	42
3.2.3	Trust in Computer Science	46
3.3	Trust-Influencing Factors	49
3.3.1	Main Trust Factors	50
3.3.2	Other Trust Factors	52
3.4	Trust Properties	53
3.5	Trust Inference Process	55
3.6	Trust Models	57
3.6.1	Trust Modeling Framework	57
3.6.2	Trust and Reputation Models	60
3.7	Discussion	80
3.8	Summary	81
4	Trust Framework	83
4.1	Introduction	83
4.2	Related Work	84
4.3	Multi-user Virtual Environments	86
4.3.1	Types of VW/MMOGs	86
4.3.2	Interactions	86
4.3.3	Trustworthiness	87
4.3.4	Trust Data Sources	88
4.4	Trust framework	89
4.4.1	Input	90
4.4.2	Output	93
4.5	Discussion	93
4.6	Summary	94

5	Trust Representation	95
5.1	Introduction	95
5.1.1	Research Questions	97
5.1.2	Methodology	97
5.1.3	Organization of the Chapter	98
5.2	Related Work	98
5.3	Interactions	99
5.3.1	Activities	100
5.3.2	Interactions	101
5.3.3	Avatar-Avatar Interactions	102
5.3.4	Actions and Events	104
5.3.5	Collecting Interaction Data from Events	107
5.4	Trust Relationships	109
5.4.1	Trust Relationships	109
5.4.2	Plain Trust Networks	111
5.4.3	A Case Study Example	112
5.5	Trust Opinions	114
5.5.1	Opinions and Subjective Logic	115
5.5.2	Trust Relationship-Opinion Conversion	117
5.5.3	Abstract Case Study: A Revisited Example	117
5.6	Assembling Trust Networks	118
5.7	User's Trust Inference System	119
5.7.1	First Stage: Collecting Avatar-Avatar Interactions	119
5.7.2	Second Stage: Storing Trust Relationships and Opinions	119
5.7.3	Third Stage: Trust Assessment	120
5.8	Discussion	121
5.9	Summary	122
6	Trust Inference	123
6.1	Introduction	123
6.1.1	Motivation	124
6.1.2	Contributions	124
6.1.3	Organization of the Chapter	124
6.2	Personal Trust System: an Overview	125
6.2.1	Collecting (1st stage)	126
6.2.2	Representing (2nd stage)	126
6.2.3	Assessing (3rd stage)	128
6.3	Finding Trust Paths	128
6.3.1	Finding Paths using BFS	131
6.3.2	Finding Paths using DFS	134
6.4	Subjective Logic - based Trust Operators	135
6.4.1	Trust Opinions	135
6.4.2	Discount Operator	136

Enhancing Trustability in MMOGs Environments

6.4.3	Consensus Operator	136
6.4.4	Trust Inference Scenario	137
6.5	Simulation Experiments and Discussion	142
6.5.1	Simulation Scenarios and Experiments Settings	142
6.5.2	Experiment 1: Absence of Trust Modeling	145
6.5.3	Experiment 2: Existence of Trust Modeling	147
6.5.4	Experiment 3: Trust Modeling per User Category	148
6.5.5	Experiment 4: Trust Modeling for Malicious Users	149
6.5.6	Experiment 5: Trust Modeling for Mixed Misbehaved Users	152
6.5.7	Experiment 6: Impact of Trust Computing Time	153
6.6	Discussion	154
6.7	Summary	156
7	Conclusions	157
7.1	Context of the Research Work	157
7.2	Research Questions	158
7.3	Contributions	159
7.4	Research Limitations and Future Work	159
	Bibliography	161

List of Figures

2.1	MMOGs users perception on value of assets	29
2.2	MMOGs player assets	29
2.3	MMOGs game overall assets	30
3.1	Social Sciences areas that employ trust conceptualizations	43
3.2	Computer science areas that employ trust conceptualizations.	46
3.3	Trust cycle	54
3.4	Trust properties and influence factors.	54
3.5	The trust decision making process	55
3.6	Trust computational model key components.	57
3.7	Data sources.	58
3.8	Trust methods.	60
4.1	Trust Framework	93
5.1	Hierarchical structure of data gathering.	101
5.2	Interaction process within an OpenSimulator's client window.	102
5.3	Interaction process.	103

5.4	Action types of the interaction between A , B , and C over time.	104
5.5	Actions	105
5.6	OpenSimulator architecture and services.	105
5.7	Recording A interactions with others in A Aol.	108
5.8	A plain trust network \mathbb{T} concerning avatar interactions in a region. . . .	112
5.9	Individual trust networks (\mathbb{T}_i) of 7 avatars interacting in a game scenario.	113
5.10	Opinion in the subjective logic space triangle	115
5.11	Example of an extended trust network \mathbb{T}_e^A for A	119
5.12	Trust inference system.	120
6.1	Pipeline of our personal trust system.	125
6.2	A trust network \mathbb{T} from avatar interactions in OpenSimulator.	132
6.3	Individual trust networks (\mathbb{T}_i) of 7 avatars.	132
6.4	Extended individual trust network \mathbb{T}_A for A	132
6.5	Breath First Search process initiated from avatar A	133
6.6	Digraph of BFS paths from trustor A	133
6.7	Extended individual trust network \mathbb{T}_A for A	134
6.8	Depth First Search initiated from A	134
6.9	DFS paths from trustor A	134
6.10	Aggregated results of the BFS/DFS paths linking <i>trustor</i> and <i>trustee</i> . . .	135
6.11	Transitive trust derivation with operator discount (\otimes).	136
6.12	Trust aggregation with operator consensus (\oplus).	137
6.13	Digraph representing the trust network \mathbb{T}_E^A	140
6.14	OpenSim region with 500 avatars an 50 misbehaved.	143
6.15	Impact on user performance from rising the number of misbehaved users.	146
6.16	Effect on performance from rising the number of misbehaved users. . .	147
6.17	Effect on the performance from rising the number of sybil users.	149
6.18	Effect on the performance from rising the number of malicious users. .	150
6.19	Impact on performance due to purely malicious users.	150
6.20	Effect on the performance from rising users and interactions.	151
6.21	Impact of the volume variation in the performance of honest users. . .	152
6.22	Trust computing time impact under different conditions.	154

List of Tables

2.1	MMOG's game client threat-asset association and comparison	31
2.2	MMOG's network threat-asset association and comparison	31
2.3	MMOG's game environment threat-asset association and comparison . .	32
2.4	MMOG's game server threat-asset association and comparison	33

Enhancing Trustability in MMOGs Environments

2.5	MMOG's player threat-asset association and comparison	34
3.1	Surveys on trust models.	39
3.2	Testbeds and their trust models.	41
3.3	Comparison on how trust is used in society versus VW/MMOGs.	45
3.4	Comparison of trust usability in different areas versus VW/MMOGs.	47
3.5	Trust related concepts and VW/MMOGs counterpart.	50
3.6	Trust influential factors from real world situations.	52
3.7	Trust models and their sources and trust methods (engines).	61
5.1	Types of users activities in VW/MMOGs.	101
5.2	Deployed Events.	106
6.1	Data formats.	126
6.2	Honesty-based behavior models.	143

Acronyms

AI	Artificial Intelligence
Aol	Area of Interest
Captchas	Completely Automated Public Turing Test to Tell Computers and Humans Apart
DOS	Denial of Service
DDoS	Distributed Denial of Service
DRM	Digital Rights Management
EULA	End-user License Agreement
FPS	First-Person Shooter
HCI	Human Computer Interactions/Interfaces
IT	Instituto de Telecomunicações
IM	Instant Messaging
MANET	Mobile Ad hoc Network
MAS	Multi-agent Systems
MMO	Massively Multiplayer Online Game (shortened version)
MMOG	Massive Multiplayer Online Game
MUVEs	Multi-user virtual environments
NPC	Non player characters (automated avatars controlled by the service provider)
ODR	Online dispute resolution
P2P	Peer-to-Peer
PDF	Probability Density Function
PKI	Public Key Infrastructure
PvP	Player vs Player
RPG	Role-Playing Game
SL	Subjective Logic
ToU	Terms of Use
TNA-SL	Trust Network Analysis with Subjective Logic
UBI	Universidade da Beira Interior
VE	Virtual Environment
VW	Virtual World
VWs	Virtual Worlds
WoW	World of Warcraft

Terminology

Avatar	A 3D graphical representation of a character used in MMO/VWs, It is a user “ <i>alter ego</i> ” representation in-world that characterize how users are represented and perceived within the virtual world, usually as a 3D rendering customizable avatar representation of an human or humanoid being
Captchas	Are challenge-response tests whose purpose is to ascertain whether a particular user is human. The test is frequently used to identify human users and block computerized applications when signing up, for some forms of internet accounts. An example of this use is to block “bot” players. Usually the test involves the recognition of a distorted image of letters and numbers.
Ganking	Attacking another player without warning, when he is distracted, with low health, engaged with other activity. Usually meaning that the attack occur when the targeted player is at high level disadvantage.
Griefing	Playing a game simply to aggravate and harass other players.
Guild	Represents an association of players in a MMOG/VW with similar interests or pursuits. Guilds are formal alliances that foment the sense of belonging. After joining, usually the guild name is showed above the player’s avatar for easy identification. It also common for MMOG to provide guild specific chat channels to ease guild member communication.
Inventory	Represents a set of assets associated with the user (e.g., clothes, items, scripts).
Lag	Represent a perceptible delay between the action of players and the reaction of the server resulting in having players with slower reactions allowing the others to obtain advantage within game environment as their actions are processed faster by the game server. Although lag may be caused by high latency, it may also occur due to insufficient processing power in the client. Lag can also happen in single player games as well.
NPCs	Are game controlled artificial intelligences, designed to mimic the actions of human players. Their purpose is to provide some challenge to players and to populate the MMOG virtual world.
Region or Shard	A subdivision of the MMO/VW virtual world, usually served by a single server. These sharded worlds are independent instances of the game-world running on its own. Sharding also reduces the complexity of distributed game state coordination. Constitute a game developer solution to MMOG scalability problem. As a hundred of thousands of simultaneous players, could not be at the same time in the same precise location. A solution to maintain a pleasant game experience to all was to split players by their geographic location, creating copies of the game world known as shards. Boosting network performance and reducing packet delay. The disadvantage is that players cannot physically interact or usually even communicate across “shards”.
Virtual World	Is a 3D immersive scenario representation including the landscape, avatars, animations and existing objects.

Chapter 1

Introduction

The present thesis fits in the field of trust and reputation systems. In the literature, we find trust and reputation models for multi-agent systems (MAS), wireless sensor networks (WSNs), vehicular ad-hoc networks (VANETs), but, as far as we know, this thesis addresses the first trust and reputation model designed for virtual worlds and massively multiplayer online games (VW/MMOGs).

1.1 Motivation

Trust is a challenging concept. Intuitively, most people understand what is trust, but its representation and modeling in computational systems is not an easy task, largely because of its context-dependence and subjectivity. In computing, trust has been used broadly across a number of topics, disciplines, and applications [AG07], namely networking security, reliability in distributed systems, intelligent systems, game theory, and so forth. Moreover, as [JIB07] noted sometime ago, there is not yet a consolidated basis to build up a general trust theory from which we can derive a computable trust model. Instead, we have assisted to the appearance of specific trust models that depend on a particular domain of application.

Some examples of domain-specific trust models are as follows. In online services, [CKW03] noted that the perception of credibility, ease of use, and risk implications have a direct impact on how trust is perceived. These three trust factors play also an important role in player's perception when he/she interacts with the game services. In the context of e-markets, it is common to have a reputation-based trust model that multi-agent systems can use to protect agents from malicious traders [You07]. This model can be easily transposed to trading activities inside MMOGs or other virtual worlds. Another trust dimension has to do with user profiling. In [LDRL09], Liu describes a computational stereotypes-based trust model to determine trust even when player's interactions do not match the available user profiles. It is clear that user profiling provides a valuable insight for trust in MMOGs.

Summing up, in trust computing research, we find two ways of approaching trust. The first is a domain-specific trust approach [AG07], while the second tries to come to a general and abstract model for trust [MDH02]. The latter is due to Marsh [Mar94], and is an attempt of formalizing trust as a computational concept. Obviously, further attempts have been made in order to understand limitations in existing trust models, having been even addressed the problem of mimicking the real life social trust in digital

or virtual worlds [Yan08b].

In this thesis, we put forward a domain-specific trust model in the sense it was designed for VW/MMOGs, not for e-commerce, social networks, wireless sensor networks, or else. However, we intend to introduce a general model from the psychological and sociological point views that applies to both humans and virtual characters (or avatars impersonating humans). Thus, this model has to do with events and interactions between avatars *within* a virtual/game world.

1.2 Problem Outline

What is interesting about MMOGs is that they seem to reunite most trust flavors we can experience in real life, so that we believe that MMOGs provide the ideal testbed to come out with a general trust theory and computable trust model. In general terms, and following [RK05], we find three major approaches of modeling trust in computer-mediated systems: infrastructure trust, services trust, and community trust. As expected, these trust dimensions are also present in MMOGs, which reinforce the idea that MMOGs can work as a testbed to modeling trust in interactive virtual worlds in the future [Noo10].

According to [RK05], those three trust dimensions can be hierarchically stratified into three layers. The bottom layer concerns *infrastructure trust*, which corresponds to the initial research on trust endeavored by [Nib79]. Currently, this layer corresponds to key enablers for the development of a trustworthy Information Society (IS) like secure and trusted Information and Communication Technology (ICT) infrastructures [VCS07], as well as the evolution and challenges regarding trust and security in ICT infrastructures [Var09]. The middle layer *service trust* relates to trust in online services [MS04], and currently focuses on web services [WBOM15, ZWZL15] and the effective role of trust in software services [DCK16], as well as trust developments on cloud services [BS16]. The top layer has to do with *community trust*, and is where reputation systems aggregate information about the past behaviors of a group of entities as community's shared perception [ARH00]. In our view, this can be extrapolated to consider other situations in which trust can be drawn from different communities like social networks [SNP13] [GOG13], or even in immersive environments like VW/MMOGs, addressing avatar behaviors in virtual communities [ORMCB12], or to enhance community participation and increase the gaming experience [BHR509]. Of particular interest is to realize how sociological factors affect trust development in virtual communities [DH08].

In this thesis, we are not interested in infrastructure and service trust, but only on *community trust* concerning the aforementioned top layer. This is so because infrastructures and services are more connoted with contexts like networks and online services. On the contrary, we are interested in studying trust inside immersive virtual worlds from psychological and sociological points of view, i.e., how avatars relate with one another as the humans do in real life. Therefore, this thesis focuses on trustability in MMOGs,

in particular on trust between avatars living in the virtual environment.

1.3 Thesis Statement

Currently, trust is not represented and handled in a computable form *within* the virtual world. This immersive perception of trust in virtual worlds is a distinctive factor in relation to other trust modeling solutions, namely those used in multi-agent systems (MAS) and networks. In fact, as in the real world, avatars see and hear other avatars within a virtual world, so that their visual appearance, their poses and speech may provoke a number of emotions that influence the way an avatar evaluates the trustworthiness of another.

Following the leading idea of mimicking real-world trust in virtual worlds, we promptly realize that relations established between virtual users (or avatars) result from the interactions between them. These interactions generate data that can be employed by the virtual engine to update each user's status and rendering their avatar actions. Therefore, the thesis statement that corroborates our claims is:

Assuming that in-world data generated from avatar-avatar interactions can be employed to derive a trust representation for each individual user, will it be feasible to have an in-world trust assessment mechanism suitable to support and enhance users' trust decisions?

Indeed, this thesis proposes a new trust approach in VW/MMOGs, which is based on an individual trust representation (i.e., a decentralized trust representation) which is built upon direct interactions between avatars impersonating users or players. In addition, we will show that no centralized reputation system is necessary to users in their trust decisions about others, and this holds even when an avatar meets an unknown avatar. This is accomplished using an inference mechanism that combines graph searching (or pathfinding) together with subjective logic [Jøs13].

1.4 Research Objectives

As mentioned above, trust is not a new research topic in computer science, pervading areas as diverse as networking security, reliability in distributed systems, game theory, etc. But, trust building in computer-mediated social environments such as MMOGs, where multiple players coexist and interact using multiple communication channels like sight, hearing, as well as some channels outside the game, is not so common, and thus this constitutes the grand challenge of the research work underlying this thesis.

Recall that MMOGs commonly use centralized and proprietary reputation systems to keep privacy and anonymity of players, so that trust is only considered in a limited manner, simply because proprietary systems basically release data concerning player's

Enhancing Trustability in MMOGs Environments

game scoring, not classified trust data. But, as known, reputation systems have several drawbacks, mainly because reputation feedback can be used to maliciously degrade other player reputation and, consequently, the reputation system, and the game itself.

With all this in mind, the main *objective* (or general objective) we pursue in this doctoral thesis is to show that trust can be deployed in immersive worlds, where each individual avatar/user makes trust decisions about those with whom he/she interacts, in a similar way as humans do in real life. In terms of research *goals* (or specific objectives), they are the following:

- To introduce the state-of-the-art concerning trust models developed within different fields, aiming with that process to identify suitable trust modeling solutions for VW/MMOGs.
- To devise a general security framework for MMOGs in order to identify their specific malware and cheating problems, as well as possible solutions.
- To develop an innovative individual-based trust model in contrast to the common global reputation systems. We believe that this trust model deployed within MMOGs is less prone to defamation and ganking than current reputation systems.
- To develop a trust inference procedure capable of providing a mean of measuring trust in MMOGs, using for that purpose solutions that consider the subjectivity of human behaviors. In particular, we believe that subjective logic due to [Jøs13] can work as a suited trust metric in MMOGs.

The objectives mentioned above are the milestones of the doctoral work that lead to the design and development of a trust model for VW/MMOGs. Let us now address the specific objectives in more detail:

State of the Art. The value of modeling and reasoning about trust computationally has been increasingly recognized in computing communities. Trust conceptualizations are employed in many areas for addressing different types of issues. But, in VW/MMOGs, trust mechanisms that provide or induce trustability are scarce. Therefore, we survey multiple trust models from different fields to assess their viability in VW/MMOGs.

Security framework. Online games and MMOGs rises a number of security-related issues, namely: player authentication, game availability and resilience, trust and anonymity concerns, means of ensuring security of player and his/her virtual assets, cheating, ganking, gold farming, game law enforcing solutions, game client problems, and also game development issues like scalability and persistence. Therefore, MMOGs have the same security risks as other online applications, but also present new and interesting challenges as a consequence of the risks mentioned above. Despite the increasing user's awareness in respect to risks of his/her online behavior and, consequently, the inherent security threats, the MMOG player usually has a negligent perception about security. For him/her, it is just an online game, where players play anonymously for fun. The usual understanding is that what happens inside the game world does not have consequences in real life. But, many industry developers are aware that this naive judgment

by many players does not help that much the game business, in particular when the player credentials are stolen away, trust is also thrown away. Thus, our intent was first to study the relationships between security, privacy and trust within a general security framework, before proceeding to a trust modeling solution for MMOGs.

Individual-based trust model framework. We believe that this individual trust model within MMOGs is less prone to defamation and cheating than current reputation systems. Within a MMOG, trust builds on the interactions between avatars (i.e., their behaviors), and thus modeling trust describes perceptual values or factors from the player point of view, that is, trust leans a lot on psychology and sociology-related principles and concepts (e.g., competence, beliefs, risk, importance, utility, etc.). Regardless of whether trust is different from the sum of its parts or not, its parts help our understanding of the more subtle and complex aspects of composing, capturing, and using trust in a computational setting.

Trust inference. Developing a trust metric as a means of measuring trust in MMOGs is a real challenge. In conjunction with the trust model designed for VW/MMOGs, such a metric represents the grand contribution of this doctoral work. Such trust metric takes advantage of subjective logic due to [Jøs13].

In our way to achieve a trust model for VW/MMOGs, we used a WoW (World of Warcraft) dataset taken from Academia Sinica in Taiwan [LCCL11] in the beginning of our research work. Soon after we realized that this dataset was of limited relevance to trust, as data only provided location and rank-related input over a given period of time. Due to limitations in accessing to game state and events in WoW, we started using OpenSimulator [Lop07], an open-source multi-user virtual environment (MUVE). OpenSimulator incorporates a MySQL database module to store relevant data about avatars and their interaction experiences with others (e.g., trading, socializing, chatting, and so forth).

1.5 Contributions

The main contributions of this thesis research work are the following:

- C1** - The major contribution comes from the deployment of a trust model into VW/MMOGs. This trust model works at the top layer of the trust hierarchical architecture structured into three layers: infrastructure, services, and community. As noted above, our trust model lends itself to social trust, also called community trust, in particular for immersive worlds where avatars impersonating users or players interact with one another via sight, hearing, chat, messaging, and so forth. Therefore, our trust model applies to what is going on inside the virtual world, not outside it. That is, our trust model is not designed towards infrastructure and services issues.
- C2** - The second contribution is more specific, which results from a proposal of a trust

framework for MMOGs based on the individual perception of trust. Essentially, the proposed framework reconciles different trust perspectives from psychology and sociology, because one intends to mimic how humans count on each other. This framework is described in Chapter 4.

- C3** - The third contribution concerns a new trust representation for MMOGs, which builds upon a new methodology for collecting and aggregating data generated by avatar-avatar interactions. This data representation is described in Chapter 5.
- C4** - The fourth contribution stems from the inference operators to compute trust in immersive environments. They rely on the trust representation addressed in Chapter 5. These inference operators are described in Chapter 6, and are useful when the trustee avatar is unknown for trustor avatar.

In short, the contributions have to do with the context (i.e., VW/MMOGs), trust framework, trust representation, and trust operators.

1.6 Publications

The research work that has led to the writing of this thesis has originated the following scientific articles:

- P1** - Cardoso, R. C., Gomes, A. *Security Issues in Massively Multiplayer Online Games*. In M. Cruz-Cunha (Ed.), *Handbook of Research on Serious Games as Educational, Business and Research Tools: Development and Design*, IGI Global, pp. 290-314, February, 2012.
doi:10.4018/978-1-4666-0149-9.ch016

Abstract. Massively Multiplayer Online Games (MMOGs) have been steadily growing in interest over the past decade. Their economic value turns them into one of the main targets of malware and cheating in Internet. This paper presents and discusses security issues in MMOG environments. The study starts with a preliminary characterization of MMOGs, highlighting their main features. Afterwards, the authors present the security approaches that are applicable to MMOGs, exposing the implications of security breaches and the need for better protection mechanisms. Next, the paper presents current safety measures and solutions to tackle specific security issues. Finally, security trends that can be relevant in the future are described.

- P2** - Cardoso, Rui Costa, and Gomes, Abel, and Freire, Mário. *Trust Trends and Developments in Virtual Worlds: A Survey* (to be submitted for publication).

Abstract. Virtual worlds, in particular massively multiplayer online games (MMOGs) and online virtual environments, have not been approached by the existing trust models and frameworks. The paper intends to fill this gap in the computer science and engineering literature. In fact, trust research encompasses contributions orig-

inated in different knowledge fields, other than computer science and engineering, therefrom resulting a plethora of distinct concepts, definitions, models, and frameworks. Therefore, this survey will make usage of these multivariate trust elements in order to describe and compare trust solutions found in the literature, as well to show how they can be embedded in virtual worlds.

- P3 -** Rui Costa Cardoso and Abel Gomes. *Towards a trust framework for multi-user virtual environments*. In Beniamino Murgante, Sanjay Misra, Ana Maria A. C. Rocha, Carmelo Torre, Jorge Gustavo Rocha, Maria Irene Falcão, David Taniar, Bernady O. Apduhan, and Osvaldo Gervasi (Eds.), *Computational Science and Its Applications (ICCSA'2014)*, Lecture Notes in Computer Science, Vol. 8579, pp. 754-768, Springer-Verlag, 2014.

doi:10.1007/978-3-319-09144-0-52

Abstract. Trust conceptualizations in multi-user virtual environments (MUVes) are not covered as a whole by existing trust models and frameworks. Apparently, the representation and modeling of trust in a computational environment is an elusive task, largely because that seems to depend on the context within which entities (e.g., users) interact with each other. Hence, the existence of multiple trust solutions that address domain-specific problems. These solutions are scarce, or even inexistent, in MUVes. In this paper, we thus elaborate on a trust framework for MUVes. For this purpose, we carry out a study in order to identify and characterize the MUVE specific features or data sources, as well as to assess how extant trust models (say, TNA-SL, Regret, EigenTrust, Stereotrust and TACS) satisfy MUVes requirements. As a result, we get a valuable insight on how to build up a trust framework for immersive environments.

- P4 -** R. C. Cardoso, A. Gomes, and M. Freire, *A User Trust System for Online Games – Part I: An Activity Theory Approach for Trust Representation*, IEEE Transactions on Computational Intelligence and AI in Games, 2016 (published online first on July 19, 2016).

doi:10.1109/TCIAIG.2016.2592965

Abstract. In virtual worlds (including computer games), users develop trust relationships from their in-world interactions with others. However, these trust relationships end up not being represented in the data structures (or databases) of such virtual worlds, though they sometimes appear associated to reputation and recommendation systems. In addition, as far as we know, the user is not provided with a personal trust tool to sustain his/her decision making while he/she interacts with other users in the virtual or game world. In order to come up with a computational formal representation of these personal trust relationships, we need to succeed in converting in-world interactions into reliable sources of trust-related data. In this paper, we develop the required formalisms to gather and represent in-world interactions—which are based on the activity theory—, as well as a method to convert in-world interactions into trust networks. In the

companion paper, we use these trust networks to produce a computational trust decision based on subjective logic. This solution aims at supporting in-world user (or avatar) decisions about others in the game world.

- P5** - R. C. Cardoso, A. Gomes, and M. Freire, *A User Trust System for Online Games – Part II: A Subjective Logic Approach for Trust Inference*, IEEE Transactions on Computational Intelligence and AI in Games, 2016 (published online first on July 19, 2016).

doi:10.1109/TCIAIG.2016.2593000

Abstract. Representing, manipulating, and inferring trust from the user point of view certainly is a grand challenge in virtual worlds, including online games. When someone meets an unknown individual, the question is “Can I trust him/her or not?”. This requires the user to have access to a representation of trust about others, as well as a set of operators to undertake inference about the trustability of other users/players. In this paper, we employ a trust representation generated from in-world data in order to feed individual trust decisions. To achieve that purpose, we assume that such a representation of trust already exists; in fact, it was proposed in another paper of ours. Thus, the focus here is on the trust mechanisms required to infer trustability of other users/players. More specifically, we use an individual trust representation deployed as a trust network as base to the inference mechanism that employs two subjective logic operators (consensus and discount) to automatically derive trust decisions. The proposed trust inference system has been validated through OpenSimulator scenarios, which has led to a 5% increase on trustability of avatars in relation to the reference scenario (without trust).

1.7 Thesis Structure

This thesis is organized into seven chapters. The fourth to sixth chapters constitute the core of the thesis because they detail the trust model here proposed. More specifically, this thesis is organized as follows:

Chapter 1 This is the present chapter, in which we introduce the thesis statement, research objectives, research contributions, and publications that have resulted from our research work.

Chapter 2 This chapter addresses the security issues in immersive virtual environments, including MMOGs. We identify and evaluate different types of problems: the safety of property and intangible goods purchased by users, privacy, anonymity, identity theft. Interestingly, we noted that most players are not aware of the implications of lack of effective security solutions. Indeed, this chapter proposes a new approach on how to address MMOG security through an information security analysis, as well as presented a comparison with previous approaches. In true, we

end up proposing a security framework for MMOGs as a contribution for further research on security in MMOGs. This chapter corresponds to publication P1 listed in Section 1.6.

Chapter 3 This chapter reviews several trust models, mainly those designed for multi-agent systems (MAS) and networks. Our study was limited to trust models deployed in known benchmarking testbeds. The idea was to evaluate how such trust models can be reformulated in order to satisfy requirements of VW/MMOGs. This is particularly relevant because this chapter represents the first literature review focused on trust in virtual worlds. This chapter corresponds to publication P2 listed in Section 1.6.

Chapter 4 This chapter elaborates on a trust framework suitable for VW/MMOGs. Trust concepts in VW/MMOGs or MUVES have not been addressed in the past from an integrated perspective. In this chapter we present an introductory view on existing problems related to trust in VW/MMOGs. A special effort was made in order to identify trust models susceptible to be integrated in a VW/MMOG trust framework. An effort was also made in order to analyze the adaptability of well established solutions or models to this specific scenario. This chapter corresponds to publication P3 listed in Section 1.6.

Chapter 5 This chapter addresses the problem of a trust representation for VW/MMOGs. It is clear that such trust representation requires a methodology for collecting and aggregating data generated by avatar-avatar interactions, i.e., the in-world data generated by avatar-avatar interactions have to be worked out and transformed into a trust representation. This was achieved by a formalization of trust as a usable concept for VW/MMOGs, which is sustained on the activity theory. Let us mention that this chapter corresponds to publication P4 listed in Section 1.6.

Chapter 6 This chapter addresses the problem of trust computing, i.e., trust operators. These operators act on the trust representation described in the previous chapter, in order to allow a trustor come up with trust result about a given unknown trustee in an automated manner. These operators combine BFS/DFS graph searching and subjective logic operators to compute the trust value to be ascribed by trustor to trustee. This chapter corresponds to publication P5 listed in Section 1.6.

Chapter 7 This chapter presents the main conclusions of the research work underlying this thesis, as well as puts forward with some open issues and directions for future work.

As a concluding remark, let us mention that this thesis fits in the scope of trust computing, making a bridge between computational intelligence and virtual worlds (and digital games).

Chapter 2

Security Issues

Massively Multiplayer Online Games (MMOGs) have been steadily growing in interest over the past decade. Their economic value turns them into one of the main targets of malware and cheating in Internet. This chapter presents and discusses security issues in MMOG environments. The study starts with a preliminary characterization of MMOGs, highlighting their main features. Afterwards, the authors present the security approaches that are applicable to MMOGs, exposing the implications of security breaches and the need for better protection mechanisms. Next, the chapter presents current safety measures and solutions to tackle specific security issues. Finally, security trends that can be relevant in the future are described.

2.1 Introduction

The security paradigm that supported game industry for many years was on protecting game software. This was achieved by making difficult the reproduction of copies of game, so trying to protect game development and investment revenues. Later, with the advent of the Internet, new opportunities arose in the game industry [JED⁺03], but this also implied changes in game security. Therefore, while the main security issues of the pre-Internet games were developing copy protection mechanisms, now security is seen in a wider perspective. Currently, online game industry companies obtain most of their profits from pay-to-play solutions, and not from selling games [Yan03]. Basically, MMOGs business model changed with the progressive disappearance of game copies [CHL06], but new problems arose with those pay-to-play solutions [DP08]. In particular, online games and MMOGs put security challenges, namely: security problems related with player authentication, issues related with game availability and resilience, trust and anonymity concerns, means of ensuring security of player and his/her virtual assets, game law enforcing solutions, game client problems [MGM06], and also game development issues like scalability and persistence. In short, MMOGs share the same security risks as those of other online applications, but also present new and interesting challenges as a consequence of the risks mentioned above. Despite user's increased awareness in respect to risks of his/her online behavior and, consequently, the inherent security threats, the MMOG player usually has a negligent perception in terms of security. For him/her, it is just another type of online game, where players play anonymously and therefore don't constitute a real threat to him/her and other users. The understanding is that what happens inside game's virtual environment does not have consequences in real life. It is clear that this is a wrong understanding in terms of game

security and privacy. There are threats that must be considered when developing and managing MMOG [DP08]. But, many industry developers do not follow this perspective. Due to MMOG business model, whose success results from the amount of players that a game attracts and maintains, a MMOG needs to keep players immersed in the game and luring new ones to allow growth on the number of subscriptions and publicity revenues in order to support the cost of having a computer infrastructure to deploying the game. Therefore, game's success is a result of what players feel on the game. If the game is not interesting, it does not have an interesting history, it is not graphically appealing, it has communication lags issues, and there is a sense that the game is unfair and players feel that it is almost impossible to evolve in the game, that there are few players to interacting with, that they are being scammed, and that they likely lose assets in game due to cheating, that the game does not provide a fair dispute resolution to solving game disputes, then players end up leaving the game. Although some of the previous considerations are not directly security-dependent, many others are. Therefore game developers must incorporate a well-defined security policy in their business model. In general terms, the success of a MMOG is a corollary on game trust and reliability by players. In fact, the player's perception about security is not in accordance with the amount of information that he/she shares in a MMOG environment with unknown players [BBC⁺08]. This fact can be used for player profiling and social engineering attacks. Security in MMOGs goes beyond the security problems of current online applications. The lack of security in MMOGs has implications to user in- game and off-the-game activities. There is a need to promote awareness to security issues within player community, and also to lead game industry to develop better and new security procedures. By identifying the current situation within security in MMOGs, this chapter aims to serve as base for further security research in MMOGs.

This chapter is organized as follows. It starts by briefly describing the game security procedures and their evolution toward online games and MMOGs. Then, we present an overview of MMOGs, with a detailed description of their main characteristics, with a focus on security related features. Relevant security threats, incidents and consequences are then presented, investigated, and analyzed. Afterwards, we present an insight of future measures in the design of new MMOGs that may lead to build up more secure games. The chapter ends with the conclusions, where the main contributions of our research are listed.

2.2 Related Work

In online games, in particular in MMOGs, security is mainly approached in taxonomies of cheating techniques. A former tentative approach to classify security requirements in online games was made in [Yan03]. Park proposed taxonomy for online game security, having classified online game attacks in four categories: server, networking, client, and user attacks [PLC08]. In this study, the most relevant security characteristics are avail-

ability, integrity, and confidentiality. Yan and Randell proposed an interesting approach to the evolution of the computer games industry and a detailed analysis on security [YR05]. They argued that cheating is the most relevant security issue in online games, having then proposed a taxonomy that identifies fifteen types of cheating aggregated in two categories, a generic category and an online games-specific category. The generic category includes the following cheating types: cheating by exploiting lack of authentication, cheating by exploiting a bug or design loophole, cheating by compromising game servers, cheating related to internal misuse and cheating by social engineering. In the online games-specific category, we find the following forms of cheating: cheating by exploiting misplaced trust, cheating by collusion, cheating by abusing the game procedure, cheating related to virtual assets, cheating by exploiting machine intelligence, cheating by modifying client infra-structure, timing cheating, cheating by denying service to peer players, cheating by compromising passwords, and cheating by exploiting lack of secrecy. Webb's approach in networked computer games considers cheating at four levels, namely: game, application, protocol, and infrastructure [WS07]. Yee introduced a threats model for massively multiplayer online role-playing games (MMORPGs) that identified five potential threats [YKSC06], namely: illegal access to play the game, gameplay cheating, gameplay disruption, cheat at paying for game play, and steal proprietary parts of the software. Yee also proposed some mitigation solutions for these threats. Bardzell refers to MMOGs as domains for fraud, having then proposed an approach to fraud mapping by identifying vulnerabilities and potential attack vectors, to finally delineate possible countermeasures. Hu and Zambetta enhanced Yan and Randell taxonomy and presented a framework for cheating and mitigation techniques in MMOG [HZ08]. Interestingly, Yong elaborated a survey of security issues in collaborative virtual environments [YMSF08], which can be also applied to games. Barosso et. al. made a detailed analysis on security and privacy in MMOGs and VR [BBC⁺08], having identified relevant security characteristics, and existing risks, as well as a set of recommendations to make MMOGs more secure.

2.3 Massively Multiplayer Online Games

MMOGs are specific games that had their origins in the early Multi-User Dungeon (MUD). They have evolved significantly in the past years, being now a driving force in the online games industry [CHL06]. Features Massively Multiplayer Online Games (MMOGs) can be described by a set of features that are shared by many of current game deployments [APS08]. Depending on its design and development, a MMOG can have different specific characteristics. Let us list a number of relevant features that can be used to identify and describe a MMOG:

- They are played through an Internet connection.
- The interaction is set up between a client and a game server, i.e., the clien-

Enhancing Trustability in MMOGs Environments

t/server model. Although there are other approaches, like P2P, they are residual in comparison with the client/server model.

- The game environment is represented as a 3D immersive virtual environment, which usually represents a world containing cities and huge spaces in between.
- The game is populated with avatars representing human players, items, and Non-Player Characters (NPCs).
- The interface rendering is based on the client.
- There are different types of avatars to choose, each with its range of features, profession, and skills.
- Each player must set the skills for his/her avatar, including those to be developed during the play.
- The players interact in a cooperative and competitive way with others within the game environment in pursuit of their goals. This characteristic helps to create strong social bounds among players in the form of permanent or temporary groupings known as guilds.
- The game is a persistent universe, where the world continues to evolve even when players quit their sessions.
- Player's achievements are kept in a permanent manner.
- The game hasn't specific winning conditions, but the motivation of most players is to achieve a higher rank status in game, as well as to possess the best game items and skills.
- The game has a well-established economy.
- Trading is allowed among users, some-times with real currency.
- Most game players pay an allowance fee monthly to play.
- There are thousands of simultaneous players that interact in real time using their avatars, chat and voice channels.
- Game state changes, as well as interaction data, are processed on server side and usually are kept in a database.
- Game state is kept permanently update providing reliability through data integrity and consistency checking.
- There are several additional communication channels like email and chat.
- The game requires a number of servers with high availability and consistence, but this is only possible with good server scalability.
- Game induces mechanisms to engage players in time-consuming activities. When players dedicate more time to the game, they build a greater sense of community, and an increasing desire to keep playing the game, as their notoriety increases.

This feature is marketed by game industry via the introduction of new contents and features in the game [Rob05].

- MMOGs may induce an addicted behavior in some players [WR05].

2.4 Architecture

Usually, MMOGs follow the client-server architecture, so they have at least the following components:

Game Server: This component can be implemented in different ways, namely: the server runs on a computer farm or cluster, the server is either centralized or distributed, the server is replicated into geographically dispersed servers known as shards. The server is also responsible for dealing with authentication procedures and client validation. It also provides the establishment of a reliable connection with the game virtual environment, as well as with databases that maintain the game state. The game state, transactions and player's data are stored persistently in a reliable way.

Game Client: This component is the interface with which players interact with the game. It is an application that runs in a remote device, i.e., a personal computer, a laptop, a PDA, a console, etc. It establishes a network connection with the game server, so that after being client authentication granted, the player is prompted to playing, unless the client needs to be updated or patched. The client is responsible for displaying the game to players. But, the client has limited access to game data manipulation because game developers consider that there are not reliable validation procedures on the client side to guarantee data security and privacy.

Communications: The game interactions with players involve data communication between clients and servers. The TCP and UDP networking protocols are the most used to exchange data between clients and servers, though there is also some multicast deployment at a lower level to enable the interaction with multiple players. This puts a problem in the data retransmission over active network nodes and local firewalls. There is some research on this subject due to the relevance of the latency problem to MMOGs [CHL06]. Current procedures involve the aggregation of multiple data to be sent over the network, as well as data compression, mainly due to TCP overhead size. In contrast to UDP, TCP has the advantage of data acknowledgment and ordered data packets, but TCP usually is slower than UDP. Note that there are other data communication approaches that pursue the development of new protocols [WCC⁺09].

2.5 Threats and Vulnerabilities

The security is a relevant issue in online applications, in particular in MMOGs. The following characteristics represent vulnerable aspects of the game that are always subject to impending threats:

- Game economy
- Strong social interaction
- Real time interaction
- Poor law regulations
- Game design and development

2.5.1 Game Economy

Reaching the game goals requires time, cooperation, and dedication. The valuable game items are scarce and difficult to obtain. When players progress in the game, their synthetic characters evolve to higher levels of richness and skills. In the game economy, there is the possibility of trade and exchange of valuable items with other players. This means that game goods and assets may acquire value in real life [Rob05]. This represents one of the main reasons why MMOGs are targeted for attacks [MH07].

2.5.2 Strong Social Interaction

MMOGs are immersive and time-consuming games. They promote the socialization and development of trust from previous game interactions and goal-driven actions, because such interactions are similar to interactions that occur in real world scenarios. This knowledge can be used for social engineering and game scams by malicious players. Eventually, this malicious behavior may lead to goods stealing of other players, and even threaten their real life assets, provided that the malicious player is able to induce other players to install malware in their clients or pass their game credentials.

2.5.3 Real Time Interaction

The design and implementation of a MMOG can be a challenging task when the real-time interaction is a requirement. Besides, state and time in games can become a major issue in terms of game security [MH07]. In fact, updating the game state must be done as soon as possible to prevent not only eventual problems related to consistency and reliability of the game data, but also to prevent eventual exploitation by malicious gamers.

2.5.4 Poor Law Enforcement Schemes

The game developers oblige every single player to sign up an end-user license agreement (EULA) and terms of use (TOU) specific to each game, in order to resolve eventual disputes and controversy in the future. Usually, the resolution of disputes follows one of two main approaches. The first is that the player account is simply closed if any issue arises in the game. The second is that game rules are observed and surveyed within game boundaries, so that eventual disputes outside the games rules like the ones due to cheating are dealt by the players themselves [dZ09]. It is clear that these two perspectives do not provide to players an effective and reliable governance, as there are in-game dispute situations that have implications on real life as was seen in China and Korea [Per09]. All this, together with the real living value of economy of the game, makes MMOGs more appealing and prone to fraud and virtual theft [HM07].

2.5.5 Game Design and Development

In respect to game development, security represents an increasing problem mainly due to the outsourcing of developers, who are motivated to finish up the game development quickly, and as cheap as possible. Obviously, this has consequences in game design, and may lead to appearance of flaws and bugs, because third-party developers tend to neglect security issues in early developing stages. This bring to the game industry extra costs and problems. Whether it is from bugs and flaws in game or costs associated with software patches that are supported by the costumer, these problems may be maliciously exploited, and end up leading to other threats. In addition to developers, also game management services and game providers split responsibilities in the life cycle of a given game, and this has consequences to the overall security [DP08].

2.6 Risk Assessment

Here we present relevant risks to core game assets. Game information is data of the game environment. Game developers have to have a good governance policy in managing the game environment, and this means to keep game playability, maintain the game state, and protect the player data. This has risks concerning how to ensure: protection of sensitive game state's data; unauthorized access to data; manipulation of data, and also mitigate intrusions and active attacks (such as denial of service attacks) against game server [CPK08]. Risk assessment measures the probability of an attack to a game server, and its perturbing consequences. A threat represents the source of the risk and can eventually trigger the risk. Additional risks are those that apply to the networks used to exchange data with the game server. In fact, such a data flow over a network may be tapped to sniff or even redirect data to get unauthorized access to client. Consequently, if a security breach occurs, a malicious player may take an

unfair advantage over other users. This likely will degrade game credibility, as well its reputation, and consequently some players stop playing it, so reducing game revenues. Protection against misuse or attacks in MMOGs is therefore a vital objective to establish, maintain and strengthen the trust of players in the game [D'H00]. But, it is important to bear in mind that there are not miraculous security solutions, i.e., without flaws. Security should follow a multi-faceted approach in order to adjust it to specific situations or even specific games. In short, the game security depends on several exogenous and endogenous factors, namely: player, client hardware/software, client application, client networking, networking service provider, game server, gaming governance policies, game databases (game state), game developers, and technicians. In a game, security is the “weakest link” amongst all game components. However, and above all, security threats largely depend on the motivation, capability and persistence of the attacker.

2.7 Security

Security can be perceived as a mean of ensuring protection of information confidentiality and integrity and also its availability [CM02]. There are two well-known standards on security, ISO 27001 standard (previously known as ISO 17799) and NIST 800-30.

Information security expressed in ISO 27001 standard is defined as the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can be also involved (ISO/IEC 17799:2005).

NIST 800-30 provides a foundation for the effective risk management necessary for assessing and mitigating risks identified within information technology (IT) systems to help organizations to better manage IT-related mission risks. The three foundational security goals/properties are integrity, availability, and confidentiality, although other additional attributes such as, for example, authenticity, accountability and non-repudiation may be also considered.

In a MMOG, security can be perceived as the game capability to protect confidentiality and integrity of the game state, providing also a high level of availability, accountability in the data transactions, as well as the assurance that the game will continue to perform its mission and within the initial design goals.

Although the previously referred concepts are helpful to identify and classify well-known security problems, MMOG security has to be guaranteed and addressed in a more eclectic fashion, because it involves other concepts like protection of chat and email within

the game. Trust is another relevant factor in MMOG security.

There are also different types of threats and risks to take into account in MMOGs. Here we understand security risk as the potential to lose one or several of the proprieties previous described. In fact, MMOG security has several security dimensions to be considered. Previous works on this subject addressed particular issues, mainly cheating but not the overall security problem. As a multidimensional problem that crosses several areas, it requires that all issues be addressed together in an understandable and reliable way. Game economy, technological issues, social interactions, trust, dispute resolution and governance, privacy and anonymity, intellectual propriety, and marketing are all security relevant issues in MMOGs. They all need to be considered in an effective and global security framework in MMOGs. Although some relevant works have already addressed several of the previous described issues, there isn't a whole solution for an integrated security framework.

2.8 Security Dimensions

In respect to MMOGs, let us present the following list of problems relevant to security and privacy. Identifying and addressing these problems is done with reference to the game dimensions, namely: game client, game communication channels, game server, game environment, and player.

2.8.1 Game Client

Security of game clients is an important issue in MMOGs. It has implications on the game and also on user privacy. Problems are due to: validation of client application with the game server, data integrity, security and privacy for user/player data as a consequence of the installation of monitoring tools. This is achieved on client side by deploying game entities to ensure integrity of game client [MGM06]. This has implications on software installed on the client side, and on what would happen if it were compromised (e.g., the Warden software monitoring tool used by WoW).

Game application adulteration This occurs when the game client is compromised, giving an edge advantage to the player. The game industry tackles this serious vulnerability using validation mechanisms of the client application, namely: MD5, surveillance/monitoring tool installed in the client, online service (e.g., Steam) to validate and update the game client.

paragraphClient memory and process handling This procedure does not aim at manipulating and altering the game client, but just the client data (e.g., making is avatar invisible, altering data sent in game state updates). This procedure was solved in some

Enhancing Trustability in MMOGs Environments

MMOGs implementations with the use of client side monitoring devices like WoW Warden.

Keylogger installation When an ordinary player neglects the security issues in games, he/she can be induced by a malicious player to install a malware device in his/her client (e.g., a player installs a keylogger that pretends to be a client update, losing consequently his/her game credentials).

Augmented reality The player may use this technology to give him/her a better perception of the game environment in comparison to other players. For example, in a battle scenario, if a user has two game accounts, i.e., two players/avatars, and one of them joins to the opponent guild, the user accesses other players' information before time.

2.8.2 Game Communications

In this context we present security issues that may occur in communications, like sniffing and manipulation of game data in transit over the network.

Client network tap and eavesdropping This happens when a player has enough skills to gather transaction packets in the communication of other clients with the server, being then able to identifying data relevant about other players in order to take advantage over his/her opponents. This situation is much more difficult to detect when the tap is outside the client network.

Man-in-the-middle This type of attack in client network allows the attacker to manipulate and change information, producing in this way an advantage over others. The procedure can be detected by monitoring ARP tables searching for ARP Poisoning attack evidences. Induction of lag delay: This type of attack introduces an induced lag in game communication as a way of achieving a goal within the game environment more quickly than his/her game opponents. In this manner, a malicious player takes advantage over his/her careless opponents.

Denial of service (DoS) This attack targets not on game servers, but gateways and accessible points. The goal is to disrupt the game service, by flooding service with communication requests, which artificially induce lag in data communications, taking players to quitting their game sessions. This issue could be solved if attacker's IP is correctly identified, discarding then its data packets automatically.

Distributed denial of service (DDoS) The distributed denial of service is similar to DoS attack with the difference that it has multiple and dispersed origins that in simultaneous makes a Denial of Service (DoS) attack to the game service. This type of attack is more difficult to identify due to the massive number of accesses.

Botnet attack In the case of botnet attack, a malicious user gets control of other user computers to perform a DDoS. This constitutes a real threat to game by causing not only a DDoS to the game server, but also damages on users that go far beyond the loss of game credentials.

2.8.3 Game Virtual Environment

In the following we present several types of security issues that originate in game's virtual environment.

Harassment Barosso described this issue as a serious threat to users and resources [BBC⁺08]. Harassment causes emotional distress to users, disrupting or interrupting their game experience. It is clear that this problem also is a real threat for game providers because leads many users to unsubscribe the game, reducing this way its revenues and reputation. According to Barosso, there are several harassment types:

- **Avatar grieving** This happens when a player is denied repeatedly access to a game location or resources due to attacker's actions [Adr10].
- **Avatar ganking** This is a kind of situation such that a higher-rank character kills a player repeatedly, making it impossible to player continue with playing [ND05].
- **Avatar kill stealing** A player starts a fight with a NPC and when it is almost done, another player attacks and receives the correspondent gold.
- **Avatar ninja looting** This issue represents an act of a player during which he/she obtains something that he/she is not entitled.
- **Channel harassment** In this case, the attacker uses inappropriate language to harass other players through communication channels associated to the game like chat and VoIP (Voice over IP).
- **Reputation harassment** The goal is to deliberately damage user reputation within and out of the game.
- **Reputation damage through identity theft** This issue represents a situation where a malicious player is granted access illicitly to another player's account, and poses himself/herself as the legitimate player, passing to have a scamming and cheating behavior that degrades the reputation of the legitimate player.

Enhancing Trustability in MMOGs Environments

- Reputation damage by offensive posting This issue represents an attack to a player's reputation by offensive posts and false information about him/her within game forums or even in the game itself, causing rejection of the player by guilds or even disruption of trade (i.e., exchange of assets) due to his/her deteriorated reputation.
- Reputation damage by abuse of online dispute resolution The fraudulent procedure of a player in reporting false harassment complaints to online dispute resolution systems, in an attempt to revoke a player account or degrade his/her reputation, represents a serious threat to ordinary players, as well as a waste on game resources.
- Eavesdropping This issue represents a way to obtain advantages against a player by sneakily listening his/her private conversations and actions within the game environment.
- Social engineering This issue uses a deception-oriented approach that is used by malicious players to deliberately deceiving and luring other players in a way to give to those malicious players insightful information about the others. For example, luring players to login in a server in order to get and download a special item, and in this way lure them to a rogue server to get their game credentials.
- Avatar Escaping This issue represents an exploit of game design once that the player quits the game when near of being killed, and before the game state be updated. The security procedure to be followed in this case involves a better management of time and state of the game with the objective of ensuring atomic transactions for game data, in a way similar to atomic transactions found in database management systems.
- Gold farming This is that sort of situation in which a player/avatar only plays for profits. His/her actions almost reduce down to collecting items and gold to achieve the objective of enhancing and increasing his/her character level. Afterwards, the player exchanges his/her virtual assets for real currency. Gold farmers can be considered a threat to game playability.
- Content rating system Pan European Game Information (PEGI) is a European video game content rating system. The system is based on a set of rules followed by publishers. PEGI self-regulation is composed by five age categories and eight content descriptors that advise the suitability and content of a game for a certain age range based on the games content. In respect to MMOGs, rating systems like the PEGI one try to classify MMOGs with reference to the available contents. Because MMOG players generate more contents than the content available by the game provider, we end up having a problem. It is true that game providers can determine which player's content that is acceptable within the game, by enforcing the use of guild norms, chat filters, TOS, and prescribed chats to minors. Besides, the content rating system is important, but not all MMOGs use it. On the other hand,

the game industry effort in imposing better control on player game content is in fact insufficient to control the available content found inappropriate to specific age groups.

- **Age verification** The means used by MMOGs to access and check player age usually reduce to a simple agreement that states that the player is eighteen. It doesn't constitute an enough deterrence system and hasn't efficacy enough to succeed.
- **Collusion** Represents a way of cheating that is difficult to detect and mitigate because players cooperate to gain unfair advantages over their opponents. One common way of collusion is to exchange information between avatars that in another way a single avatar hardly could find directly. As noted by Hu [HZ08], in a typical 'win-trading' collusion in the StarCraft game, a player loses once every two times for his/her opponent in a ladder competition. The loss of one point by a player results in a gain of one point by another player, raising his/her ladder rank, and vice versa. Thus, both players could climb to top position in the ladder without playing a legitimate game.
- **Bots** Playing MMOG requires time and dedication because the game puts certain goals that players have to achieve, like obtaining a specific skill or even the characteristics of a game item. These time-consuming activities, together with some repetitive and dull interaction within the game environment, instigate players to use bots to perform those tasks on their behalf. Although most games don't allow it, regular players and gold farmers use bots to perform tasks autonomously as a way to quickly progress within the game. It is difficult to detect and to eradicate; Glider is an example of a bot used in WoW. We may use stored players' data in order to infer and to detect bot activity but it happens that human gold farmers are often mistaken as bots. Other approaches use CAPTCHAS to detect a bot, but its repeated interruptions could be annoying to regular players, because they disrupt game play, and possibly introduce an unfair advantage over regular users.
- **False trade** When players trade and exchange goods with unknown players, eventually with virtual currency, they can be targeted to in-game fraud by paying for an item and not receiving it. This is a consequence of poor reputability-enforcing schemes. **Game culture:** Determines which is the allowed behavior for players and what constitutes a threat to the dominant culture of the game. For example, the game culture determines the cheating limits, i.e., what is tolerated and what is not allowed in respect to cheating.
- **Online Dispute Resolution (ODR)** ODR can be used to effectively resolve game disputes, but it may be also used as a defamation attack against ordinary players.
- **Governance problems due to jurisdiction on dispute resolution** Currently, the key tool for governance of MMOGs is the End User License Agreement (EULA) or Terms of Service (TOS). This mode of governance derives from the fact that online environments are essentially creations of intellectual property and thus, are copy-

righted by the game designers [dZ09]. It also must be considered national law jurisdiction in dispute resolution schemes like in-game guild rules and policies enforced resolution. The lack on accountability and dispute resolution settlement authority could lead to real live threatening situations [Zet05]. In 2005, a Chinese player was killed because of a in-game dispute [Per09].

- **Rogue server / bogus server** It is a fake game server, used by game hackers and malicious players to mimic a real site. The server aims to attract players by leading them to give away their account credentials.
- **Social engineering:** a pishing attack Is initiated within the game using email or chat to lure players to go to a fake location in a rogue server almost identical to the legitimate one and give away their game credentials.
- **Trading** It is a relevant activity in MMOGs that can lead to player's losses. Players interact with virtual world business companies to buy items, virtual currency, tips, tricks, accounts, information guides on to achieve specific goals, and also power leveling players to improve their game rank or achieve a required goal granting access to their accounts. [BBC⁺08]. This uses RMT (real money transactions) outside the game and is based in reputation and feedback scores. Also there is trading among players, although the game explicitly forbids without a reputation system for players they are targeted to fraud.

2.8.4 Game Server

In respect to game server there are several problems and risks.

- **Access point issue** The adoption of a client-server architecture gives more control to game managers but also presents vulnerabilities due to the small number of access points, that facilitate DoS and DDoS attacks.
- **Game Time** Time synchronization among users can present several challenges due to induced latency that could enhance or degrade player performance.
- **Game State** Keeping the game state consistent raises state synchronization issues due to concurrent transactions among players.
- **Game Bugs** Bugs constitute a common problem in software in general, and MMOGs are not an exception. Occurrences of a bug in a MMOG can lead to unexpected behavior of the game, which if exploited could bring disruption to normal running of the game.
- **Inside attack** It represents a problematic situation in which there is a privileged access to game data and game state that can be used for illicit profits in some circumstances such as, for example, colluding between players. This issue can be minimized by adoption of effective security policies within the game.

- **Behavior analysis** Taking into consideration that game entities have a need to develop means of detecting problems in games, they end up gathering and storing a significant amount of data that can have implications on player privacy. This issue is controversial because, according to EULA, the user has not any right or propriety in regarding to game environment. Note that data on each player/avatar provides a way to infer behavior of the player, so that it is possible to develop specific advertising not just for the avatar but also for the player/user in the real world.
- **Game Economy** Game's developers and managers control the game economy. They can manipulate the availability of special and valuable items, the NPCs' powers, and develop quests and goals that have implications on virtual economy values, as well as direct implications on real money transactions (RMT). A company insider in colluding with a player may manipulate this aspect of the game in order to obtain special features in exchange of real money.

2.8.5 Player

Cheating Represents any action of a player to gain an unfair advantage over opponent players. Even following to the game rules, an action can be considered cheating if it represents an advantage that the player is not entitled [YR05].

Exploit An exploit happens when a player uses a bug or game flaw to take advantage for himself/herself in a manner not intended by the game's designers. Exploits have been classified as a form of cheating. However, the precise determination of what is or is not considered an exploit can be controversial. This debate stems from a number of factors, but typically involves the argument that these issues are part of the game and require no changes or external programs to take advantage of them.

Social Engineering A definition of social engineering in MMOGs can be referred as a way of clever manipulation of the natural human tendency for trusting. Social engineering has to do with targeting players to obtaining personal information that allows a malicious player to gain unauthorized access to valuable assets (game credentials, game items or even assets from player real life). A malicious player interacts with other players to gather knowledge about such players and to gain their trust. The goal of social engineering is the same as hacking in general: to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network [Adr].

Revoke Payments This problem appears in online payments. For example, a player buys a special skill at a trade company in order to allow him/her to achieve a higher rank. After using the skill, and selling it to another player for gaining virtual money,

the malicious player revokes the initial transaction at the payment system of the trade company.

2.9 Security Evaluation

In our security evaluation approach that follows, previous MMOGs security issues are grouped in accordance with their information security procedures. We follow ISO27001 and NIST 800-30 guidelines, and we adopt implementations from Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE).

The OCTAVE methodology was developed in CMU (Carnegie Mellon University) in an effort to make information-protection decisions of assets. It identifies risks to the confidentiality, integrity, and availability of critical information assets [AD01]. Here we try to use this methodology to address security in MMOGs by identifying and analyzing possible threats to game assets. Furthermore, we used the detailed taxonomy for common language for computer security incidents [HL98], and adapted it relevant features in conjunction with OCTAVE to provide a specific security classification schema for MMOGs.

In this context, we refer to a threat as an indication of a potentially undesirable problem to the game, e.g. a DoS attack. Threats can therefore be recognized by the following characteristics:

- **Attacker:** An attacker is who deliberately breaks the security requirements (confidentiality, integrity, availability) of an asset. He/she attempts one or more attacks in order to achieve a goal through a variety of methods. Here we classify attackers in function of what they intend to accomplish:
 1. **Hackers** attack games for challenge, status or the thrill of obtaining access.
 2. **Gold farmers** attack games for personal financial gain.
 3. **Malicious players** attack games usually by cheating to enhance their game performance but also to harass others and use fraud to deceive players.
 4. **Insiders** are employers that manipulate game data for getting profits by selling such data to players.
- **Vulnerability:** In order to reach the desired result, an attacker takes advantage of a game vulnerability. Vulnerability represents a game weakness that allows for an unauthorized action. Vulnerabilities can arise in different stages of development or use of the game. They can be:
 1. **Design vulnerability** is inherent to the design or specification of the game.
 2. **Implementation vulnerability** that occur from errors made in the software or hardware implementation.

3. **Configuration vulnerability** results from an error in the configuration like not restricting the number of failed tentative accesses to the game server allowed to users [HL98].
- **Asset:** something of value to the game (e.g., player credentials, player privacy, game reputation, game state, game server access point, stored data).
- **Implications:** consequences to game assets relate to availability, integrity and authenticity.
 1. **Availability** as the game readiness for correspond to player requests in a correct form and within the error tolerance boundary.
 2. **Integrity** represents the absence of improper game alterations.
 3. **Confidentiality** is a property of the game that ensures that data or information is not made available to unauthorized players employees or processes [HZ08].
- **Goals:** represent the purpose of the attack and are the following:
 1. **Challenge**
 2. **Financial gain**
 3. **Harassment**
 4. **Damage**
 5. **Quicker progress**
- **Outcome:** is the result of a successful attack and will result in:
 1. **Disclosure of information** to anyone not authorized to access it.
 2. **Modification** made by unauthorized alteration of game data.
 3. **Destruction or loss** of game information.
 4. **Interruption** of access represents an intentional degradation by blocking game resources (i.e. denial of service).

In this context we didn't consider relevant optional OCTAVE characteristics like motive and access. The security evaluation process involves three steps. First, we have to identify the assets that are relevant in MMOGs. Then, we delineate a threat profile for each asset. Finally, and once the first two steps are finished, we end up a more clear idea about the risk profile.

2.9.1 Asset identification

Considering the previously listed security dimensions in MMOGs, let us now identify those assets that require security procedures in game play. Following our approach, we have identified two categories of assets, player assets and game assets, which show

Enhancing Trustability in MMOGs Environments

different perspectives on what is relevant to protect in a MMOG.

Player assets Taking into account the previously enunciated security problems, we have identified the following player assets:

- User extra game issues like its privacy and client device protection.
- User reputation outside of the game environment.
- User game account credentials protection.
- User payment data stored by the game.
- Player stored information about his/her communications, avatar movements, actions, and transactions.
- Player avatar identity in the game environment.
- Player avatar reputability among its peers.
- Player avatar assets like skills, powers items, and currency.

Interestingly, this identification of player assets, which is based on our analysis of security dimensions, does not match fully those of Barosso's [BBC⁺08]. As shown in figure 2.1, Barosso conducted a questionnaire-based survey to identify those most valued assets by players, i.e., those that most cherish and require protection.

From Barosso's survey, it results that players value the assets that they do not possess due to EULA. These results also corroborate the game's negligent perception that players have about security.

In respect to the assets we have identified above, we elaborated a relational map to show interconnections and relations among assets from the player's point of view, where each terminal node represents an asset that may be prone to threats. This hierarchical map indicates that if a threat exists for a specific asset node, then all the dependent asset nodes may be also compromised and, consequently, attacked. Thus, in our opinion, the map depicted in figure 2.2 shows the MMOG assets that are relevant to players more clearly than Barosso's survey, because it exhibits the dependencies between player assets.

Game assets Taking into consideration the raised problems in the dimension-based approach above, the relevant game assets are the following:

- Governance and related End User License Agreement (EULA) issues.
- Networking and DoS situations, security of communication channels.
- Extra game issues related with legal jurisdiction, problems with intellectual propriety and financial issues.

Enhancing Trustability in MMOGs Environments

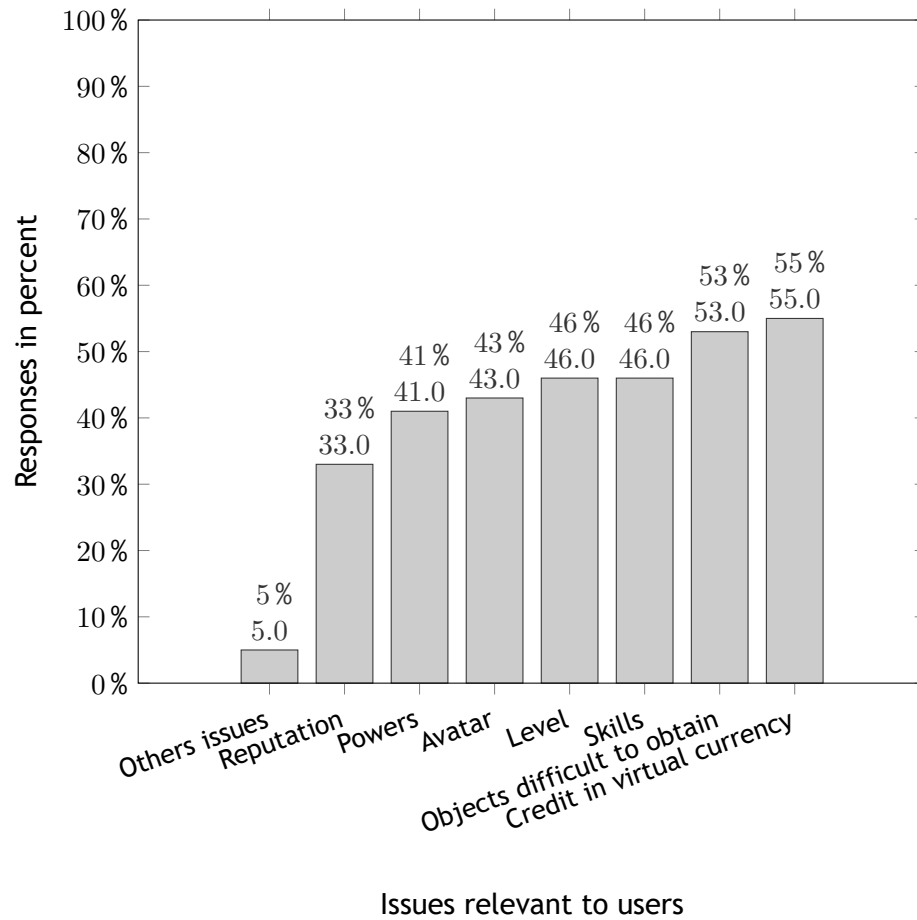


Figure 2.1: MMOGs users perception on value of assets (adapted from [BBC⁺08])

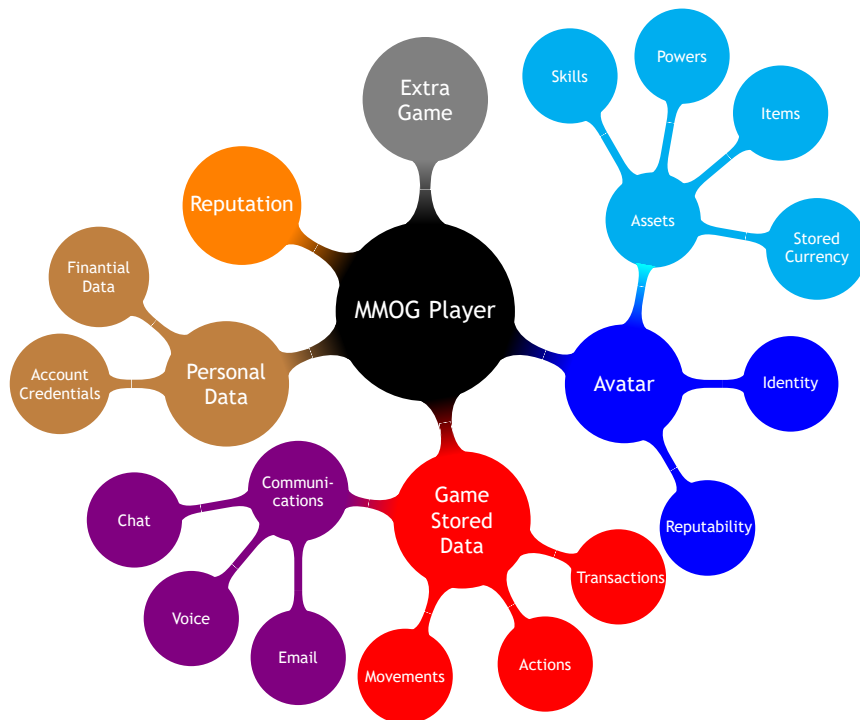


Figure 2.2: MMOGs player assets

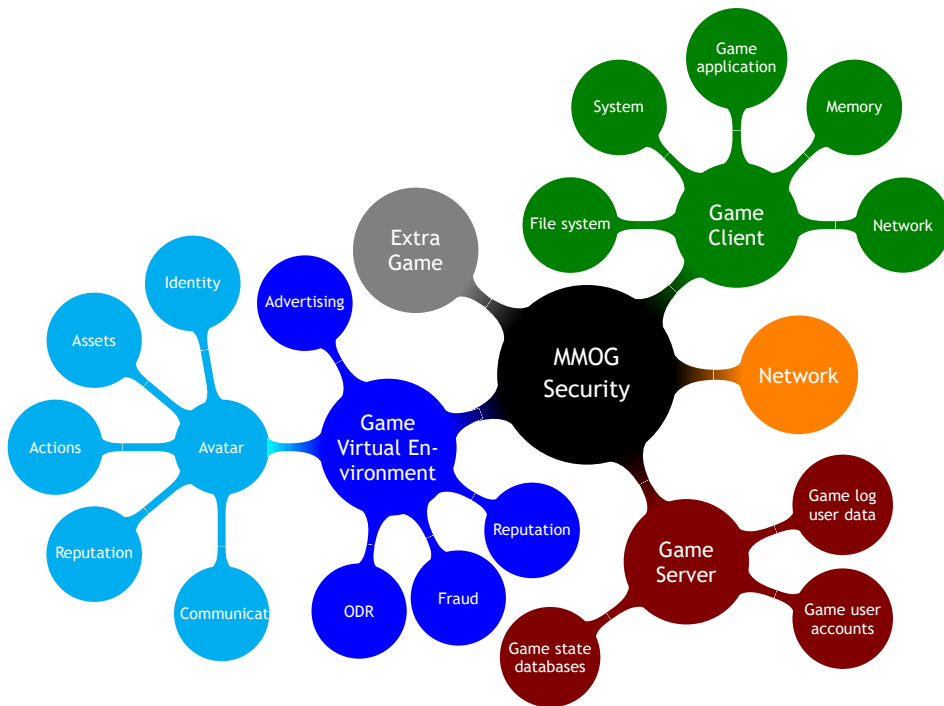


Figure 2.3: MMOGs game overall assets

- For game managers, game clients are perceived as untrusted partners who require special attention and monitoring for ensuring fairness.
- Game availability, integrity, and confidentiality.
- Game data, including player data, user personal details, and financial data.
- Game reputation.
- Game environment is a key game asset that is targeted by different means: bots, gold farmers, frauds, and scams in a similar fashion to real live situations.

The relational diagram between game assets is shown in figure 2.3. The idea here is to put in evidence the relationships among game assets, and consequently to understand how a security issue at one node has implications to the overall security. Note that game assets are hierarchically organized around the central MMOG security node.

2.9.2 Threat classification

We use OCTAVE-based methodology to identify and associate assets to the corresponding threats. Besides, we have tried to make also a comparative analysis with previous classifications, in particular those due to Hu and Zambetta [HZ08], Barosso et al. [BBC⁺08], and Park and Lee [PLC08]. The results are presented in the following tables addressing five levels of threats (dimensions). The first addressing game client threats is shown in Tab. 2.1, the second dimension regarding threats that occur in networks is summarized in Tab. 2.2, from within the game environment we identified the threats listed in

Tab. 2.3, the threats to MMOGs originated in the game server are shown in Tab. 2.4, the last dimension that address threats from players is represented in Tab. 2.5.

Table 2.1: MMOG's game client threat-asset association and comparison

Atk	Threat Name	Asset	Goal	Other classifications		
				Hu and Zambetta [HZ08]	Barosso et al.[BBC ⁺ 08]	Park and Lee [PLC08]
MP	Game application adulteration	Client application	Game advantage	F Cheating by modifying client infrastructure	Game client features	Client attack
MP	Client memory and process manipulation	Client application	Game advantage	F Cheating by modifying client infrastructure		Memory hack
MP HK	Client Malware installation Key logger	Player credentials	Damage, challenge	I Cheating by compromising passwords	Access and authorization	
MP	Augmented Reality	Game fairness	Game advantage			

Legend: Atk attacker type, MP malicious player, HK hacker, GF gold-farmer, IN insider

Table 2.2: MMOG's network threat-asset association and comparison

Atk	Threat Name	Asset	Goal	Other classifications		
				Hu and Zambetta [HZ08]	Barosso et al.[BBC ⁺ 08]	Park and Lee [PLC08]
MP HK	Client network tap and eavesdropping	Game communications	Game advantage	J Cheating by exploiting lack of secrecy		
HK	Man-in-the-middle	Game data	Damage, challenge	J Cheating by exploiting lack of secrecy		
MP	Lag delay to induce advantages	Game server	Game advantage	G Cheating by denying service to peer players		
HK	Denial of service	Game server	Damage, challenge	G Cheating by denying service to peer players		
HK	Distributed Denial of service	Game server	Damage, challenge	G Cheating by denying service to peer players		DDoS
HK	Botnet attack	Game Server	Harassment	G Cheating by denying service to peer players		

Legend: Atk attacker type, MP malicious player, HK hacker, GF gold-farmer, IN insider

Enhancing Trustability in MMOGs Environments

Table 2.3: MMOG's game environment threat-asset association and comparison

Atk	Threat Name	Asset	Goal	Other classifications		
				Hu and Zam- betta [HZ08]	Barosso et al.[BBC ⁺ 08]	Park and Lee [PLC08]
MP	Harassment	Player privacy	Harassment		Harassment	
MP	Avatar Grief- ing	Avatar	Harassment		Character related ha- rassment	
MP	Avatar Gank- ing	Avatar	Harassment		Character related ha- rassment	
MP	Avatar kill stealing	Avatar	Harassment		Character related ha- rassment	
MP	Avatar ninja looting	Avatar	Harassment			
MP	Channel ha- rassment	Player privacy	Harassment		Verbal harass- ment	
MP	Reputation harassment	Player privacy	Harassment		Reputation related ha- rassment	
MP	Reputation damage through iden- tity theft	Player privacy	Harassment		Avatar iden- tity theft and identity fraud	
MP	Reputation damage by offensive posting	Player privacy	Harassment		Reputation related ha- rassment	
MP	Reputation damage by abuse of ODR	Player privacy	Harassment		Reputation related ha- rassment	
MP	Eavesdropping	Player privacy	Game advan- tage	C Cheating by abusing the game procedure		
MP	Social Engi- neering	Player privacy	Game advan- tage	C Cheating by social engineering		Social engi- neering
MP	Avatar Escap- ing	Game rules	Game advan- tage	D Cheating re- lated to vir- tual assets		
GF	Gold-farming	Game econ- omy	Financial gain	C Cheating by abusing the game procedure		
MP	Content rating system	Game rules	Damage		Content rating systems	
MP	Age verifica- tion	Game rules	Damage		Age verifica- tion	
MP	Collusion	Game rules	Game advan- tage	B Cheating by collusion	Access and authorization problems, blocking	Collusion
MP	Bot	Game rules	Game advan- tage		Automation possibilities	Gamebot

Legend: Atk attacker type, MP malicious player, HK hacker, GF gold-farmer, IN insider

Table 2.4: MMOG's game server threat-asset association and comparison

Atk	Threat Name	Asset	Goal	Other classifications		
				Hu and Zam- betta [HZ08]	Barosso et al.[BBC ⁺ 08]	Park and Lee [PLC08]
MP	False trade	Game transac- tions	Financial gain			Fraud
MP	Game culture	Game rules	Game advan- tage		Game culture	
MP	ODR	Game rules	Game advan- tage			
MP	Governance	Game rules	Game advan- tage		Governance	
MP	Jurisdiction on dispute resolution	Game rules	Game advan- tage		Dispute reso- lution	
MP	Rogue Server/ bogus server	Player creden- tials	Damage	K Cheating by exploiting lack of au- thentication		
MP	Social en- gineering phishing at- tack	Player privacy	Game advan- tage	0 Cheating by social engineering		
MP	Trading	Game econ- omy	Game advan- tage	D Cheating re- lated to vir- tual assets	Trading possi- bilities	
MP	Access point issue	Game server	Damage		Game server features	Server Attacks
MP	Game Time	Game design	Game advan- tage			Speedhack
MP	Game Sate	Game design	Game advan- tage			Game data at- tack
HK	Game Bugs	Game design	Damage, chal- lenge	L Cheating by exploiting a bug or design loophole		Game bug at- tack
IN	Inside attack	Game data	Damage, Financial gain	N Cheating re- lated to inter- nal misuse		
MP	Behavior anal- ysis	Game data	Game advan- tage		Player track- ing and behav- ior analysis	
IN	Game Econ- omy	Game rules	Damage		Financial sys- tem	

Legend: Atk attacker type, MP malicious player, HK hacker, GF gold-farmer, IN insider

Enhancing Trustability in MMOGs Environments

Table 2.5: MMOG’s player threat-asset association and comparison

Atk	Threat Name	Asset	Goal	Other classifications		
				Hu and Zam- betta [HZ08]	Barosso et al.[BBC ⁺ 08]	Park and Lee [PLC08]
MP	Cheating	Fairness	Game advan- tage		Cheating	User attack
HK	Exploit	Game design	Damage	Exploiting a bug or design loophole		
MP	Social Engi- neering	Player privacy	Game advan- tage	Cheating by social engi- neering		Social engi- neering
MP	Revoke ments	Pay- Game transac- tions	Financial gain		Financial sys- tem	

Legend: Atk attacker type, MP malicious player, HK hacker, GF gold-farmer, IN insider

From tables Tab. 2.1 – 2.5 we shown that our OCTAVE-based methodology is more complete than the previous ones found in the literature [BBC⁺08, HZ08, PLC08]. With this methodology, we have a better understanding of how all ingredients involved in MMOGs security work together, namely: dimensions, attackers, threat-asset relationships, and attack goals. In this way, we end up presenting a novel approach to MMOGs security that is based on an essentially practical risk assessment with three steps: what asset needs to be secured, what is the underlying threat, and to determine the associated risk [AD01].

2.10 Security Framework

Now we present a possible security framework for identifying security and privacy issues that occur in MMOGs. The framework shows the three steps followed in the security evaluation:

- Assets identification (including vulnerability classification).
- Threats assessment.
- Evaluation of each threat-asset pair in respect to the potential risk to the game.

In the framework shown in the tables Tab. 2.1 to 2.5, for each security dimension, we consider the implications to a given asset if a security breach occurs, as well as the attacker’s characterization, his/her motivations, and which are the results if security were effectively compromised. For example, in respect to the dimension concerning game environment in , a gold farmer explores vulnerabilities of game economy, taking advantage of the methods on how the game economy was designed, implemented, and tuned. A gold farming attack has implications on the game economy because it reduces the availability of items to other players, and therefore raises artificially their value, what consequently affects game economy integrity. It is clear that confidentiality in

game economy is also affected due to difficulty in identifying the attacker. Thus, this kind of attack aims to obtain revenues and also block game resources to others.

As argued before, we have adopted existent security assessment solutions, and then applied them to MMOGs. In this manner, we end up having a framework that encompasses several lines of security analysis. Therefore, this framework reconciles diverse points of view, namely: business model, game implementation models, legal issues, socialization and privacy, and financial issues. By combining different points of view on MMOGs security, our framework allows for a more systematic approach to game's security threats by means of the identification of vulnerabilities and corresponding consequences of their exploitation. In short, we have tried to bring a different perspective to privacy and security in MMOGs using well-established practical procedures related with information security. For that purpose, we have made some adaptations to the OCTAVE methodology to satisfy the requirements imposed by MMOGs.

As shown in this chapter, MMOGs have several security open issues. Let us then quote some of the corresponding challenges in the future development of MMOGs:

- Develop new algorithms for better end-to-end security.
- Develop new mechanisms for a stronger authentication, one time password, or using other channels of authentication validation.
- Develop new solutions to ensure atomic transactions in multiple databases.
- Provide new approaches to client security.
- Develop new mechanisms for improving resilience of game servers to DDoS attacks.
- Develop new server certification solutions to improve player trust in game.
- Develop new solutions to user's privacy and anonymity and, simultaneously, provide a way of unequivocally identifying avatar with the corresponding user.
- Develop better bot and gold-farmer detection procedures.
- Develop solutions to minimize cheating.

Nevertheless, additional security problems could appear due to signs of migration of MMOGs to other devices like game consoles, pda's, tablets, netbooks, and smartphones [Koi07]. The fact, that the availability is increasing, will probably motivate an increasingly time dedicated to gaming. This situation presents a new paradigm where "players can play a MMOG everywhere at anytime". As Shirmohammadi noted, MMOGs present the potential to be the cornerstone of any eSociety platform in the near future, because they bring the massiveness, awareness, and inter-personal interaction of the real society into the digital realm [SC09]. This dissemination of MMOGs across new platforms allows players to play in the same worlds with different types of clients, software, and rendering capabilities. This could bring new and interesting security problems, not only due to different sorts of client's applications but also to their support systems security. There are developments of targeted publicity aimed to players that use avail-

able player game data as a way of adding more revenues to those that result monthly fees. This underlying player profiling can be considered as an abuse of player privacy, and presents security issues to be dealt in the future. The development of better time and state control to enforce consistency in game design is also a relevant issue that needs to be tackled [MH07]. Developing trust and reliability mechanisms applicable to MMOG is a requirement to ensure data security and player privacy [Noo10]. Also, improving security of clients through client validation approaches can lead to enforce fairness in gameplay. Yet another trend is related to ensure reliability and protection of game communication channels. Schluessler's work on preventing cheating via hardware represents another approach that could bring interesting results in the future [SGJ07].

2.11 Summary

In this chapter, we have discussed and presented most current security issues in MMOGs, having also shown insights on current problems and addressed possible solutions. In contrast, we noted that most players are not aware of the implications of lack of effective security solutions. We have also proposed a new approach on how to address MMOG security based on an information security analysis, as well as presented a comparison with previous approaches. Looking at the current trends in the development of MMOGs and security systems, we end up proposing a security framework for MMOGs as a contribution for further research on security development and implementation in forthcoming MMOGs.

Chapter 3

Trust in Virtual Worlds

Virtual worlds, in particular massively multiplayer online games (MMOGs) and online virtual environments, have not been approached by the existing trust models and frameworks. The chapter intends to fill this gap in the computer science and engineering literature. In fact, trust research encompasses contributions originated in different knowledge fields, other than computer science and engineering, therefrom resulting a plethora of distinct concepts, definitions, models, and frameworks. Therefore, this chapter will make usage of these multivariate trust elements in order to describe and compare trust solutions found in the literature, as well to show how they can be embedded in virtual worlds.

3.1 Introduction

Trust is recognized as a fundamental feature of interactions [Luh79]. Interactions between multiple and different types of entities (people, computers programs, services, organizations, games, biological beings, virtual entities, countries) result in trust relationships. Trust works as a driving factor for facilitating, inducing and strengthening relations between entities [Deu58]. Therefore, efforts to clarify and model the concept of trust are being developed in different research fields like philosophy [Bai02] and computer science [Mar94], because there is a multitude of different and sometimes divergent and contrasting views on the topic [LM54, Fuk95, RCS⁺10]. Although there is a persistent lack on unanimity, all those views contribute to enrich knowledge on trust.

In computing, trust is seen as context-dependent, as computing technologies evolve and became more ubiquitous over time, so that new ways of interaction end up to show up, eventually requiring new approaches to trust abstractions. For example, VW/MMOGs constitute a more immersive and persistent medium than other computing systems over a network; as a consequence, trust in VW/MMOGs has to be approached in context somehow. In fact, by definition, a virtual world is a 3D immersive and persistent environment where multiple remote users interact in real-time through their avatars.

3.1.1 Trust in VW/MMOGs

Traditionally, (un)trust relationships between humans result from their face-to-face interactions. With the advent of the information era, such face-to-face interactions in-

creasingly tend to be replaced by compute mediated devices. Therefore, as human interactions increasingly occur through such devices, new methodologies must be developed to assure trust within these environments. For example, VW/MMOGs are an example of an environment that requires the incorporation of new trust inference mechanisms and solutions to help human users (i.e., avatars and players) in their decisions. It is clear that this demands for a trust model and a set of trust operators somehow. To achieve such a trust model, it is first necessary to realize why and how trust does work as the ground of the human interactions.

3.1.2 Trust Approaches

Trust has been under scrutiny by scholars and researchers since the early half of the previous century [Luh79]. Early research on trust followed two main approaches. The first tried to reach consensus on what is trust, initially from a philosophical and sociological perspective [Luh79] [Deu58], which was later followed by researchers of other scientific areas—in particular, computer science—, in the attempt of reaching some form of trust formalization that could be independent of context-specific circumstances. This approach led to a mathematical formalization of trust, more specifically the seminal work of Marsh [Mar94] (see also [Net06, Kru06, You07, JIB07, CSC11]).

The second approach, seen in recent years, addresses trust in a more practical manner, in the sense that it is focused on context-specific situations, the so-called empirical studies [CKN⁺15, EFK10]. This latter approach benefits from the cumulative knowledge produced within context-specific scenarios, i.e., within the scope of each research area. In general, these more practical trust solutions do not take advantage of cross-domain knowledge about trust. In fact, to the best of our knowledge, trust in cross-domain environments like VM/MMOGs are practically inexistent in trust-related literature. Even so, trust in MMOGs was firstly approached by [RCS⁺10], and [AP11] carried out a study on trust among avatars in virtual worlds (VW), yet that without a trust computational implementation. Interestingly, [Gol05] studied trust in social networks, which can be also considered as cross-domain environments.

3.1.3 Other Surveys

Research in trust is extensive, and consequently the trust-related literature is also extensive. However, it is too compartmentalized, i.e., it does not go further the limits of each research area, constraining in this way its pollination across different disciplines. In computer science, several surveys on trust have been published mainly during the last decade, namely:

- *Internet applications.* [GS00] surveyed trust in internet applications.
- *Online services.* [WE05] wrote a survey on online trust, while Jøsang et al. [JIB07] surveyed trust and reputation systems for online services.

Table 3.1: Surveys on trust models.

Topics/Surveys	Trust Models													
	A&H [ARH00]	Sporas [ZM00]	REGRET [SS01]	BRS [J102]	Y&S [YS03]	EigenTrust [KSGM03]	FIRE [HJS04]	PeerTrust [XL04]	Y&S [YSS04]	AppleSeed [ZL05]	TNA-SL [JHP06]	TRAVOS [TPJL06]	PowerTrust [ZH07]	TACS [GMMPGS09a]
Agents/MAS														
Granatyr et al. [GBL ⁺ 15]	○	○	.	.
Jelenc et al. [JHSMT13]	○	.	.	●	●	●	.	.	●	.	.	●	.	.
Pinyol and Sabater-Mir [PSM13]	●
Lu et al. [LLYY09]	●	.	.
Sabater and Sierra [SS05]	●
Online Services														
Jøsang et al. [JIB07]	○
Artz and Gil [AG07]	○
Trust Modeling														
Chandrasekaran et al. [CE15]	●	.	●	.	●
Pranata et al. [PSA12]	●	○	.	.
Medic [Med12]	●	○	●	●	●	.	●	●	.	.	.	●	.	.
Marmól and Pérez [MP11b]	●	.	●	.	.	.	●	.	●
Noorian and Ulieru [NU10]	.	.	●	●	●	.	●	●	.	.	.	●	.	.
Social Networks														
Sherchan et al. [SNP13]	○	.
Ziegler and Lausen [ZL05]	●
Networks														
Kumar and Dutta [KD16]	○	○	○
Shree and Basha [SB14]	○	.	○	○	.
Marmól and Pérez [MP10]	●	.	●	.	.	.	●	●	.
Marmól and Pérez [MP09]	●	.	●	.	.	.	●	.	●
Other														
Viriyasitavat and Martin [VM12]	●	.

Legend: ● reviewed ○ refereed . not considered

- *Web services.* [AG07] wrote a survey on trust in computer science and semantic web, and more recently [WBOM15] elaborated a survey on trust and reputation models for web services. See also [BRDM11] for a meta-study on consumer trust.
- *Trust management.* [RK05] released a survey on trust management, and more recently [ZDB11] also surveyed trust management on various networks, while [PSA12] developed a more holistic perspective on trust management systems.
- *Social networks.* [Gol05] approached the trust across social networks in her doctoral thesis. [Bhu10] and, more recently, [SNP13] overviewed trust social networks.
- *Wireless sensor networks.* [Mom10] produced a survey on trust models in wireless sensor networks.
- *Digital rights management.* [ZPMY09] elaborated a survey on security and trust in

digital rights management.

- *Mobile and ad-hoc networks.* [CSC11] carried out a survey on trust management for mobile and ad-hoc networks. More recently, [ABC⁺15] surveyed trust-based detection of malicious users in ad-hoc and sensor networks.
- *Heterogeneous networks.* [GH11] wrote a survey on trust analysis for heterogeneous networks.
- *Online auction.* [WHS11] wrote a survey on trust models for online auction.
- *Software development.* Trust play also a significant role in assessment of trustability in software development, as identified by the major industry players via Trustworthy computing Initiative (<https://www.trustedcomputinggroup.org/>) [PMW13] [HR13].
- *Cloud computing.* The impact of the virtualization in cloud computing lead also to trust issues linked with security and reliability of information [FGH11, HHRM12, Pea13, HN13, FSG⁺14].
- *Internet of Things.* In recent years, trust management has been also studied in the context of the Internet of Things [YZV14, CC12].
- *Peer to Peer Networks.* [SB14] carried out an exhaustive survey on trust models in P2P networks.
- *Agents and Multi-agent Systems.* Recently, [PSM13], as well as [GBL⁺15], reviewed trust and reputation models for agent and multi-agent systems.

In short, one can say that trust solutions are mostly context-dependent. Recall that, from a historical point of view, trust in computer science can be traced back to 1979, more specifically to the early works of Nibaldi on trusted computer systems [Nib79] at MITRE (<http://www.mitre.org/>). Nevertheless, quite recently it seems to have a trend to address trust in a more general, cross-domain setting, as observed in the works due to Medic [Med12] and Cho et al. [CCA15].

However, in the present survey, we only consider the surveys listed in Table 3.1 because they are the ones that address trust models already implemented in known testbeds, as necessary for comparison purposes. Such testbeds are listed in Table 3.2, as well as their 17 trust models to be analyzed throughout the chapter. As shown in Table 3.2, the majority of the testbeds considered in the survey was developed in the context of multi-agent systems (MAS), with two exceptions, WSN [GMMPGS09a] and P2P [WAC⁺09].

3.1.4 Outline

This chapter is organized as follows. Section 3.2 addresses trust studies in distinct fields of knowledge. Section 3.3 describes the trust-influencing factors during in-world inter-

Table 3.2: Testbeds and their trust models.

Characteristics/Models	Testbeds									
	ART [FKM ⁺ 05]	Simulator [SVB05]	P2P-Sim [WAC ⁺ 09]	TRMSim-WSN [GMMPGS09a]	Treet [KC10]	Dart [SAW12]	ATB [JHSMT13]	EStarMom [PNJd15]	C&E [CE15]	
Characteristics										
Field	MAS	MAS	P2P	WSN	MAS	MAS	MAS	MAS	MAS	
Language	Java	Java	Java,C	Java	Java	.	Java	Java	Java	.
Source code	•	•	•	•	◦	•	•	•	•	.
Incorporate new models	•	•	•	•	•	•	•	•	•	•
Trust models										
A&H [ARH00]	•	.	.	.
Sporas [ZM00]	.	•
REGRET [SS01]	•
BRS [JI02]	.	•	•	.	.	.
Y&S [YS03]	•	.	•	.	.	.
EigenTrust [KSGM03]	.	•	•	•	.	.	•	.	.	•
FIRE [HJS04]	•
PeerTrust [XL04]	.	.	.	•	•
Y&S&S [YSS04]	.	•	•	.	.	.
AppleSeed [ZL05]	•
TNA-SL [JHP06]	.	.	•
TRAVOS [TPJL06]	.	•	•	.	.	.
PowerTrust [ZH07]	.	.	.	•
TACS [GMMPGS09a]
BTRM-WSN [MP11a]	.	.	.	•
LFTM [MMBP12]	.	.	.	•
TRIP [MP12]	.	.	.	•

Legend: • available/deployed/tested model ◦ only application available

actions. Section 3.4 describes the trust properties inherent to in-world interactions. Section 3.5 details the process of determining trust in the trustor-trustee interactions. Section 3.6 details the most representative trust models in computer science, in the context VW/MMOGs. Section 3.7 discusses trust models and testbeds in a summary manner, and in four areas of application, including VW/MMOGs. Finally, Section 3.7 concludes the chapter, putting forward the main contribution of the survey.

3.2 Trust Studies

Trust as a multidisciplinary area of research has received a lot of attention [Fuk95, BFL96] [Gam88] [ARH00] [GS00] [LT01] [XL04]. However, this is not the case of trust in the context of virtual worlds (including MMOGs) [BGRP01] [Bar03] [PRMSL⁺09] [DL10].

It is clear that this makes the literature review we carry out in this chapter much more challenging. Our approach is mainly focused on computer science literature. Also, we have limited the scope of the approach to the period of 2005-2015, with a few exceptions like [Mar94] or [KSGM03], because of their instrumental role in the field of trust computing. Another limitation in terms of scope was the use of trust to specifically address interactions between humans, although mediated computationally.

3.2.1 Historical Notes

Trust was initially refereed in *The Republic* by Plato [FG00], in which he stated “*We should trust others only if we are confident that they fear detection and punishment sufficiently to dissuade them from harming or stealing from us*”. This quotation shows a fundamental characteristic of trust as a society catalyst used to foment compliance with society rules and in this way promote acceptable society behaviors [McL11]. People are driven by their own interests, which if taken by the letter would collapse the society [McL11]. In society, trust plays a pivotal role, as it provides a vehicle to make our social life simpler and safer, working as the driving force behind the development of cooperation between humans and societies [McL11].

Another way to characterize trust is due to Deutsch [Deu58], who noted that trust leads to a non-rational choice when a person is faced with an uncertain event in which the expected loss is greater than the expected gain [Deu58]. Hosmer [Hos95] argues that if the reverse was true then trust would be just a rational concept. Luhmann [Luh79] and others sociologists follow a different conceptual approach, identifying trust as a fundamental feature in establishing and maintaining relationships between people. These views have led to further trust developments in knowledge fields so diverse as marketing [JB08a, UAL09], social organizations, management [CSC11, CC12], economy and political sciences [KHZF05], and also computer science [Nib79, ARH00, AG07].

Initially, trust in computer science had a flavor of security targeting hardware and software reliability. Nibaldi's work [Nib79] on the specification of a trusted computing base (TCB) at MITRE is seen as a representative of the early stages of trust developments in computer science. These initial incursions in trust were important to endeavor the posterior theoretical foundations due to Marsh [Mar94], which constitute a milestone in trust research in computer science. Nowadays, as seen further ahead, trust computing spans different research areas.

3.2.2 Trust in Social Sciences

Trust was and is fueled by the emergence of information society, which brings together new collaboration and interaction possibilities for humans using computational mediated devices. But, this is not without potential risks like, for example, identity theft [NV12] [BBC⁺08]. To address threats of this sort, new approaches are necessary to

preserve online personal identity, personal data, and privacy. In our view, the ways by which people, services and organizations interact could benefit from the adoption of trust computing, because trust plays an important role in strengthening and developing social relationships [Luh79]. Current issues and trends represent a new perspective on trust usability in social networks [SNP13, Bhu10] and virtual worlds [SLT10, SKK⁺12, CZDB11]. Nevertheless, trust permeates different research fields in social sciences, as illustrated in Fig. 3.1. Let us then briefly address social trust issues in VW/MMOGs.

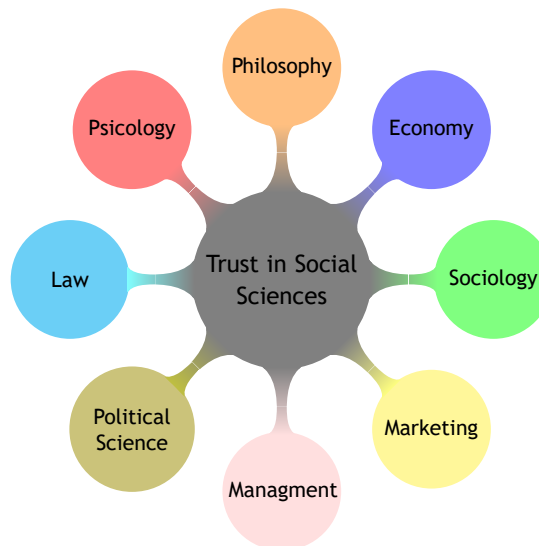


Figure 3.1: Social Sciences areas that employ trust conceptualizations

3.2.2.1 Trust in psychology

In psychology [Joh74], trust is seen as a personal concept [Deu58]. The definition of personal trust has been addressed in psychology [Bul13, Lju08], but not in the context of virtual worlds and MMOGs so far. As detailed throughout this thesis, this concept of personal trust plays a very important role in our trust theory and model as applied to virtual worlds and MMOGs.

3.2.2.2 Trust in management

Efforts have been made to address how trust evolves over time within organizations [Hos95, JB08a]. In this context, trust is understood as vital to enhance management of organizations [CI06], which is realized as varying over time [CI06]. In general, several types of trust have been identified within the context of a given organization, which are hierarchically structured as follows: interpersonal trust, trust in the hierarchy, and trust in the organization. This perspective correlates with the situation of group development in virtual worlds and MMOGs guilds.

3.2.2.3 Trust in marketing

In marketing, trust is seen as a requirement for inducing and developing interactions with costumers [LJL⁺15, HLL10] [UAL09]. In fact, trust plays a fundamental role in the establishment and management of market relationships [MH94, Rai00]. In online trade, trust is even used as a marketing tool [LT01] and a key feature in buyer-seller relations [PMD97, WE05]. In regard to VW/MMOG, the active usage of an avatar can lead to disclosure of information like user behavior, group membership, activities, and in-world locations susceptible of being used in marketing [CYL13]. In a virtual world like SecondLife, where users collaboratively develop and share contents, but also enhance their social skills within multiple types of social activities, we realize that data produced from these activities may be used as trusted resources, from which Linden Labs may develop marketing strategies towards current users and to attract new ones [PRMSL⁺09].

3.2.2.4 Trust in sociology

In sociology, trust is seen as a key facilitator for establishing and developing human relationships and interactions [Luh79, Luh00] [Gol05, PK08]. From a sociological point of view, trust can be seen as an attitude which allows for risk-taking decisions to be made [Luh79, Luh00], which depends on the context and personal experience [DH08]. Interestingly, in neurology, trust is seen as an in-built human feature that triggers specific behaviors based on evidence of an existing relation between the hormone oxytocin and trust. As the hormone promotes “*tribal behavior*”, trust is tied to empathy between in-group members and to suspicion and rejection relative to outsiders [KHZF05]. This fact is a relevant contribution towards existing discussion on how to tune initial trust values in computer science models [JIB07, Per99, OCB12, WHS11]. When interactions between users (or avatars or players) take place, and no initial trust values exist, one can use as default those taken from the biological/hormonal setting as noted above. This also seems to be relevant in virtual worlds as a way of addressing user assessments when no previous knowledge about such a user exists.

3.2.2.5 Trust in law

Trust represents a fundamental link between the legal and technical approaches to digital rights management (DRM) and governance [Hum08, TJG⁺10], as well as in digital rights production [ZPMY09], in which multiple entities are involved: individuals, corporations, enterprises, international entities, and even countries. Taking into consideration that virtual worlds (including MMOGs) mimic real worlds somehow, trust in computational systems also accounts for jurisdiction and legislation issues, as well as governance issues [NSB06]. The concerns towards ownership of virtual assets like virtual items, personal profiles, virtual presence in social networks and other types of online

presence, are becoming nationally relevant [SLPK09], and addressed by supra-national entities like EU [(IN11, BBC⁺08]. The development of a legal framework for trust management and copyright protection would certainly have implications on trustability of the governance of virtual worlds and MMOGs, DRM, virtual object propriety assurance, end-user license agreement (EULA), and in preventing identity theft.

Table 3.3: Comparison on how trust is used in society versus VW/MMOGs.

Areas	Trust perception	VW and MMOGs
Law	Trust in the judicial system. Trust in the policy body.	Platform/Game Governance.
Management	How to strength trust relations within people in organizations.	Trust among avatars/users and guild members.
Marketing	How to induce trust in a product or service.	Behavior tracking.
Economy	Mechanisms of trust in predicting scenarios.	Trustability in platform/game trade engine.
Sociology	Trust as a tool to promote socialization.	Game interaction facilities.
Psychology	Trust as a personal assessment tool.	Players behavior, notoriety and ranking.
Philosophy	Interpersonal trust and the morality of trust relationships.	Avatar behaviors, like grieving, ganking, harassment.
Political Science	Trust in political science is linked to how leaders behavior is perceived.	Notoriety and player rankings are fed by their interactions and achievements.

3.2.2.6 Economy

Trust plays a key role in economic exchanges [WE05], which has much to do with how trust is established between buyers and sellers, and their products in e-commerce [LT01]. In fact, there is evidence that indicates that trust contributes to economic success [WE05]. We believe that trust in economics can be easily transposed to VW/MMOGs to address in-world trade, and in-world economic dynamics (e.g., by determining the level of scarcity of a highly required asset and, in this way, to determine its in-world value).

3.2.2.7 Political science

As known, trust pervades human societies. In regard to politics, trust plays a key role not only in the establishment of political legitimacy [KHZF05, Het98, CL16], but also in the trustworthiness of a country's institutions and their leaders [Kaa99], not to mention how international relations are established [Hof02].

3.2.2.8 Philosophy

As mentioned above, trust was addressed initially by ancient greeks philosophers like Plato [McL11, Bai02]. From a philosophical perspective, we trust to develop relationships with others, including love, advice and help [McL11]. Others see the link between

our willingness to cooperate and trust as a benefit for the society as a whole [WE05], suggesting the existence of an association between trust in society and philosophy [Hos95].

Table 3.3 summarizes and compares different real-world contexts to their counterparts in virtual worlds and MMOGs. In short, we can say that these virtual environments tend to mimic at least some real-world contexts for good and for bad.

3.2.3 Trust in Computer Science

In computer science, the leading idea of trust is to transpose solutions and frameworks used in our daily lives –and already studied in other areas of research– to computer-mediated devices and services. Society as a whole evolves over time, so that interactions via such computer-mediated devices tend to become prevalent, what obviously requires the adoption of new solutions for trust that go beyond the face-to-face relationships established by humans.

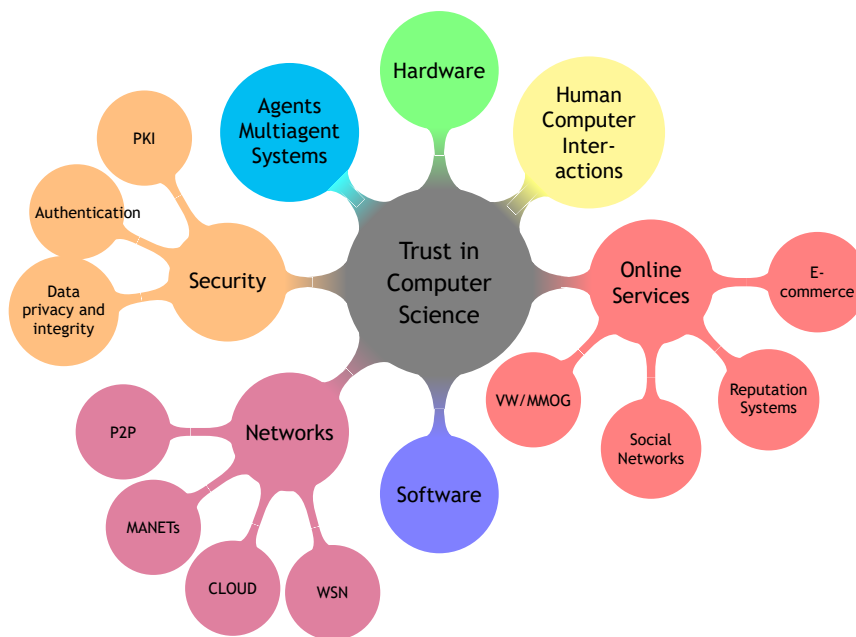


Figure 3.2: Computer science areas that employ trust conceptualizations.

3.2.3.1 Hardware

Trust in hardware is tied to the beginnings of computer systems, and has much to do with integrity, reliability and performance of integrated circuit designs, and hardware in general. In fact, trustworthier hardware plays an pivotal role in security [ZYW⁺15, IL07]. A prevalent issue regarding hardware is the hardware integrity and reliability of compute devices, in particular those disseminated via the Internet-of-Things (IoT). Such hardware integrity and reliability must be primarily assured with the exclusion of adulterated integrated circuits produced in untrusted foundries, because adulterated

Table 3.4: Comparison of trust usability in different computer science areas versus VW/MMOGs.

Areas	Trust usage	VW and MMOGs
Hardware	Embedded chip to secure functionality. Trustworthy computational devices.	Could be used to validate client applications and prevent client side adulteration (e.g., change game rendering and make all walls transparent).
Software	Trust models. Trustworthy computational devices.	Embed trust modeling in platform engine.
Networks	Trust Models. Trusted and reliable nodes.	Analogy between network nodes and in-world avatars.
Online Services	Trust in e-commerce. Social networks.	In-world and engine services relationships.
Security	Embedded chip to secure functionality. Trustworthy computational devices.	Poor governance and regulation can lead to security incidents.
HCI	Trust in the usability of the interface. Develop trust between users and online services.	Trust in the immersive environment from how it is perceived and sense by users.
Agents MAS	Trust Models. Buyer-Seller Markets. Agents Trustability.	Avatars as Agents.

hardware is vulnerable to a wide range of malicious attacks via software. Adulterated chips work as hardware trojans (HTs) and could be exploited as backdoors to disrupt normal operation of compute devices, which may lead to performance changes and service degradation [NCD⁺10].

This has led the industry (within the Trust Computing Group) to develop efforts towards the adoption of the Trusted Platform Module (TPM) hardware chip by the manufacturers. TPM is a dedicated micro-controller designed to secure hardware by integrating cryptographic keys into compute devices (e.g., laptops, tablets, smartphones, IoT devices), with the primary goal to ensure the integrity of a platform and effectively guarantee that hardware operates as supposed to be. This micro-controller is not bounded to a particular operating system, with the further advantage that it potentially benefits encryption-enabled applications like digital rights management (DRM), protection and enforcement of software licenses, and also prevention of cheating in VW/MMOGs [BM07]. The downside of TPM is that it raises privacy concerns in respect to users of compute devices.

3.2.3.2 Software

Trust in software has given rise to several initiatives, namely by the Trust Computing Group (TCG) [PMW13] and their TPM usage software developers, in order to assure a more reliable and trustworthy software, i.e., software with a reduced number of or even without security faults [ARJ09]. Software is also used to assure data integrity and data trustability through digital signatures in [DPJX12]. Others researchers and practitioners address integration of trust in software as a service (SaaS) [DCK16], or trust in open source software [HR13]. Also, in software agents, trust is used [Pat02]

crosswise in e-markets in buyer-seller situations, or in trust modeling [JHSMT13].

3.2.3.3 Networking

Trust is also important in networks and communication protocols, mainly in scenarios in which uncertainty is associated to network nodes. Such uncertainty depends on the node dynamics, i.e., volatility, lack of or incomplete information (on new nodes characteristics), alleged node behavior, and node capacities, as observed in different types of networks, namely: WSN [CC12, MP11a], P2P [SB14], MANETs [GM12] and also identified in IoT [YZV14, Koi11]. Trust is also essential in certification authorities [OCB12, Lev04, LA98], PKI [DPJX12, Per99], as well as other specific protocols developments. Additionally, grid and cloud services and technologies pose interesting trust challenges [HHRM12, HS13].

3.2.3.4 Online services

Trust has been also addressed in online services, being today one of the most important trends in the era of the information society [JIB07, Mas07, YZCZ11], with a particular focus on specific scenarios like e-commerce [BRDM11, ST11, MDH02, MCR12], web services [WBOM15, Gol09, AG07, UAL09, MS04], and supra-national initiatives and research on enabling technologies for security and trustworthiness of network infrastructures and services [IN11], so that trust issues related with privacy and identity in information and communications technology (ICT) are also addressed [VCS07].

3.2.3.5 Security

Security may appear in many flavors. Often it is bound to reliability, availability, but also addresses features like confidentiality of information, data integrity, vulnerabilities and resilience to faults or attacks as stated in a Trustworthy ICT Research EU FP7 technical report [(IN11); see also [MSS14, Kou12, ST11, GMMPGS09a, ZPMY09] for further details. Trust is a key feature to security. In cybersecurity and digital privacy, trust plays a pivotal role [(IN11]. The issue of user privacy and how trust relates to security was developed in [Sei05], but [D'H00] also discusses the issue on how trust influences security. Other works address infrastructure security [CM02], and how security of critical infrastructures depends on trust [CSM⁺11]. But, security is also an issue in hardware, so that trust in the device operational reliability is a factor to take into account [Kou12], in particular in respect to grid computing infra-structures [SHM04]. Sullivan et al. [SCM10] attempted to develop security metrics for trust. In regard to online services, there is also a concern about security issues in trust and reputation systems [ST11]. In games and virtual worlds, important security issues were put forward in [MH07, BBC⁺08] and [BJB⁺07].

3.2.3.6 Human-computer interaction

Human-computer interactions (HCIs) play an important role for users to develop trust on online services (e.g, like an online bank) [Dix09]. Intuitively, we can say that HCI aggregates contributions from multiple fields, from ergonomics and design to human behavior studies and computer science. Therefore how the interface is presented, perceived and used by users can contribute to the establishment of trust relationships between humans and services [Hwa14, LWH13], as well as among humans via compute mediated interactions like those in social networks [SNP13]. Also, in VW/MMOGs, when the human-computer interface is an in-world 3D world that lacks real world features like face-to-face communication, establishing trust across these media is something we need to develop in the near future [DIG13]. In the literature, the focus of research in human computer interaction is on online services/applications interfaces [DHMV14]. This focus is also extensible to immersive environments like VW/MMOGs [Lop07] and augmented reality environments (e.g., placement of virtual objects in real world) [Har14, Ali97], which represent new challenges for trust developments in the HCI field.

3.2.3.7 Agents and multiagent systems

Trust in agents and multi-agent systems (MAS) were addressed by Marsh [Mar94] as proof of concept of the first conceptual approach to trust. Later on, Castelfranchi and Falcone [CF98] established the trust principles of MAS, in order to address agent interactions in a similar way to client-seller market characterizations. Additionally, trust developments in MAS were addressed in [RHJ04], and [Pat02]. Other approaches used reputation models to enhance agent interactions [You07]. Also, it is common to see trust modeling and trust management systems and tools to take advantage of agent-based trust models like REGRET [SS01], TRAVOS [TPJL06], FIRE [DHJS04, HJS04]. Note that agent-based trust models have been extensively overviewed in multiple surveys [GBL⁺15, YSL⁺13, PSM13, LLY09], and also in testbed platforms like Agent Test Bed (ATB) [EHW13] or DART [SAW12].

Summing up, in computer science, trust tends to be used across compute-mediated devices, in a similar way as humans do in their daily live. Table 3.3 illustrates how trust is used in different computer science fields, putting in evidence how it might be used in VW/MMOGs.

3.3 Trust-Influencing Factors

When we use the term “*trust*” in our daily live, the basic concept is recognized but it is meaningless to us without further information, i.e., “*I trust ...*” would only have a meaning if we add something to the term in order to bring significance to the concept.

Table 3.5: Trust related concepts and VW/MMOGs counterpart.

Concept	Description	VW/MMOG
Credulity, Gullibility Confidence	The tendency to believe or to believe too readily and therefore to be easily deceived A feeling of trust towards someone or something. This sometimes is referred as a synonymous of trust.	Greedy, hasty, and/or ignorant users targeted by scams. I have confidence in other guild members.
Distrust	The opposite of trust, i.e., suspicion or with lack of confidence in, doubt on someone's honesty.	The usual trust state when facing unknown avatars.
Entrust	To confer trust upon ("The messenger was entrusted with the general's secret"), implies the delegation of something (i.e., usually a task) from trustor to trustee.	e.g., lending a sword to a friend to enter in a PvP fight.

Different and sometimes overlapping definitions of trust coexist in the literature [MDH02]. As was noted by [Deu58], trust incorporates the reciprocal and bi-directional link between trustor and trustee, which was later, and in another context, also identified by [CI06]. However, in our view, trust is not reciprocal, i.e., trust is a direct relationship between a trustor and a trustee, not the other way round; e.g., "I trust my car to my mechanic, but he does not trust his car to me to fix it".

Trust has been subject to several unsuccessfully attempts to come up to a formal and concise definition. In fact, there is a lack on consensus about what trust is, simply because it is a multi-faceted concept that incorporates cognitive, emotional, and behavioral dimensions, amongst others, with the further difficulty of being used interchangeably with other related concepts [WE05]. As illustrated in Table 3.5, the concepts of credulity, gullibility, confidence, and entrust may be mistaken as trust, but they distinguish from each other in a subtle manner.

3.3.1 Main Trust Factors

Trust is necessary when humans need to make decisions (or choices). For each individual, a trust-based decision is made with reference to a number of factors, here called trust-inflencing factors, or simply trust factors. The main trust factors are the following: *past experience* and *risk*. Also, as illustrated in Table 3.5, these trust-influencing factors are common to real and virtual worlds, including MMOGs; for example, when a player lend an high value object to a guild member he accepts the risk that it could not be returned, but he knows him, he is in is team. Further ahead, we shall see that there are other trust factors that help humans to make decisions.

In social sciences, we find a number of definitions for trust in different contexts. Herein, we are interested in definitions originated in psychology and sociology, because they have to do with the individual and groups of individuals (i.e., communities), respec-

tively, as usual in VW/MMOGs. In psychology, the following definition shows that the question of trusting/untrusting is inherent to personal choices. Moreover, any choice has a consequence or associated *risk*.

Definition 1 *Trust represents the reliance on another's good will, therefore letting others taking care of something the trustor cares about which involves some exercise of discretionary power [Bai86].*

On the other hand, the following definition shows that *past experience* is a factor to take into account in the process of making a decision (i.e., choice) based on trust:

Definition 2 *When we trust other people, we expect that they will fulfill their promises, either because we know that they have usually done so in the past, or because we believe that we shall fare better if we presume that others are trustworthy [Usl02].*

In fact, as argued by [Luh79], from the sociological point of view, trust is a mean for reducing the complexity of living in society. Such complexity stems from the interaction between individuals with different perceptions and goals [Luh79]. This sociological perspective on trust due to [Luh79] shows that trust essentially is an interpersonal concept [Jal06]. Therefore, trust is a way of simplifying the human-human interactions (or trustor-trustee relationships) underlying the living in society. Luhmann's sociological view of trust as a interpersonal concept translates itself into a one-to-one relation in computer science as follows:

Definition 3 *Trust is a relationship established between a trustor and a trustee avatar in which the trustor makes himself vulnerable to the actions of the trustee in the expectation that the trustee will produce a good outcome.*

It is clear that this definition of trust is atomic and does not fully feature the sociological view of trust as argued by Luhmann. To comply with this sociological view of trust, we have to extend the trustor-trustee relationship to all members of a group, community, or society. In computer science, this sociological view can be represented by a graph, where nodes represent individuals and edges represent trust relationships.

Definition 4 *The trust associated to a given agent (or graph node) is a subjective assessment by another agent (or graph node) on the reliability and accuracy of information received from or traversing through that node in a given context [GM12].*

This graph representation of trust relationships constitutes a first step to be able to quantify trust, as required in computer science, though trust supposedly is not quantifiable in social sciences. In fact, the first serious attempt to quantify and formalize trust, as needed to be implemented and thus evaluated on computer, was carried out by Marsh [Mar94], who used a testbed populated by trusting agents to illustrate the usefulness of the trust as a computational concept. In truth, trustor's subjective view on the trustee together with a set of available information sources (e.g., other avatars, guild members, friends, reputation systems, trust networks) can be used to evaluate and assess the trustee in terms of trust. For that purpose, it is crucial to identify and be able to quantify more trust-influencing factors (see Table 3.6).

Table 3.6: Trust influential factors from real world situations.

Real world situations	Hypothesis	Factor
I have trust in my car to drive me to work. I rely on my car brand so I'll buy them my next car. I flight often with my country airline because I trust them.	Previous experience has an impact on trust [CCA15, ABC ⁺ 15, CNP04].	Past Experience (knowledge)
I trust in my mechanic to fix my car. I don't trust my mechanic to babysitter my toddler. I trust him my car again although he crashed one a year ago.	Trustee skills to fulfil the trustor goal [HN13, CCA15, GS00]. Trust is influenced by time [ABC ⁺ 15, AHC13, AG07], since past events relevance to trust decays with time.	Trustee skills Time
I trust in my gardener because my friend suggested. I book a hotel room with high rate of positive comments. I trust my wife despite my friend opinion. I trust that this week I will win the lottery.	Opinions influence trust decisions [DYLL15, CKN ⁺ 15, CSC11]. Subjectivity determines trust decisions as they are based on past individual experience, understanding, and feelings [WBOM15, PSM13, JB08a, WE05]. The way we envision situations has an higher influence on trust than others' opinions.	Others' opinions (reputation) My own opinion (subjectivity)
I lend my special powered sword to friend in a MMOG.	Taking a risk is an essential part of a trusting relationship [BRDM11].	Risk
I trust in my child to mowing, but not to drive my car. I distrust my child to swim without supervision in a pool.	Trust depends on context [GS00, JGK06, SS05].	Context
I made him a personal loan because he is a friend. I trust him because he is from my family. I trust in my supervisor decisions.	Friendship, intimacy and, in general, proximity influences trust perception [AK02, Gul95].	Social proximity

3.3.2 Other Trust Factors

Trust as an abstraction concept can be better understood when we identify and relate it to specific real-world situations (or scenarios) in which trust is addressed from a point of view of human-human interactions. Therefore, the feeling of trust reveals itself in distinct ways when humans interact with other entities of the surrounding world, including other humans. In a way, one can say that there are several context-dependent trust hypotheses, i.e., a number of suppositions put forward on the basis of limited evidence, which work as a starting point for a deeper investigation. In order to clarify how trust works in human-human interactions, it is important to identify the *trust factors* (or trust-influencing factors) from those trust hypotheses, as well as examples of *real-world situations* that make such hypotheses more plausible, yet using the common sense approach.

In Table 3.6, we present illustrative real-world trust situations, for each one of which we put forward a trust hypothesis found in the literature in order to reinforce its evidence, being then possible to derive the corresponding trust factor. In fact, using Table 3.6, we were able to identify the following trust-influencing factors underlying many human-to-human interactions in real-world scenarios:

- *Past experience* is a key factor to enhance trust decisions (see also Section 3.3.1).

- *Risk* is another key factor that has always to be taken into account whenever a trustor makes a trust-based decision relative to a trustee (see also Section 3.3.1).
- *Trustee skills* constitute an important factor to make a trust decision .
- *Time* plays an important role in the trusting process because past decisions are less relevant than recent ones.
- *Opinions* (i.e., reputation) expressed by other users contribute to the formation of an individual trust assessment.
- *Personalization* is a mind set experience that determines how trustor makes a decision based on his/her personal perception about the trustworthiness of a trustee. Trust varies from a person to another, i.e., trust represents a personal view.
- *Context* is of paramount relevance to determine suitability of the trustee to perform the allocated task.
- *Social proximity* influences how trust is established between trustor and trustee, since a trustor tends to more readily trust on a family member or a friend than on an unknown individual.

Summing up, we can say that there are factors that contribute to know how a trustor develops trust on a trustee. In other words, trust factors can be seen as information sources used in the trust building process, as expressed in the following definition:

Definition 5 *A trust factor is information used by the trustor to build the knowledge required to the establishment of a trust relation with a trustee.*

In [JP05], trust-influencing factors were classified as intrinsic and extrinsic. Intrinsic factors constitute trustee information directly collected by the trustor, while extrinsic factors comprise trustee information obtained from other sources. In the context of web services, nineteen factors were identified in the process of how users determine trust in web content [GA07], and are the following: topic, context, popularity, authority, direct experience, recommendation, related resources, provenance, expertise, bias, incentive, limited resources, agreement, specificity, likelihood, age, appearance, deception, and recency. Others like [Yan08a, YZV14] see these factors in five categories: context factors, trustee's objective factors (e.g., trustee's reputation), trustee's subjective factors (e.g., trustee's honesty and benevolence), trustor's subjective factors (e.g., trustor's attitude and willingness to trust), and finally the trustor's objective factors (e.g., trustor's criteria specified for a trust decision).

3.4 Trust Properties

In order to address how to deploy and develop a trust representation in computer science, it is necessary to come up to an understandable set of trust properties associated to *trustor-trustee relationships* (or, more specifically, human-human interactions), yet

Enhancing Trustability in MMOGs Environments

taking into consideration the trust factors addressed in the previous section. This is illustrated in Fig. 3.3, where one describes the cycle of trust initiated and concluded at the trustor. The experience-based knowledge develops and improves with the trust results obtained from the trustor-trustee interactions taking place over time.

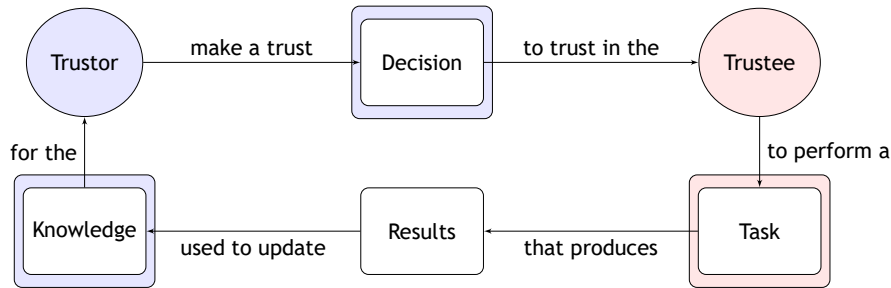


Figure 3.3: Trust cycle.

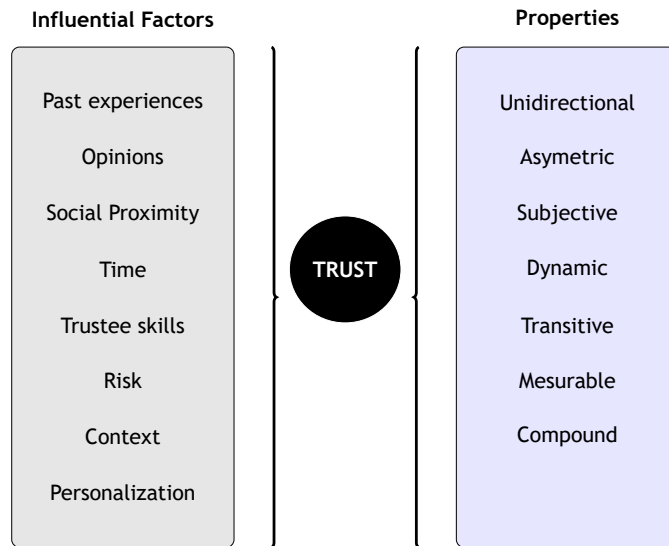


Figure 3.4: Trust properties and influence factors.

Considerable efforts have been made in order to identify a subset of common trust proprieties [GS00] [MDH02] [WE05] [Yan08b] [VM12], as shown in Fig. 3.4. They are the following:

- *Unidirectional*. Trust is unidirectional, as it represents a relationship from the trustor to the trustee [Yan08b], not the other way round.
- *Asymmetrical*. Trust is asymmetrical in the sense that the impact of a negative outcome surpasses the impact of positive outcome, i.e., a negative outcome is usually more relevant than positive outcomes previously obtained [CSMT02, CCA15].
- *Subjective*. Trust is subjective and, thus, personal [GS00]. Besides, it depends on the context the task and the trustee skills (and willingness) to fulfil such task [WE05] and Yan [Yan08b].
- *Dynamic*. Trust is dynamic because it changes over time, i.e., trustee's trustworthiness changes over time from the trustor's point of view, being highly correlated with

the knowledge that trustor has about the trustee at a given time [VSMH10, ZKB11].

– *Transitive*. Trust is transitive in the sense that it flows along a chain of (or network) of recommendations (i.e., reputation). Transitivity is often bound to the context and the trustor’s objective factors [Yan08b]. Note that trust degrades along the chain, so that trust is not perfectly transitive in the mathematical sense [Gol05].

– *Mesurable*. Trust must be measurable in the sense that it is feasible to quantify trust, i.e., distinct numeric values to represent different degrees of trust. “Trust is measurable” also provides the foundation for trust modeling and computational evaluation [Yan08b].

– *Compound*. Trust may possess multiple attributes, namely reliability, dependability, honesty, truthfulness, security, competence, and timeliness, among others, which may have to be considered depending on the context in which trust is being specified [GS00]. Therefore, composition is an important property to take into account in trust computations.

As shown above, the trust properties depend on how trust works in the human-human interactions. That is, these properties become clear after understanding how the trust-influencing factors work during human-human interactions, in order to determine whether or not an individual trusts in another individual. When a trustor-trustee interaction runs well (i.e., if the interaction outcome is positive), the trust score associated to the trustee tends to slightly increase; otherwise (i.e., if the interaction outcome is negative or behind trustor’s expectations), it tends to noticeably degrade.

3.5 Trust Inference Process

The establishment of a trust relation between two humans (i.e., a trustor and a trustee) is a complex process, which is illustrated in the diagram depicted in Fig. 3.5; the blue diagram elements concern the trustor, while those in pink are associated to the trustee. Trustor and trustee are represented by ellipses, while the tasks/actions involved in the trustor-trustee interaction are displayed as rounded rectangles.

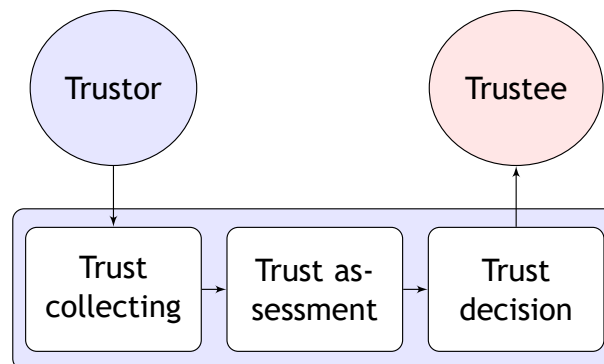


Figure 3.5: The trust decision making process.

The trust inference process is obviously initiated by the *trustor*, and consists of the following steps:

- *Trust intention*. This is a necessary pre-condition for the trustor because it is him/her who establishes a goal to be achieved (and the potential associated risk) with the his/her interaction underlying the trust relationship [CCA15]. The concept “*intention to trust*” was employed in a normative model of trust proposed by [Bew08]. A clear distinction between trust intentions, trust beliefs, and trust behaviors was addressed in [MDH02]. Others like [JB08a] saw trust intention closely tied with managing user’s behaviors by creating positive perceptions of one’s behavior and intentions.
- *Trust collecting*. This is a key stage (or task or action) to develop trust knowledge about one or more individuals [AG07], agents [ABC⁺15], or else [CSC11]. The leading idea for the trustor is to collect and aggregate trust-related data from available information sources (e.g., other users, reputation systems).
- *Trust assessment*. This step aims at calculating a trust value associated to the trustee from existing trust knowledge sources [CE15], while others like [CCA15] consider trust assessment as the trust inference process itself.
- *Trust decision*. A trust decision about the trustee is made by the trustor with reference to his/her natural tendency to trust, beliefs and past experience with the trustee [GS00] [CSC11] [CCA15]. As argued in [SNP13], in sociological and psychological terms, the trust decision process is calculative, relational, emotional, and cognitive, so that these features must be considered to reflect the human trust decision-making process [SNP13].
- *Trust action*. In our view, a trust action represents the action carried out by the trustor after his/her decision making. But, in some contexts, it may also represent an action performed by the trustee as he/she executes the task on the behalf of the trustor [VM12]. This delegation procedure was approached within a MAS context, with the argument that delegation makes relations more robust and truthful [GBL⁺15]. The delegation occurs when an trustor intent to to exploit the actions of a trustee to achieve his/her goals [CCA15].
- *Trust outcome*. The trust outcome represents the result of the action performed by the trustee after completing the task delegated by the trustor.

Fig. 3.5 shows a diagram of the main steps involved in the decision-making procedure, as part of the trust inference process diagrammatically represented in Fig. 3.3, which shows how a trust relationship is established between humans (and mediated by avatars), as usual in VW/MMOGs. Note that we are here using trust to address human-to-human interactions computationally mediated by avatars as needed in VW/MMOGs. That is, we are not much interested in other types of interactions as, for example, agent-to-agent and node-to-node interactions. It is clear that social science perspective is relevant in human-to-human interactions, particularly in respect to the reputation of the trustee,

which has to do with the community assessment about the trustee. But, the perception of the trustor about the trustee is also important, i.e., the individual assessment made by the trustor about the trustee plays an important role in the decision-making process performed by the trustor.

3.6 Trust Models

Trust modeling is a complex process because quantifying trust is not an easy task. In fact, trust is a multidimensional, multidisciplinary, and multi-faceted concept [YP11, GBL⁺15, MT11], so that finding a solution for representing trust as a quantifiable value is a real challenge. As seen above, trust congregates different properties originated in trust-influencing factors during the human-human interactions, which have much to do with not only cognitive and individual perceptions, but also reliability of information and communication [CCA15], in a way as illustrated in Figure 3.4.

Note that, as far as we know, computational trust models targeting VW/MMOGs are inexistent in the literature, simply because most trust models have been designed for agent-agent interactions, but we can find also solutions for node-node interactions in a number of networks. Thus, our approach intends to identify trust models in the literature that are susceptible of being employed in trust model solutions for VW/MMOGs. We are now in position to say that such trust model here put forward for VW/MMOGs was mainly inspired in those due to [VM12, Mom10, AKW⁺11, ABC⁺15].

3.6.1 Trust Modeling Framework

A general trust framework is shown in Fig. 3.6. It consists of three tiers: data sources, trust engine (i.e., trust model in running mode), and interaction entities (i.e., trustor and trustee).

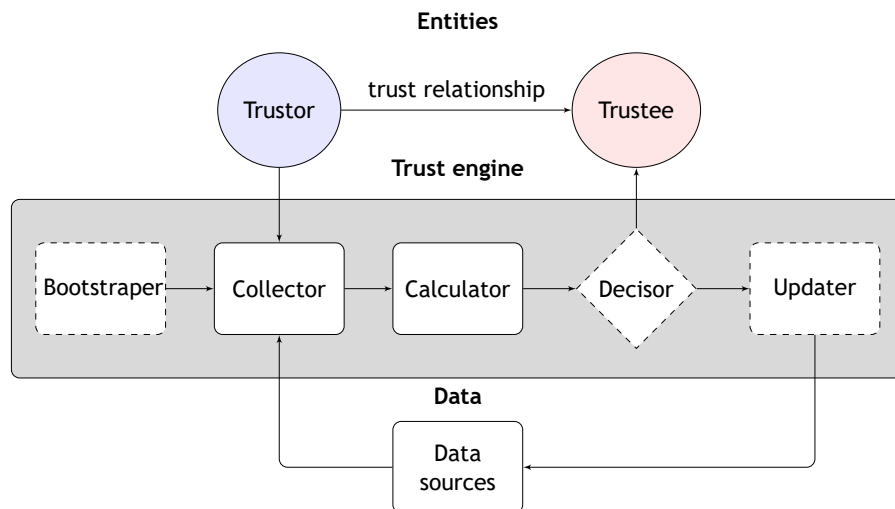


Figure 3.6: Trust computational model key components.

3.6.1.1 Trust framework tiers

Taking into consideration multiple contributions and studies on trust modeling and trust-related surveys found in the literature [SS05, ABC⁺15, NU10, GBL⁺15, JHSMT13, LLYY09, HZNR09, PSM13, SNP13, Tav12], we come across with a trust modeling framework that consists of the following three tiers:

- **Data** represents the bottom level of the framework as a set of multi-dimensional data sources, which comprises the input data that feed up the trust engine (second tier).
- **Trust engine** constitutes the middle level of the framework, which is responsible for transforming trust related-data into a quantifiable trust result. Therefore, it implements one or more trust models.
- **Entities** represent the trustor and trustee of any human-human interaction; they constitute the top level of the framework.

In general, existing computational trust models described in the literature [PSM13, CSC11, WE05] include in a way or another the tiers (and their components) displayed in Fig. 3.6. Given that the top tier was already addressed above, let us then detail the other two tiers.

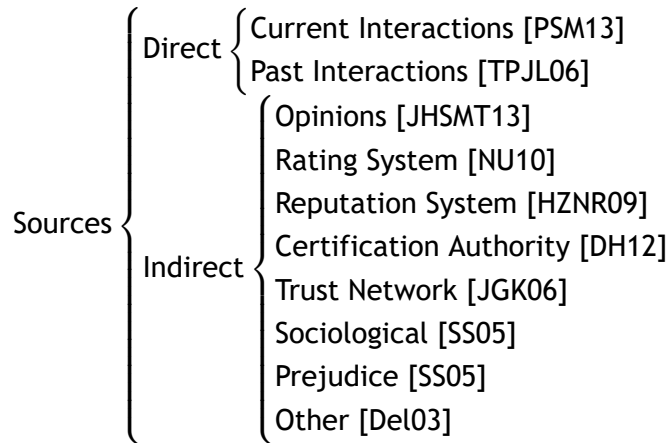


Figure 3.7: Data sources.

3.6.1.2 Data sources

Data sources (first tier) work as input for the trust engine (second tier) that implements one or more trust models, which will be discussed further ahead. They are of paramount importance because they determine which trust representation will be used in the trust model. It is clear that data sources and their representations in a given trust model varies in conformity with the context. In a simple MAS buyer/seller scenario [CE15, BRDM11], one may only include data concerning direct agent-agent interactions [JHSMT13], but in more complex scenarios like MMOGs we have to further include data

retrieved from ranking sites, reputation systems, high rank users, and guilds, some of which are external to the virtual world.

A classification of data sources is shown in Fig. 3.7, which is a result of combining different taxonomies existing in the literature [GBL⁺15, CCA15, VM12, PK08]. Data sources divide into main classes: *direct* and *indirect*. Direct data sources are generated from entity-entity interactions (*current* and *past interactions*), which are human-human interactions in VW/MMOGs. In turn, indirect data sources are third-party sources as, for example, other users/friends (*opinions*) [JHSMT13, TB06, TPJL06], *rating systems* (e.g., buyer/seller market) [Med12, NU10, GS00], *reputation systems* [JIB07, GM12, LLYY09, SNP13], *certification authorities* [OCB12, GS00], *trust networks* (e.g., Facebook) [JGK06, AKW⁺11, VGCK11, GM12, LLYY09, SNP13], *societal sources*, i.e., social networks [SS05] [SNP13] [McL11, NV12, Hos95], *prejudice*, which represents a mechanism to derive a set of preset characteristics to the trustee based on signs that identify the trustee as a member of a given group (e.g., a guild in MMOGs) [SS05, PSM13].

3.6.1.3 Trust engine

A trust engine essentially is an implementation of a given trust model. Its data structures are a computational representation of data retrieved from data sources (see Fig. 3.6). These data are important to calculate a trust value for a trustee. Taking into account trust modeling solutions found in the literature [WBOM15, SS05, JIB07], we can say that a trust engine (and its underlying trust model) consists of the following steps:

- **Collector** represents the process by which the engine collects and aggregates data relevant for building a trust representation on others (e.g., using direct interaction, reputation systems, trust networks, opinions) [GM12, YZCZ11, Med12, WBOM15, KD16]. In some circumstances, a initialization process (or **bootstrapper**) precedes the data collector step to cope with initial state or lack of information [ABC⁺15, CKN⁺15, NU10, OCB12, SB14, WBOM15].
- **Calculator** is the process used to calculate a trust value for a trustee based on the data collected about him/her in the previous step [CSC11], i.e., the trust value represents the degree of trustability of the trustee as perceived by the trustor. In the absence of such data, one uses the default data taken from the bootstrapper.
- **Decisor** is the process that leads to a decision making with reference to the trust value calculated in the previous step [JIB07, AG07, CCA15, GS00]. Note that this trust value can be changed by the own opinion of the trustor at this stage; let us called it trust outcome. That is, the trustor may opt for a discretionary decision, i.e., according to his/her beliefs and intuition [WBOM15, AG07].
- **Updater** is the process used to update or/and forward the trust outcome —determined in the previous step— to different data sources (e.g., a reputation system, a personal knowledge base, or even other users) [WHS11, GM12, Mom10].

Note that the general trust model description presented above is compatible with the majority of existing computational trust models described in recent surveys [ABC⁺15, CSC11, CCA15, LLYY09, SS05, JHSMT13]. Note that the decision step is not considered in some MAS trust models. This is so when the aim is not to provide a decision, but, instead, to provide the trustor with an individual quantifiable mechanism to assess the trustee.

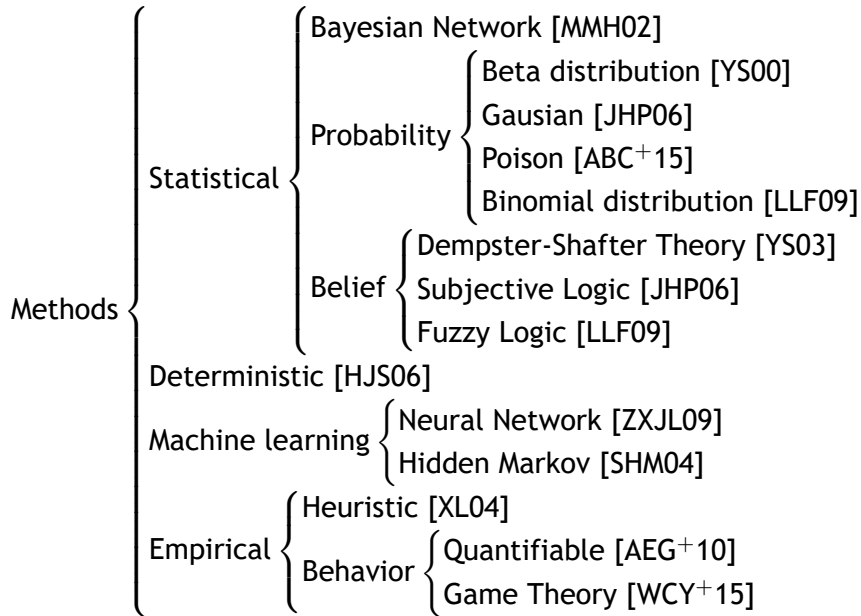


Figure 3.8: Trust methods.

3.6.2 Trust and Reputation Models

The scope of our approach is aimed to VW/MMOG trust solutions as previously stressed, although current research in computational trust solutions target to human-to-human interactions mediated by avatars in a virtual immersive environments is to the best of our knowledge neglect by the research community.

To devise possible trust modeling solutions suitable for VW/MMOGs, an assessment of existing literature was made that resulted in a selection of seventeen trust models. Aiming with this procedure to evaluate their potential for usage in VW/MMOGs. The selection process was based on two key features: the first similitude with VW/MMOG issues and the existence of a suitable testbed platform in which the modeling solution could be experimental assessed, further evaluated and or used further in experimental developments targeted to VW/MMOGs.

Regarding the choices made in the selection of the models were based in a wide coverage of contributions that span different areas from agent and multi-agent systems to P2P and WSN networks, using different types of data and trust assessments and trust decisions mechanisms. We present next a brief description of the models main features regarding its implementation (i.e. types of data used, aggregation trust mechanism and trust

Table 3.7: Trust models and their sources and trust methods (engines).

Data sources/Engines	Trust Models																
	A&H [ARH00]	Sporas [ZM00]	REGRET [SS01]	BRS [JI02]	Y&S [YS03]	EigenTrust [KSGM03]	FIRE [HJS04]	PeerTrust [XL04]	Y&S&S [YSS04]	AppleSeed [ZL05]	TNA-SL [JHP06]	TRAVOS [TPJL06]	PowerTrust [ZH07]	TACS [GMMPGS09a]	BTRW-WSN[MP11a]	LFTM [MMBP12]	TRIP [MP12]
Data sources																	
Direct experiences	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Opinions/witnessed	•	.	•	•	•	•	•	•	•	.	.	•	•	.	.	.	•
Authority	•	•
Social	.	.	•
Role based	•
Trust methods (engines)																	
Deterministic	•	.	•
Probabilistic	•	.	.	•	.	.	•	.	•	.	.	.
Machine learning	.	•
Statistical/geometrical	.	.	•	•
Dempster-shafter	•
Subjective logic	•
Beta probability	.	.	.	•
Subjective probability	•	•
Bayesian learning	•
Fuzzy logic	•	.
Other	•	•	.	.

Legend: • used ◦ not used . not applicable

decision as well as its key proprieties). For a more detailed view on the models consider the authors publication in the references and the existing surveys that address these trust models illustrated in Tab. 3.1.

3.6.2.1 Abdul-Rahman (2000)

Abdul-Rahman's trust model is inspired in a sociological view of trust as of real world situations, aiming the virtual communities in this manner [ARH00]. Data sources: Therefore, it is based on real-world social interactions (i.e., direct interactions), and also on reputation data (i.e., recommendations) produced by the word-of-mouth mechanism, this way empowering individual users with trust decisions about others, rather than relying on a centralized approach [Mom10].

Data collection and representation: Each agent is associated to two sets (or data structures). The first is the set D of direct interactions, whereas the second is the set R of recommendations, a recommendation per recommender agent.

The set of direct interactions can be expressed as $D \subseteq C \times A \times E$, where $C = \{c_1, \dots, c_n\}$ is the set of contexts faced by the agent, $A = \{a_1, \dots, a_m\}$ is the set of agents with whom the agent has interacted with, and $E = \{(G, g, b, B)\}$ is the set of past expe-

riences, where G is the integer accumulator for very good experiences, g the integer accumulator for good experiences, b is the integer accumulator for bad experiences, B the integer accumulator for very bad experiences.

The set of recommendations can be expressed as $R \subseteq C \times A \times T$, with $T = \{(T_G, T_g, T_b, T_B)\}$ denoting adjustment experiences relative the (trustor) agent. As explained further ahead, the domain of T_G , T_g , T_b , and T_B is the set $\{-3, -2, -1, 0, 1, 2, 3\}$, with each value expressing a possible semantic distance between the trust degree determined by the trustor and the trust degree determined by the recommender agent. In fact, the trust degree d takes on one of the following qualitative values: very trustworthy, trustworthy, untrustworthy, and very untrustworthy [ARH00]. Then, let a_i be a trustor agent and a_j a recommender agent; if a_j recommends to a_i that a_k is very trustworthy in a given context, and a_i assessment of its experience with a_k is very untrustworthy, we can say that a_i experience with a_k downgrades a_j recommendation by 3 (i.e., the adjustment difference is $T_B = -3$).

Trust computation and decision: As said above, the trust degree d (or trustworthiness) of an agent takes on one of the following values: very trustworthy, trustworthy, untrustworthy, and very untrustworthy. The trust degree depends on past experiences with other agents. For example, let a_i be the trustor agent and a_k the trustee agent, and $(G, g, b, B) = (9, 4, 5, 3)$ the tuple consisting of the number of very good past experiences ($G = 9$), the number of good past experiences ($g = 4$), the number of bad past experiences ($b = 5$), the number of very bad past experiences ($B = 3$).

Taking into account that the trust degree is defined as $d = \max(G, g, b, B)$, we see that the trustor a_i considers the trustee a_k as very trustworthy, because there is one-to-one correspondence between the qualifier of past experiences and the qualifier of trust degree. After calculating the trust degree, the direct interactions take the form of 3-tuples (a, c, d) , where a stands for the trustee agent, c the context of interaction, and d the trust degree.

Note that this model is capable of learning and correcting opinions, mainly because of the downgrading and upgrading mechanisms provided by the semantic distance explained above. In a way, it is a simplification of Marsh's work as only four trust values are considered. But, nothing is said about how to discover other agents that have interacted with the trustee agent being assessed, so that updating the data structures may be very time-consuming, in particular for systems for a large number of agents. For further details about the model, the reader is referred to [ARH00].

Surveys and Testbeds: The reader is referred to Table 3.7 for further details about this model when compared to other trust models. This model is also described and compared to others models in various surveys [JHSMT13, Med12, NU10, TPJL06], as shown in Table 3.1. As a proof of concept, this model developed as a MAS platform testbed [ARH00] (see Table 3.2).

Usage in VW/MMOGs: In our opinion, this trust model might be incorporated in VW/MMOGs, because it copes with misbehaviors, with the advantage that it uses a learning mecha-

nism capable of correcting opinions (e.g. when an agent consistently badmouths other agents its opinions are downgraded) [JHSMT13].

3.6.2.2 Zacharia & Maes (2000)

[ZM00] proposed two reputation mechanisms for trust management, called *Sporas* and *Histos*, in the context of electronic commerce, though they argue that those mechanisms are applicable to electronic communities (e.g., chatrooms, newsgroups, and mailing lists). These two complementary mechanisms are based on collaborative rating and personalized assessment of the various ratings ascribed to each user. *Sporas* was thought of to be applied to loosely connected communities, whereas *Histos* is more adequate for highly connected communities.

Data sources: *Sporas*' data sources only consider direct interactions (called *transactions*) in the rating procedure, while *Histos* also considers opinions.

Data collection and representation: Essentially, *Sporas*' representation is a set of pairs (u_i, r_i) , where u_i stands for the i -th user and r_i its global reputation value in the community. The reputation of each user is updated over time with the interactions he/she experiences with other users. That is, *Sporas* fosters the collaborative rating in respect to reputation.

Unlike *Sporas*, *Histos* represents the pairwise ratings as a directed graph, whose nodes represent users, while directed edges represent the most recent reputation ratings assigned to users by others. Thus, when a transaction starts taking place between two users, we have to check whether there is a graph path between them, in order to consider the reputation ratings associated to the edges of such path. The leading idea is to calculate the trustworthiness of someone using a transitivity-based mechanism that translates into the following: we tend to trust someone who has the confidence of someone in whom we trust. This allows for online transactions with someone a user has never interacted with before, since there is a path between them in the graph. *Histos* uses a breadth-first search (BFS) algorithm to determine all the paths between two users, selecting then the most recent of them.

Trust computation and decision: *Sporas* uses a *machine-learning method* that calculates a global reputation value for each user belonging to the online community. Basically, it uses a recursive formula that updates the reputation value ascribed to each user whenever a new transaction with a third party takes place. This means that the most recent ratings have more impact on the global reputation value of a user than the less recent ratings. In fact, the model does not take into account a track record of past behaviors, nor the context within which the interactions take place; as a consequence, it does not possess anti-cheating mechanisms to deal with misbehaviors [PSM13].

In regard to *Histos*, it also uses a recursive reputation formula or function to calculate personalized reputation values, which takes into consideration the graph path between two interacting users. This formula can be seen as a modified version of *Sporas*' repu-

tation formula. However, Histos does not consider the existence of loops in the paths between two users. Note that the recursion of both Sporas and Histos reputation formulas provide a straightforward mechanism to proceed to reputation updates.

Surveys and Testbeds: For more details about this model, when compared to other models, the reader is referred to Table 3.7. This model was surveyed by [Med12] (see Table 3.1), though it was also considered and studied in [MP10] [Tav12] [MMH02] [Urb13]. For one of its implementations, it is convenient to have a look at the testbed described by [SVB05] (Table 3.2).

Usage in VW/MMOGs: As explained above, this model is not adequate for VW/MMOGs because it is not able to deal with misbehaviors in a proper manner.

3.6.2.3 Regret (2001)

This model has been proposed by [SS01]. Its applicability is focused on complex e-commerce environments where coexist several types of agents in which social relationships play a relevant role [NU10]. Nevertheless, Regret lacks a trust update mechanism [WHS11], and does not allow anonymity [MP10]. However, this model differs from others described above because the social stance of each agent in society plays an important role in weighting of opinions of other agents. That is, the social group of a given agent influences the reputation value ascribed to the agent itself.

Data sources: Taking into consideration that this model essentially comprises not only agents, but also groups of agents, and their interactions.

Data collection and representation: Results or outcomes of interactions are collected into impressions, which are represented as 6-tuples (a, b, o, ψ, t, W) , where $a, b \in \mathbf{A}$ denote members of the set \mathbf{A} of all agents, $o \in \mathbf{O}$ is the outcome of a given interaction between a and b , ψ is the variable of the outcome that is judged by a , t is the time of the occurrence of the impression, and $W \in [-1, 1]$ represents the subjective opinion of the agent a relative to ψ for the particular outcome o .

The 6-tuples above are used for impressions resulting from direct interactions $a \rightarrow b$ between two agents $a \in \mathcal{A} \subseteq \mathbf{A}$ and $b \in \mathcal{B} \subseteq \mathbf{A}$. Similar tuples can be used for impressions that result from other three types of interactions, namely: (i) $a \rightarrow \mathcal{B}$ for interactions between the agent a and the group \mathcal{B} , to which the agent b belongs; (ii) $\mathcal{A} \rightarrow b$ that translates into impressions featuring what the (members of) group of a think about b ; (iv) $\mathcal{A} \rightarrow \mathcal{B}$ that translates into impressions featuring what the (members of) group of a think about the (members of) group of b . The direct interactions aim at capturing what we call *individual reputation*, while other three types of interactions aim at capturing what we call *social reputation*.

Trust computation and decision: This model comprises five reputation measures. The first concerns the computation of individual reputation (i.e., direct interactions) as the weighted mean of the impression rating factors, though considering that recent impressions are more relevant than any other ones, i.e., this measure follows a *statistical approach*. The next three measures concern the social reputation fueled by the three

types of social interactions. Each one of these three social reputation measures is defined as convex combinations of individual reputations, i.e., these measures follow a *geometric approach*.

Regret combines the above four reputation measures concerning the individual and social reputations relative to a number of aspects, with each aspect defined by the variable ψ in the impressions, in order to calculate the overall reputation of a given agent represented by a node of an ontological graph. Thus, the model strengths lie in the compositional approach that successfully deal with many of the issues of trust and reputation in virtual communities [Pat07]. However, Regret does not distinguish dishonest from incompetent agents [Med12].

Surveys and Testbeds: This model is surveyed by [NU10] and [Med12] (see Table 3.1), though it appears also discussed in [Bhu11] [MP10] [Tav12] [MMH02] [Urb13] [MP10] [You07]. Its characteristics are summarized in Table 3.7. As shown in Table 3.2, it was incorporated in TREET testbed [KC10].

Usage in VW/MMOGs: As noted by [Med12], Regret is not capable of distinguishing dishonest from incompetent agents, so its applicability to VW/MMOGs is undermined.

3.6.2.4 BRS (2002)

The trust model underlying the beta reputation system (BRS) is a *probabilistic model* based on the beta distribution [Jl02]. Unlike the majority of prior reputation systems, which in a way were intuitive and *ad hoc*, the BRS has firm foundations in the theory of statistics. BRS was designed for online communities (in particular e-commerce applications) according to a centralized approach, but it can be easily reformulated to be used in a distributed manner.

Data sources: This model uses direct interactions (here called *transactions*) between agents. Each agent provides feedback (i.e., opinions) about the other agent involved in the same transaction.

Data collection and representation: Transactions are collected into a centralized repository called feedback collection and reputation rating centre. Transactions are represented by two 5-tuples, (a, b, p, n, t) and (b, a, p, n, t) , where where a and b are the participating agents in the transaction, p and n stand for the positive and negative feedbacks, respectively, which are provided simultaneously, and t is the time of the occurrence of the transaction. These 5-tuples extend the 2-tuples (p, n) called feedback tuples referred by Jøsang [Jl02].

Trust computation and decision: BRS is based on the computation of beta probability density functions in order to combine positive and negative agent feedback and determine reputation ratings. In order to prevent that feedback tuples accumulate over time, one uses a recursive formula that expresses the overall feedback about each agent as the result of combining all of its partial feedbacks in transaction tuples; this formula also incorporates a forgetting factor that models the decay of the newest feedbacks to oldest feedbacks. Besides, this formulation also considers that feedback from agents

with high reputation rating is more significant (i.e., more weighted) than agents with low reputation rating, using a discount operator for that purpose.

Surveys and Testbeds: For further details about the BRS trust model, the reader is referred to Table 3.7, where its characteristics are shown. It also appears discussed in the surveys due to [JHSMT13, Med12, NU10], as listed in Table 3.1. As far as we know, implementations of this model are available in two testbeds, Simulator [SVB05] and ATB [JHSMT13] (see Table 3.2).

Usage in VW/MMOGs: The model do not consider misbehaviors explicitly in its deployment. However, it supports a protection mechanism against unfair ratings (positive or negative), which can be used to diminish the risk of misbehaved users' attempts to manipulate the reputation system for their own benefits. The model uses statistical filtering techniques based on beta distribution to dynamically expel users with unsatisfactory rating levels [NU10]. In short, BRS seems to be relevant to minimize the impact of misbehaviors in VW/MMOGs reputation services.

3.6.2.5 Yu & Singh (2003)

This trust modeling solution was put forward by [YS03], and is a follow-up of an approach towards social reputation management [YS00], in which the belief ratings of an agent about another are represented as scalars, which are then combined with testimonies, using for that purpose combination schemes that are similar to certainty factor models. But, these models have drawbacks that led to search for alternative approaches, more specifically an evidential model of reputation management [YS02] based on the Dempster-Shafer Theory of Evidence [S⁺76], which ended up being further extended to consider the concept of deception in the present model [YS03].

Data sources: The model uses two different sources of information: direct interactions and opinions. Opinions are relevant in the absence of direct results. In this model, recommender agents are called *witnesses* and opinions are named *testimonies*. But, there is here a subtle difference between a recommender and a witness in the sense that an opinion may lead to rumors (i.e., an agent may hold an opinion that it heard from another agent, a problem known as double counting of evidence), while a testimony is based on independent direct observations.

Data collection and representation: Each agent holds a set of acquaintances, some of which are known as its neighbors. These neighbors play the role of witnesses because they are those agents that firstly a given agent will contact for testimonies, but they are also those that such an agent will refer to others. It is clear that each agent may change the state of its acquaintances as a result of the following events: (i) based on its direct interactions with a particular acquaintance; (ii) based on interactions with agents referred to by a particular acquaintance; and (iii) based on ratings of this particular acquaintance as received from other agents. It is also clear that an agent changes its neighbors among its acquaintances over time. Testimonies are thus obtained from a trust network (in the form of a directed graph) of its acquaintances that can also refer

to other agents (i.e., transitivity) but using a depth bound in the chain, in order to limit the processing burden of running large multi-agent systems.

Trust computation and decision: The model uses a straightforward aggregation mechanism of testimonies as a way of avoiding the effect of rumors. Such testimonies are represented using Dempster-Shafer belief functions, which are still used not only to capture uncertainty but also to proceed to rating. For rating purpose, one uses a particular weighted majority algorithm (WMA), because the ratings that come from witnesses are belief functions, not scalars. In fact, this WMA variant was thought of to predict the trustworthiness of a given agent from a set of testimonies provided by witnesses. Interestingly, this model uses a simple mechanism to detect deception in the aggregation process of ratings.

Surveys and Testbeds: For a comparison of the model characteristics with other trust models, the reader is referred to Table 3.7 for additional details. The trust model due to Yu & Singh appears in the surveys [JHSMT13, Med12, NU10] listed in Table 3.1. To the best of our knowledge, implementations of this model are carried out in two testbeds, TREET [KC10] and ATB [JHSMT13] (see Table 3.2).

Usage in VW/MMOGs: Taking into consideration that this model addresses the adulteration of reputation to help an agent to distinguish reliable witnesses from deceptive witnesses, minimizing the effect of testimonies from deceptive witnesses, we can conclude it is relevant for VW/MMOGs. Nevertheless, it considers that a reliable witness is always reliable, and a deceptive witness is always deceptive, i.e., it does not consider that a witness changes its behavior over time. Later on, this constraint was relaxed in the follow-up model described further ahead in Section 3.6.2.9.

3.6.2.6 EigenTrust (2003)

Unlike BRS, which is based on a centralized system to store transactions and manage trust ratings, EigenTrust relies on a distributed trust model, provided that it was designed for peer-to-peer systems [KSGM03]. Peer-to-peer systems are a common choice for sharing and distributing information. However, given the anonymous and open nature of these networks, they provide the ideal environment for the spreading of malware. EigenTrust proposes a method to address this issue by assigning a global trust value to each peer in the network based on its past activities or interactions with other peers. As peers use these global trust values to make their choices, malicious peers are easily identified and their impact on the system is minimized since measures are taken in order to isolate them in the network.

Data sources: EigenTrust' data sources hold direct interactions between agents, as needed in the rating procedure.

Data collection and representation: EigenTrust represents trust in a distributed manner, so that it is considered as a peer-to-peer reputation system. This means that each peer a holds the interactions with other peers in the form of 3-tuples (b, n, p) , where b denotes the trustee peer (i.e., the peer judged by a after the transaction), n is the ac-

cumulator holding the number of negative interactions with a , and p is the accumulator holding the number of positive interactions with a . The local trust value of b hold by a is then given by the difference $p - n$.

Trust computation and decision: The challenge for peer-to-peer reputation systems like EigenTrust is how to aggregate the local trust values spread over the peers to determine the global trust value for a given peer, i.e., without using a centralized repository. To obtain such a global trust value associated to a peer b , one has to aggregate the local ratings of all peers –though weighted by their global reputations–, but this would congest the network with system messages requesting the local trust value of b to every single other peer. Note that local trust values have to be normalized to ensure that malicious or untrusted peers are identified are excluded from the trust network.

To overcome this problem, EigenTrust uses transitive trust, i.e., the peer a asks its acquaintances (or friends) for their opinions about peer b , and in turn a asks its acquaintances' acquaintances, and so forth. Interestingly, transitive trust leads to a matrix of normalized local trust values left principal eigenvector represents global trust values. This method of computing global trust has a *probabilistic* interpretation similar to the Random Surfer model [BP98].

Surveys and Testbeds: The reader is referred to Table 3.7 that summarizes EigenTrust's key features. EigenTrust is also briefly described an compared to others models in various surveys [CE15, HZNR07, JHSMT13, PSA12, LLYY09], namely those listed in Table 3.1. As far as we know, EigenTrust model is implemented in five testbeds listed in Table 3.2.

Usage in VW/MMOGs: This approach is particularly adequate for VW/MMOGs because it allows us to identify misbehaved avatars by means of the normalization of the local trust values that an avatar holds about others [CG14].

3.6.2.7 Fire (2004)

This is a trust and reputation model for open multi-agent systems [DHJS04] [HJS06]. This model considers trust relationships as one-to-one relationships between agents, and reputation relationships as many-to-one relationships between society and each agent, i.e., trust is understood as being individual and societal.

Data sources: The model exploits four information sources: direct interactions, context-based roles, (witness) testimonies, third-party referrals or credentials. The first two sources allow for rating *individual trust*, more specifically interaction trust and role-based trust. Interaction trust is determined from each agent's past experiences in its direct interactions with other agents, whereas role-based trust builds upon on direct interactions between agents of the same group or context (or role) as, for example, group of friends [NU10].

The last two sources allow for rating *reputation* (also called *societal trust*), i.e., witness reputation and certified reputation. Witness reputation is built upon testimonies (or reports or observations) of witnesses in respect to an agent's behavior, while certified

reputation stems from certified or third-party references made available by the agent itself upon request.

Using four data sources makes FIRE more robust and reliable when compared to other models. Of particular importance, it is the fact that FIRE puts forward with a novel type of reputation, here called certified reputation. The other three ways of building trust (i.e., interaction trust, role-based trust, and witness reputation) have well-known limitations. In fact, certified reputation is particularly beneficial for the initial interactions among agents, when no other prior input is available.

Data collection and representation: As usual, individual interaction-related data are represented in the form of tuples (a, b, c, i, v) , where a and b represent agents participating in the interaction i , $v \in [-1, 1]$ (i.e., -1 for absolutely negative and +1 for absolutely positive) is the trust rating ascribed by a to b in respect to the term c (e.g., honesty, quality). Societal data represent many-to-one interactions, which can be decomposed into one-to-one interactions as before. For example, witness interaction is an aggregate of a number of one-to-one interactions that a trustor agent collects from other agents that have interacted with the trustee agent before. Nevertheless, given the limited memory space resources, each agent only holds the latest ratings ascribed to any other agent. This means that FIRE is a decentralized model so that each agent stores its local rating database.

Trust computation and decision: This model combines those four trust sources from multiple agents to achieve a trust value for a target agent. More specifically, trust is defined as the subjective *probability* given by the weighted mean of all available ratings as follows:

$$\mathcal{T}_K(a, b, c) = \frac{\sum_{r_i \in \mathcal{R}_K(a, b, c)} \omega_K(r_i) \cdot v_i}{\sum_{r_i \in \mathcal{R}_K(a, b, c)} \omega_K(r_i)} \quad (3.1)$$

where $\mathcal{T}_K(a, b, c)$ stands for the trust value ascribed by agent a to agent b relative to term c , which is determined by the component $K \in \{I, R, W, C\}$, with I standing for interaction trust, R role-based trust, W witness reputation, and C certified reputation; $\mathcal{R}_K(a, b, c)$ denotes the set of ratings associated to component K in the computation of trust of a in b ; $\omega_K(r_i)$ stands for the rating weight function that determines the relevance of the rating r_i ; and v_i stands for the value of the rating r_i . For more details about the computation of this trust formula, the reader is referred to [HJS06].

Surveys and Testbeds: The FIRE model has been discussed in prior surveys [Med12, NU10] (see also Table 3.1), and briefly addressed in the trust-related literature in general [AG07, Med12, Tav12, PSM13, You07]. Its key characteristics are listed in Table 3.7, where it is compared with other modeling solutions. Let us also mention that the FIRE trust model was implemented in TREET testbed [KC10] (see Table 3.2).

Usage in VW/MMOGs: The FIRE model solution [HJS04, DHJS04] employs multiple data sources to build a trust assessment. Therefore it is based on a more complex representation that can lead to more accurate assessments. Its multi-variate representation may work as a basis to design a valuable approach in the development of trust assessments

in VW/MMOGs avatar interactions.

3.6.2.8 PeerTrust (2004)

The PeerTrust model was developed in the context of trust and reputation solutions for P2P e-commerce communities [XL04], i.e., it follows a decentralized approach. PeerTrust is a reputation-based trust framework that builds upon an source-adaptive trust model. This model is based on transaction-based feedback mechanisms that allow us to quantify and compare the trustworthiness of peers. In more specific terms, the trust ascribed to each peer is determined by five factors: (i) the other peers' feedback received by a peer; (ii) the total number of transactions performed by a peer; (iii) the credibility of the feedback source or peer; (iv) transaction context factor for distinguishing critical transactions from less or non-critical ones; and (v) community context factor that represents community-related characteristics and vulnerabilities.

Data sources: The input sources are the transactions (or direct interactions) between peers. It is clear that each agent provides feedback (i.e., opinions) about any other agent with whom it interacts.

Data collection and representation: As usual, transactions are represented as tuples. In conformity with the trust formula further below, each transaction tuple at least includes the evaluator peer, the target peer, the transaction identifier, the occurrence time of the transaction, the satisfaction value assigned by the evaluator peer to the target peer after the transaction.

Trust computation and decision: Taking into account the five aforementioned parameters, PeerTrust uses a *deterministic* formulation to compute the peer u 's trust value as follows:

$$T(u) = \alpha \cdot \sum_{i=1}^n S_i \cdot K_i \cdot T_i + \beta \cdot C(u) \quad (3.2)$$

where n stands for the total number of transactions involving peer u and other peers, S_i represents the normalized amount of satisfaction that peer u receives from the other peer participating in the i -th transaction, K_i denotes the credibility value of the feedback provided by other peer participating in the i -th transaction, T_i is the adaptive transaction context factor associated to the i -th transaction, and $C(u)$ is the adaptive community context factor relative to peer u , while α and β stand for the normalized weight factors concerning the collective assessment and the community context factor, respectively. Note that the trust value $T(u)$ assigned to peer u is cumulative, i.e., it can be calculated in an incremental manner without the need of storing all past transactions locally.

Surveys and testbeds: PeerTrust's key characteristics are listed in Table 3.7, but we can find further details about this model, as well as a comparison with other modeling solutions in a number of surveys, namely those due to [Pat07, GMMPGS09a, NU10, Xin11, Med12, PSA12, VM12] (see also Table 3.1). It also worthy noting that PeerTrust's model

was implemented in two testbeds, TRM-Sim [GMMPGS09a] and Testbed [CE15], as indicated in Table 3.2.

Usage in VW/MMOGs: The model incorporates the advantages of feedback information from peers, as a key feature in trust development. This is also a feature that could be incorporated in future trust models for VW/MMOGs.

3.6.2.9 YSS (2004)

YSS is a shorthand of authors' surnames of trust model put forward by [YSS04]. YSS trust model was developed for multi-agent systems over P2P networks with high scalability, where each peer is a software agent. In fact, it is a follow-up of the Yu-Singh trust model described above [YS03]. This model introduces a new distributed reputation mechanism capable of detecting malicious or unreliable peers in P2P systems. In fact, it goes a step forward relative to prior models in the sense that it effectively aggregates noisy (dishonest or inaccurate) ratings based on weighted majority techniques, no matter they originate from independent or collusive peers. Besides, it allows for the analysis and defence against eventual attacks on reputation mechanisms. Note that YSS model does not take any advantage of using trusted third parties or authorities.

Data sources: As in [YS03], this model uses two types of data, direct interactions and opinions. Note that others' opinions are a particular case of indirect interactions [JHSMT13].

Data collection and representation: Similar to [YS03], YSS also uses tuples to represent interactions, and each peer owns a set of acquaintances, among which a subset of neighbors is adaptively selected when it comes the time of rating someone else. A given peer's neighbors work as the preferential interface between it and the community when it needs to get/provide feedback about a third-party peer, what may help in detecting malicious peers.

Trust computation and decision: Contrary to most existing methods at that time, which use binary ratings, YSS uses a *probabilistic* method for both local and aggregate ratings, which take on values between 0 and 1. This method uses aggregate ratings to produce a trust value either as simple averaging or as exponential averaging, and this makes a difference in relation to authors' previous approach [YS00, YS02]. In addition, YSS model also addresses attacks from colluding groups.

Surveys and testbeds: YSS' key characteristics are listed in Table 3.7. This model has been discussed in the literature as, for example, in [Pat07, Xin11, CE15], including in a previous survey due to [JHSMT13] (cf. Table 3.1). Note that the YSS trust model was implemented in two testbeds, Simulator [SVB05] and ATB [JHSMT13]. For further details, the reader is referred to Table 3.2.

Usage in VW/MMOGs: Essentially, this model computes trust from direct experiences, so that opinions are only taken into account when there is not enough supporting evidence from such experiences. But, an incorrect opinion results in a cut by half in the corresponding agent credibility [JHSMT13], what is advantageous for VW/MMOGs

because allows us to deal with liars.

3.6.2.10 AppleSeed (2005)

This trust modeling solution was designed for the semantic web, and uses a flow-based assessment to devise a local group trust network [ZL05], though its authors noted its suitability to other purposes, namely group trust in online communities, open rating systems, and ad-hoc and peer-to-peer networks. Appleseed takes advantage of spreading activation models used in psychology to simulate human semantic memory, relating their concepts to trust assessment in an intuitive manner. These spreading activation models were first proposed by [Qui68].

Data sources: As usual, this model uses direct interaction between agents as input.

Data collection and representation: Direct interaction data are then employed to produce a directed weighted graph, whose nodes and edges represent agents and trust relationships, respectively; the weight associated to each edge denotes the trustworthiness of an agent in another. This graph is used to determine the amount of trust that flows across the trust network.

Trust computation and decision: AppleSeed is based on a *deterministic* method for trust. Similar to Advogato [LA98] [Lev04], yet the latter is a non-deterministic model, AppleSeed aims at helping online community members to discover and distinguish between trusted users and untrusted users. Both models proposed local group trust metrics, but Advogato is based on the maximum network flow computation, while Appleseed's leading idea lies in spreading activation models.

The assessment process is initialized with a trust seed, an energy value, a spreading factor decay and a convergence threshold, Appleseed then produces a trust score of agents from the perspective of the trust seed. To avoid occurrence of loops in Appleseed trust graph processing a termination condition is required to be associated to Appleseed decay factor. The motivation for the approach has two goals. The first is to use a partial trust graph exploration to reduce computational complexity. The second approach eliminates the need to explore a global trust graph in most cases, thus helping to reduce the computational complexity by limiting the scope of the computation to a reduced trust graph [SNP13].

Surveys and testbeds: AppleSeed was evaluated in the following surveys [CE15, SNP13, Bhu10, AG07] and further detailed in [Gol05, Bhu11, Sei05, Tav12]. Currently, AppleSeed is deployed and implemented in Chandrasekaran & Esfandiari testbed [CE15], as shown in Table 3.2. However, the testbed is not publicly available at current time.

Usage in VW/MMOGs: The concept of trust network representation can also be used in VW/MMOGs as the partial trust graph exploration could reduce the computational burden on VW/MMOGs from the additional trust solution.

3.6.2.11 TNA-SL (2007)

Trust Network Analysis with Subjective Logic (TNA-SL) is a trust model that uses a trust network to represent trust relationships and uses subjective logic to calculate trust between arbitrary network nodes [JHP06]. Recall that a trust network consists of transitive trust relationships that may involve people, organizations or/and software agents, which interact through some communication medium.

TNA-SL is different from TNA based on normalization (e.g., PageRank and EigenTrust). Normalization-based trust models have the advantage of allowing for the analysis of large highly connected random graphs in their entirety. However, these normalization-based trust models cannot express and handle (e.g., propagation of) negative trust, what makes trust metrics relative instead of absolute, as needed in measuring, for example, statistical reliability. On the contrary, TNA-SL can express and propagate negative trust in a transitive manner. In addition, TNA-SL trust measures are equivalent to beta PDFs; as a consequence, trust measures can be straightforwardly interpreted in statistical terms (e.g. as measures of reliability). The main shortcoming of TNA-SL is that a trust network has to be simplified before its trust analysis, which may lead to loss of relevant information.

Data sources: This model resorts to a data source of direct interactions to represent trust relationships.

Data collection and representation: TNA-SL essentially builds upon the analysis of trust networks (i.e., graphs), which can be represented by means of canonical expressions. Nevertheless, such trust networks are simplified as directed series-parallel graphs (DSPG)—what amounts to simplifying canonical expressions—, before combining such expressions with subjective logic operators in order to derive a trust value about someone. Trust network simplification consists in finding all DSPG paths between trustor and trustee, i.e., paths along which an edge appears only once; in other words, there is no room for cycles.

Trust computation and decision: This model takes advantage of subjective logic [Jøs13]—a generalization of binary logic and probability calculus that includes degrees of uncertainty in addition to belief and disbelief—to calculate a trust value between any arbitrary nodes of a trust network. In fact, it is capable of deriving a trust value between any two nodes, even when there is no explicit trust path between them [JHP06, CG12]. Recall that subjective logic is a particular belief calculus (from the belief theory) that makes usage of a belief metric—called opinion—as necessary to express beliefs.

Surveys and testbeds: The key characteristics of the TNA-SL model are listed in Table 3.7, which are also addressed in a number of publications [JHP06, CG12, WAC⁺09, YZCZ11, PAS13, ZXL⁺12]. The reader is also referred to Table 3.1 for a comparison with other modeling solutions found in the literature. Note that, as shown in Table 3.2, the TNA-SL model was implemented in the P2P-Sim testbed [WAC⁺09].

Usage in VW/MMOGs: Regarding its suitability for VW/MMOGs in-world avatar trust relationships could use this modeling solution to assess trust among avatars.

3.6.2.12 TRAVOS (2006)

Trust and Reputation Model for Agent-Based Virtual Organizations (TRAVOS) model was conceived to grasp an agent's trust in another agent with which it has just finished interacting [TPJL06]; more specifically, it was developed for large open multi-agent systems (MAS) [Med12]. TRAVOS is similar to the Beta Reputation System (BRS) discussed above, since they use the beta family of probability functions to determine the probability of a trustee's behavior from past interactions with such trustee. But, the models diverge in the way they handle inaccurate reputation. TRAVOS rates each reputation source in an individual manner from the supposedly accuracy of past opinions, whereas BRS starts from the assumption that most reputation sources provide accurate opinions, discarding any opinion that is noticeably far from the average. Recall that BRS does not distinguish reputation from direct observations. Moreover, TRAVOS' estimation errors decrease noticeably as the number of reputation sources increases, while BRS's error estimation performance remains constant, i.e., BRS does not learn from past experience.

Data sources: The model uses two types of data sources, whose data are obtained from direct interactions (or direct experiences) and opinions collected from other agents.

Data collection and representation: The direct interactions between trustor a and trustee b are represented as 4-tuples (a, b, n, m) , where n and m stand for the number of successful and unsuccessful interactions of a with b , respectively. Opinions are formulated from the direct interactions between any other agent and b , i.e., they are based on the reputation of the trustee.

Trust computation and decision: TRAVOS calculates trust using *probability theory*. As usual, the computation of trust builds upon past interactions between agents, as well as upon reputation data aggregated from third parties when there is no record of past interactions between such agents. More specifically, this trust computation method employs beta distribution probability functions [NU10, TPJL06].

Surveys and testbeds: TRAVOS key characteristics are listed in Table 3.7, while Table 3.1 compares TRAVOS with other trust models found in literature's surveys [GBL⁺15, JHSMT13, Med12, PSA12, WHS11, NU10, LLY09]. The reader is also referred to [CE15, Xin11, Pat07] for more details about TRAVOS' model. Let us also mention that TRAVOS was implemented in two testbeds, Simulator [SVB05] and ATB [JHSMT13] (cf. Table 3.2).

Usage in VW/MMOGs: This modeling solution provides a measure of trust based on direct interactions and opinions [TPJL06], and has the advantage of distinguishing reputation from direct observations. This specific feature is relevant in avatar interactions taking place in immersive environments like VW/MMOGs.

3.6.2.13 PowerTrust (2007)

PowerTrust was thought of as a P2P reputation system. This model is due to [ZH07], and can be seen as an extension of EigenTrust [KSGM03], in the sense that it takes into

account the distribution of peer feedbacks. More specifically, [ZH07] discovered that essentially distributed e-commerce systems like eBay follow a power-law distribution in user feedbacks (see also [HCH07]).

Data sources: The model uses as input direct interactions and feedback opinions.

Data collection and representation: Trust derived from individual interactions among peers are aggregated into a trust overlay network (TON) built on top of the P2P system.

Trust computation and decision: PowerTrust computes the global trust values in exactly the same way as that computed by the EigenTrust, but now with pre-trusted peers replaced by power nodes [HCH07, ZH07]. In fact, PowerTrust *dynamically* selects a small number of power nodes that are most reputable using a distributed ranking mechanism. The democratic idea of replacing power nodes as soon as they become less active or exhibit doubtful behavior seems to be reasonable in the context of decentralized systems. On the contrary, in EigenTrust, the choice of trusted peers is static, which is an over-optimistic assumption because pretrust peers may become non-trustful over time.

In PowerTrust, one generates feedback scores using *Bayesian learning* [BB04] or a peer satisfaction-based average rating. The local trust scores are normalized so that their summation equals 1. Identical normalization applies to global reputation scores. PowerTrust follows an ahead random walk (LRW) strategy to aggregate global reputations in an efficient manner. Therefore, each TON's node stores its own local trust scores and aggregates local trust scores of its first hand neighbors. Then, the surfer makes the decision built upon cumulative knowledge from itself and ahead (i.e., its neighbors). Besides, PowerTrust significantly improves global reputation accuracy and aggregation speed. The model is robust with high scalability to support large-scale P2P applications and resist malicious peers [KD16].

Surveys and testbeds: PowerTrust's key characteristics are listed in Table 3.7. It is described and compared with other trust models in a number of publications [KD16, HZNR07, MP09], including a survey due to [MP11b] (see also Table 3.1). Moreover, PowerTrust was implemented in two testbeds, Simulator [SVB05] and ATB [JHSMT13], as shown in Table 3.2.

Usage in VW/MMOGs: The modeling solution provided by POWERTRUST [ZH07], establishes a scalable P2P reputation system that initially selects a set of most reputable nodes (known as power nodes) using a distributed ranking mechanism. The authors claim that improves global reputation accuracy and aggregation speed. This reputation system is a relevant feature, that has applicability also in VW/MMOGs, where high rank users/avatars could be considered as the equivalent of the model power nodes. Issues due to misbehaved and colluding users are also a feature to address and develop further in future integration in VW/MMOGs.

3.6.2.14 TACS (2009)

Trust Ant Colony (TACS) System incorporates a trust model developed in the context of P2P networks, which uses an ant colony optimization algorithm for finding good and

reliable nodes in a P2P network [GMMPGS09a]. Its novelty lies in the fact it is the first evolutionary bio-inspired trust model built upon the ant colony system. This model has the particularity that it not only gets the most trustworthy node to interact with, but also the most trustworthy path leading to the most reputable peer [FGM11]. The leading idea is to solve the problem of how distinguish reliable nodes from misbehaved nodes.

Data sources: The model uses direct interaction between a client node and the most trustworthy server node that provides a specific service [GMMPGS09a].

Data collection and representation: In TACS, one uses a weighted graph to represent a P2P network, with each edge owning two weights taking on values in the interval $[0, 1]$: τ (pheromone) and η (heuristic). For a given service, the pheromone τ stands for the *trust* that each edge's start node possesses on reaching the optimum server, though passing through edge's end node. In regard to the heuristic η , represents the *similarity* between the service requested by the client node and the service offered by the most trustworthy server node. It is clear that, a benevolent server provides exactly the service requested by the client ($\eta = 1$), while a fully malicious server does not provide the service at all ($\eta = 0$).

Therefore, it is the service similarity that allows us to distinguish honest from malicious nodes in providing a given service. In fact, as soon as the server supplies a service to the client, the client assesses its satisfaction relative to the received service, which may differ from the one initially offered by the server. A client's satisfaction is computed by measuring the similarity between the requested service and the provided one. This allows to TACS applying a punishment to malicious and dishonest nodes.

Trust computation and decision: TACS incorporates the ant colony optimization algorithm (ACO). ACO method is a *probabilistic* method suited to solve problems that can be reduced to finding good paths across graphs. Among the possible server nodes offering a given service, the client chooses the optimal server node, as well as the optimal path from the client to server (i.e., the path whose nodes possess the higher level of pheromones, and which be followed by the majority of ants [SB14]).

In order to find such good paths, the method uses the so-called *transition rule*. This rule allows us to calculate the the probability of the ant k located at a given node c of moving towards one of its non-visited neighbor nodes s as follows:

$$p_k(a, b) = \begin{cases} \frac{\tau_{ab}^\alpha \cdot \eta_{ab}^\beta}{\sum_{c \in J_k(a)} \tau_{ac}^\alpha \cdot \eta_{ac}^\beta} & \text{if } b \in J_k(a) \\ 0 & \text{otherwise} \end{cases} \quad (3.3)$$

where τ_{ab} stands for the pheromone of the edge e_{ab} , η_{ab} the heuristic information (i.e., service similarity) of the edge e_{ab} , $J_k(a)$ the set of reachable nodes from a that were not visited yet by the ant k , and α and β are two weights establishing a balance between memory information and heuristic information, respectively.

The transition rule is the core of TACS, but the punishment procedure is its key because it allows us to distinguish reliable nodes from misbehaved nodes. This latter procedure

builds upon the satisfaction of the client as expressed after its interaction with the server. Satisfaction is another face for what we call trust, and is expressed in terms of the service similarity $\eta \in [0, 1]$. If the provided service is unsatisfactory, the server is punished with a η value under 0.5; otherwise, η takes a value over 0.5.

Surveys and testbeds: The model is cited by [SB14, VSP16], as well as in a follow-up development by [FGM11] which extended TACS by incorporating a genetic algorithm to optimize the working parameters. TACS trust model is available at <http://sourceforge.net/projects/tacs>, and was deployed in TRMSim-WSN (Trust and Reputation Models Simulator for Wireless Sensor Networks) [GMMPGS09a] (see also Table 3.2), a simulation platform developed in Java to test trust and reputation models for WSNs [MP10]. This simulation platform also implemented other trust models, namely PeerTrust [XL04], Eigentrust [KSGM03], LFTM Linguistic Fuzzy Trust Mechanism [MMBP12], and BTRM-WSN (Bio Trust and Reputation Model for Wireless Sensor Networks) [MP11a].

Usage in VW/MMOGs: In real life we ask our friends or acquaintances for their opinions about a future decision, so that we expect that this procedure would be equally beneficial in VW/MMOGs virtual communities. Also as envisaged by [GMMPGS09a] in the context of P2P networks, the usefulness of an mechanism to assess the global trust or reputation of a peer from collected opinions of other peers limited the probability of being cheated by a malicious peer, is something that is a valuable approach we could employ to address trust in avatar-to-avatar relationships in VW/MMOGs.

3.6.2.15 BTRM-WSN (2011)

This model is a bio-inspired trust and reputation model for wireless sensor networks (BTRM-WSN) that was developed to provide security and trustability between interacting nodes, a key feature for the network reliability and usability [MP11a]. In practice, it is a follow-up of TACS, but applied to WSNs.

Data sources: Data sources are built on direct interactions (or experience) between WSN nodes.

Data collection and representation: A network representation of WSN nodes interactions is derived from individual interactions.

Trust computation and decision: the BTRM-WSN trust model uses ant colony systems conceptualizations to deploy agents (ants) through the WSN network aiming to identify the most trustworthy path towards the most reputable service provider in the network. In the process agents leave traces in each node traversed as a confidence value that would be use to identify the most trustworthier path [MP11a]. Once the ants reach a node with the requested service, a score has to be given to each of those paths. Regarding the modeling assessment, the path with the highest value pheromone is selected by BTRM-WSN as the one leading to the most trustworthy node in the network. Then the client explicitly requests the service to the selected node it will evaluate the received service to computes his satisfaction with the performed transaction [MMBP12, MP09].

In case of a satisfactory outcome a reinforcement in terms of pheromone addition to the path leading to the node is carried out. Otherwise, a pheromone evaporation process is applied to downgrade the path leading to that node.

Surveys and testbeds: The model is also addressed in [MMBP12, MP11b, KD16]. In respect to testbeds, BTRM-WSN trust model is deployed in TRMSim-WSN [GMMPGS09a] (see Table 3.2), which implemented other trust models, namely PeerTrust [XL04], Eigentrust [KSGM03], LFTM Linguistic Fuzzy Trust Mechanism [MMBP12].

Usage in VW/MMOGs: Note that WSN nodes resemble avatars, because a node's action radius resembles avatar's Aol (area of interest); in fact, WSN node dynamics has similarities with avatars' dynamics in terms of their interactions. Besides, its minimal deployment requirements can be also used with advantage in VW/MMOGs. But, more importantly, the trust network representation and the ant colony algorithm used here to assure reliability between nodes could also be used in VW/MMOGs to identify reliable avatars to interact with and to discard misbehaved ones.

3.6.2.16 LFTM (2012)

According to its authors, the linguistic fuzzy trust mechanism (LFTM) model is one of the first models that combine bio-inspired algorithms and fuzzy logic in the field of trust and reputation systems [MMBP12]. In fact, LFTM is a follow-up of BTRM-WSN, which in turn incorporates the TACS trust and reputation model (see above). Essentially, LFTM combines TACS bio-inspired trust and reputation model and linguistic fuzzy sets for reasoning and to enhance the interpretability of the model from the human user's point view [KD16]. That is, the main goal of LFTM is to enhance TACS in order to benefit from the advantages of expressiveness of fuzzy sets and linguistic labels.

Data sources: As for TACS, the data source of this trust and reputation model consists of direct interactions between network nodes, in particular a client node and the corresponding most trustworthy server node, which supposedly provides a specific service under request. Nevertheless, while TACS was designed for P2P networks, LFTM was thought of to WSNs.

Data collection and representation: Similar to TACS and BTRM-WSN, the LFTM model uses a weighted graph to represent the network, with each edge possessing two weights; the first weight is given by the pheromone τ that takes on values in the interval $[0, 1]$, which represents the trust of edge's start node of such edge on reaching the optimal server, yet passing through edges's end node. the second weight is provided by the heuristic η , which represents the similarity between the service requested by the client node and the service provided by the optimal server node. But unlike TACS and BTRM-WSN, the heuristic is fuzzy and not numeric in order to be more human friendly. In practice, the interval $[0, 1]$ is divided into five sub-intervals that are fuzzified into the following linguistic labels: 'very low', 'low', 'medium', 'high', and 'very high'.

Trust computation and decision: Similar to TACS and BTRM-WSN, the LFTM model uses a *probabilistic* method in the computation of trust. Its novelty stems from the fact

that it uses a *linguistic fuzzy logic* approach and fuzzy reasoning not only for knowledge representation, but also for inference within a distributed network system based on an ant-colony optimization solution [KD16].

Surveys and testbeds: The LFTM trust model was implemented in TRMSim-WSN (Trust and Reputation Models simulator for Wireless Sensor Network) testbed, as shown in Table 3.2. See also [KD16] for further details about LFTM model.

Usage in VW/MMOGs: Regarding usability in VW/MMOGs the usage of a fuzzy logic as a human friendly feature, allow us to consider extending its usage to other scenarios like in avatar interactions chat messages to express trustability.

3.6.2.17 TRIP (2012)

Trust and Reputation Infrastructure-based Proposal (TRIP) was developed in the context of vehicular ad-hoc networks (VANETs) [MP12], in order to resolve unsettled issues related to security and reliability communication channels [AB16]. According to its authors, TRIP represents a trust and reputation modeling solution to enforce honest information sharing over the network and at same time identify misbehaved nodes (e.g., nodes that do not share resources and/or spread bogus and false messages) in a simple, light, fast, scalable and accurate manner [MP12]. However, its simplicity makes it vulnerable to specific security threats as it is the case of “partially malicious collectives”.

Data sources: Within a VANET, network nodes are the vehicles on the road. The TRIP trust model uses three types of information sources, namely *direct interactions* (or experiences) between nodes, *node recommendations* (i.e., referrals or opinions) of other vehicular nodes, and *authority recommendations* through road side units (RSU), whose central authority may be a government organization or department.

Data collection and representation: TRIP was conceived for VANETs, so each network node is responsible for holding the data concerning the outcomes of its interactions with other nodes.

Trust computation and decision: Whenever the vehicle v_i interacts with any other vehicle v_j , from which v_i receives a traffic warning or message, v_i computes a reputation score $R_{ij}^t \in [0, 1]$ for v_j , at time t , based on the aforementioned three sources of information as follows:

$$R_{ij}^t = \alpha_i R_{ij}^{t-1} + \beta_i \sum_{k=1}^n w_k r_{kj} + \gamma_i \rho_j \quad (3.4)$$

where n stands for the number of recommender vehicles (after being queried) at time t , $r_{kj} \in [0, 1]$ represents the recommendation v_k provided by node v_k about node v_j , $w_k \in [0, 1]$ denotes the reliability of recommendations delivered by node v_k , $\rho_j \in [0, 1]$ stands for the recommendation provided by the central authority (infrastructure) through RSUs about node v_j (which is commonly cached and refreshed), and α_i , β_i , and γ_i represent the weights associated to direct previous experiences of node v_i , recommendations of

neighbor nodes v_k , and infrastructure recommendation about v_j , respectively. Note that Eq. (3.4) is a recurrence formula, which is in conformity with storage limitations of each node. Besides, this formula is a convex combination because $\alpha_i + \beta_i + \gamma_i = 1$; in addition, the recommendations of other nodes other than v_i also form a convex combination because $\sum_{k=1}^n w_k = 1$. In short, TRIP uses a *geometric* method to compute the reputation score of each node.

After computing a reputation score for node v_j , one has to make a decision on what to do with a given traffic warning or message received from v_j . The reputation score determines the trustworthiness (or level of trust) of v_j . TRIP defines three trust levels represented as *fuzzy* sets, namely “not trust”, “+/- trust”, “trust”; “not trust” determines that the node v_j would be excluded by rejecting all data exchange with it, “+/- trust” determines that data exchange is accepted but not forwarded, and “trust” determines that all exchanges are allowed.

Surveys and testbeds: TRIP’s key features are shown and compared with other models in Table 3.7. TRIP was implemented in TRMSim-WSN (Trust and Reputation Models Simulator for Wireless Sensor Network) [GMPPGS09a] testbed (see Table 3.2).

Usage in VW/MMOGs: Regarding is potential for VW/MMOGs we identified several characteristics relevant like the exclude a particular node from sending messages could also be extrapolated to address ganking and harassment from misbehavior avatars.

3.7 Discussion

As seen above, and to our best knowledge, trust models and testbeds have not been designed and implemented for VW/MMOGs so far. In fact, we have found trust models and testbeds in three major areas of computing research: multi-agent systems (MAS), online services (e.g., e-commerce and social networks), and networking. Among the seventeen trust models described in the previous section, six of them were specifically designed for multi-agent systems, namely A&E [ARH00], REGRET [SS01], Y&S [YS03], FIRE [HJS04], Y&S&S [YSS04], and TRAVOS [TPJL06]; three models were thought of for online services, namely SPORAS [ZM00], BRS [JI02], and AppleSeed [ZL05]; at last, the remaining eight models were developed for networking, and are the EigenTrust [KSGM03], PeerTrust [XL04], TNA-SL [JHP06], PowerTrust [ZH07], TACS [MP09], BTRM-WSN [MP11b], LFTM [MMBP12], and TRIP [MP12].

In the context of VW/MMOGs, the most important point to bear in mind is the ability of a trust model in distinguishing reliable avatars from misbehaved ones over time. It happens that only seven out of those seventeen trust models are capable of identifying misbehaved users in an explicit manner, namely: Y&S [YS03], EigenTrust [KSGM03], Y&S&S [YSS04], PowerTrust [ZH07], BTRM-WSN [MP11a], LFTM [MMBP12], and TRIP [MP12]. However, a reliable avatar may become a misbehaved avatar in some circumstances, and vice-versa.

Apart the theories/models behind the computation of trust (i.e., the trust engine itself), we can distinguish a model from any other model with reference to their data sources as follows:

- All trust models are based on *interactions*. In this sense, any trust model described above is adequate for VW/MMOGs.
- Not all trust models use *opinions* (of others) to evaluate trust, namely: SPORAS, AppleSeed, TACS, BTRM, and LFTM. This may arise some difficulties to the trustor, particularly when the trustor has never interacted with the trustee before.
- In addition to interactions and opinions, some trust models use *supplementary data sources*, namely sociograms (see REGRET [SS01]) and certification authorities (see FIRE [HJS04] and TRIP [MP12]). This would be particularly useful for VW/MMOGs, because allows us to take advantage of multiple data sources.

It is clear that there are also other issues related to strategies to limit the computational burden of trust engines, in particular issues related to networking latency, but this out of scope in this thesis. Nevertheless, let us refer that AppleSeed is capable of reducing the computational complexity of graph search by limiting the search to a small part of the graph in order to calculate the trust value tied to trustee.

3.8 Summary

With some exceptions, this chapter only approaches trust models that have been implemented in testbeds in the last fifteen years, and susceptible of being incorporated in VW/MMOGs later on; exceptions are those due to [KSGM03] and [Mar94]. Note that trust in VW/MMOGs have been already addressed in the past from a sociological perspective, but exclusively using online questionnaires [DH08], as a way of studying human behaviors from in-world interactions.

On the contrary, in the current survey, we follow a computer science perspective by considering that we have incorporated a trust engine in a given VW/MMOG, which is fed with real data concerning avatar-avatar interactions, and data originated in other sources like opinions and certified authorities. In a way, this translates into the general trust framework shown in Fig. 3.6. As seen above, this framework fits in most societal applications, namely multi-agent systems, online services, and networking, as well as in VW/MMOGs. The main difference between these applications lies in the interaction entities, i.e., agents, users, nodes, or avatars, which determine the domain of application. Therefore, the main contribution of this chapter lies in the fact that it presents the first systematic approach to compare trust models in the context of VW/MMOGs.

Chapter 4

Trust Framework

Trust conceptualizations in virtual worlds and massively multiplayer online games (VW/MMOGs) are not covered as a whole by existing trust models and frameworks. Apparently, the representation and modeling of trust in a computational environment is an elusive task, largely because that seems to depend on the context within which entities (e.g., users) interact with each other. Hence, the existence of multiple trust solutions that address domain-specific problems. These solutions are scarce, or even inexistent, in VW/MMOGs. In this chapter, we thus elaborate on a trust framework for VW/MMOGs. For this purpose, we carry out a study in order to identify and characterize the VW/MMOG specific features or data sources, as well as to assess how extant trust models (say, TNA-SL, Regret, EigenTrust, Stereotrust and TACS) satisfy VW/MMOGs requirements. As a result, we get a valuable insight on how to build up a trust framework for immersive environments.

4.1 Introduction

Trust is recognized as a fundamental feature of interactions [Luh79]. These interactions can occur between multiple and different types of entities (people, computer programs, services, organizations, games, biological beings, virtual entities, countries), and span a multitude of environments and scenarios. Trust usage is widely disseminated, as it acts as a driving factor for facilitating, inducing and strengthening relations between entities [Deu58]. Therefore, efforts on concept clarification and modeling are being developed in different research fields [Mar94]. They represent a multitude of contrasting views on the topic [DH08]. Despite the persistent lack on unanimity, all contribute to enrich knowledge on trust [JB08a]. As their approaches follow different paths to identify and develop trust relevant features [AG07].

In several scenarios, trust is seen as context-dependent, in which coexist different degrees of reliability in respect to user's intent and goals to achieve. Therefore, as supporting technologies evolve and became more ubiquitous, new ways of interaction arise that require new approaches to trust integration in these new, more immersive, and persistent media like virtual worlds and massively multiplayer online games (VW/MMOGs) [Bel08]. VW/MMOGs (e.g., SecondLife, and World of Warcraft) promote another type of online human interaction that provides an additional dimension not present in existing online interaction environments like social networks or online chat services [Bar03]. In VW/MMOGs, interactions occur in an immersive environment that recreates a 3D virtual

scenario where users interact through their avatars. The virtual environment dynamics resembles to how humans perceive the real world, therefore allowing an in-world immersion user experience. The specific features of these environments, where multiple entities interact, contribute to the development of socialization in which trust and trustability issues play an important role on how users behave within the environment [ARH00, RCS⁺10]. VW/MMOGs are used in many different contexts other than online games like MMOGs (Massively Multiplayer Online Games). VW/MMOGs are used in team cooperation scenarios (e.g., military forces performing simulation exercises), in collaborative work within organizations, in learning on virtual lecturing sessions and attending virtual conferences [BL12], and also in trading within the virtual world, just to mention a few. Therefore, a VW/MMOG distinguishes itself from other types of online services and systems in that it is an immersive environment that is perceived in a different way by users [Bar03]. In particular, the in-world interactions between users resemble much of what happens in the daily life of human beings. This gives us an idea of how much challenging is to deploy a trust framework in VW/MMOGs. And this is precisely the main purpose of this chapter.

The chapter is organized as follows. Section 4.2 briefly reviews the related work. Section 4.3 approaches VW/MMOG's in a broadly sense, identifying existing features and challenges and making a parallel with other environments regarding interactions and data availability. Section 4.4 describes the trust framework (TFW) proposed in the current chapter. Next, an assessment of the proposed framework is discussed in Section 4.5. Finally, Section 4.6 concludes the chapter.

4.2 Related Work

Research on trust follows two main approaches. The first approach is tied to a consensus on what is trust, initially from a philosophical [McL11] and sociological perspective [Luh79], [Deu58] later followed by other areas that tried to reach some form of trust formalization that was recognized as context-independent, as it was the case of the mathematical formalization introduced by Marsh [Mar94, You07]. In regards to the second approach, it addresses trust in a context-dependent manner, so that we find trust solutions focused on P2P networks [KSGM03], online services [BRDM11], and so forth. That is, it takes advantage of the context in order to identify and model trust features susceptible of being used in a solution to a specific problem.

Recently, interesting surveys on trust have appeared in computer science literature [ZDB11, CSC11, GMPGS09a]. Nevertheless, they propose context-dependent trust solutions. These contributions can be categorized by application area: networking, security, artificial intelligence, human-computer interaction, and so forth. In networking and protocols, trust is used to assess nodes reliability prior to exchange information in an attempt to ensure that there are not rogue nodes tampering data or altering its content, as observed in mobile ad hoc networks (MANETs), wireless sensor networks (WSNs)

and peer-to-peer (P2P) [WE05, CSC11]. Yet another situation emerged from the trustability of the authentication procedures via certificates, public key infrastructure (PKI) and others [YWS03]. In artificial intelligence, more specifically in agents and multi-agent systems (MAS), trust is used as a framework tool to enhance reliability in agent interactions [Mar94]. Other areas like human-computer interaction, trust plays a vital role in interactions with online services, what has to do with trust usability [BRDM11]. Trust also plays a significant role in assessment of trustability in software and hardware development, as it was identified in the industry through the Trustworthy Computing Initiative [TCG11]. The impact of the virtualization has also led to trust issues linked with security and reliability of information [DPJX12]. These problems were approached in grid contexts, but now are prevalent in the cloud [vLAV05, DPJX12].

In regards to a historical perspective, trust in computer science can be traced back to 1979 in early works of Nibaldi on trusted computer systems at MITRE [Nib79]. In a way, humanity always resorts to trust, existing thus a need to adopt new trust vehicles in new scenarios, in particular for a society that is increasingly dependent on digital media. In fact, as interactions migrate to a new medium, new cues and methodologies must be developed to provide trust within the new reality. In virtual reality of VW/MMOGs, there are only a few contributions targeted on trust [RCS⁺10]. These contributions are mostly focused on entities and issues like infrastructures (e.g., hardware and software), networking, load balancing, world state consistency, data replication control, digital rights management (DRM) [ZPMY09], privacy, etc., and not that much of users/avatars and their behavior in the immersive world. However, a few works have approached the concepts of fairness [CLPC08], reputation [HHJ08], recommendation [HSRF95] as data sources or vehicles for in-world trust management in MMOGs, as well as for user behavior profiling [SM12b] and in-world governance [Hum08]. But, we find also works of the same sort in online services [Gol09, Tav12] and social networks [Bhu10, ZXL⁺12].

Fairness systems (if they even will exist in the future), reputation systems and recommendation systems are here seen as producers of data for trust systems. That is, trust systems are data consumers. A trust system is built on some trust model; examples of trust models are the following: Travos [TPJL06], Regret [SS01] and TNA-SL [JHP06]. But, the seminal work of Marsh [Mar94] remains as one of the most significant contributions towards the formalization of trust as a computational concept. Note that we are interested in approaching trust inside virtual worlds, and the same applies to fairness, reputation, recommendation, and other types of judgments and opinions that result from human-like interactions. As observed by Ratan [RCS⁺10], MMOG players tend to interact with those having good looking, to fear high rank players and gold farmers, and also to consider their in-game friends and guild members more reliable than others, with whom they tend to use voice channels more frequently.

Summing up, although there are significant contributions addressing trust in many domains, only a few of them deal with trust in VW/MMOGs. We intend thus to bridge this gap in VW/MMOGs by means of a trust framework proposal we outline in this chapter.

4.3 Multi-user Virtual Environments

VW/MMOGs are a special type of environment that allows multiple and simultaneous users/avatars to interact in a virtual world [DC07]. VW/MMOGs provide a set of features that empower users as seen in SecondLife [MMG⁺08]. In VW/MMOGs, users involve themselves in the development of the virtual world instead of just using it [Bel08]. These virtual building capabilities that users have created a trade market of assets using virtual currencies, so that a virtual economy ended up emerging after all [Dam08]. Then, new types of functionalities, services and activities started to appear to better customize avatars, lending them a more rich human appearance. Also virtual worlds started to be used for learning and attending virtual conferences. Trading virtual land was also made possible in the virtual economy.

4.3.1 Types of VW/MMOGs

In the literature, we find a number of types of VW/MMOGs, namely: multi-user dungeons (MUDs), massively multiplayer online games (MMOGs), virtual learning environments (VLEs), and general-purpose immersive virtual environments (IVEs). MUDs were the precursors of MMOGs. An example of a MUD is the famous Dungeons & Dragons. They are also multiplayer real-time virtual worlds, but at the time they were created it was difficult to interact with other users, unless via a text-based procedure. The World of Warcraft (WoW) is a well-known example of a MMOG. The in-world interactions take place by typing commands much like a natural language. MMOGs are more sophisticated than MUDs, in largely because they take advantage of graphics to get visual realism. A VLE is an e-learning system based on the web that mimics the conventional education system. The classes are virtual, so that teacher and students have to sign in to be granted access to the virtual world. This means that the virtual world is also a social space. IVEs, in general, take advantage of two important features: immersivity and interactivity. But immersion makes all the difference in relation to other interactive systems. Immersion into a virtual world is the perception of being physically present therein. SecondLife and OpenSimulator are two examples of general-purpose IVEs.

4.3.2 Interactions

There are many types of interaction between entities in different contexts. In this chapter, we are interested in immersive interactions when users/avatars presentially interact with each other in/and the virtual world. This is so because without interactions it is not possible to formulate an idea about trust. The sorts of interaction in VW/MMOGs have evolved substantially since the text interface of the early MUDs [Dam08, Bar03] up to the current full fleshed immersive virtual environment of virtual worlds and MMOGs like Secondlife, OpenSimulator and World of Warcraft [SM12b]. Users

interact with other individuals and their environment in many ways when they perform activities therein, among which we find:

- *Exploring*. This activity can be defined as a number of avatar movements in the virtual world, eventually leading to interactions with avatars, non-playing characters (NPCs), and the world itself.
- *Building*. Users build up items in the virtual world.
- *Socializing*. This activity describes face-to-face interactions with other users in social situations like conversation, gossip, brainstorming, etc.
- *Trading*. A commercial activity that an individual has with others.
- *Cooperation*. An activity involving a number of individuals in order to fulfill a common task.
- *Role playing*. This activity aims at earning items, prestige and virtual currency (usually found in MMOGs).
- *Fighting*. Fighting occurs against NPCs or other users in duels or in cooperation with others in guilds (usually found in MMOGs).

It is clear that these interactions are limited on what can be exchanged and with whom, in largely as in the real world. A person cannot directly interact with a huge group of people simultaneously. Analogously, as happens in the OpenSimulator, the radii of chat circles can be tuned to conversational, whisper and shout in order to determine how and which messages go to other avatars and guilds. As in real life, the amount of avatars per area unit is limited by their sizes, but also by engine constraints imposed by the processing power of computers and networking bandwidth.

4.3.3 Trustworthiness

The problem to ensure trustworthiness of an entity have several dimensions. In respect to virtual worlds, trustworthiness depends on the nature of interactions, which are either immersive or not. Trust issues related to non-immersive interactions have to do with, for example, the integrity of client side (modified client software, memory tampering, network packets manipulation) of an online game, in particular when the client software is altered by the player to get unfair advantages in the game. Mitigation solutions have been adopted by the industry by placing a controlling agent at every single user device to monitor client integrity. Another trust issue has to do with the server side, in particular when it poses the question of ensuring that game state sent in client updates wraps “trustable data”. This is very important for the trustable perception that players have about the game itself. And if this is important to client-server architectures, it must be said that it is even more important in peer-to-peer architectures, in which the users interact directly over a network without an intermediate entity as a server.

In respect to immersive interactions, trust is built incrementally based on the user experience within the immersive environment (e.g., game world), who perceives and learns from the interactions he/she establishes with other users and his/her surrounding virtual world. Immersive interactions may be assisted by a third-party or not. The third-party here is another user, a group of users (e.g., game guild), or the virtual world engine itself. Indeed, some engines provide visual cues that may be used by the user to trust/untrust in other user actions; for example, displaying enemy avatar's name in different colors is an alert to take into account, as it is also the case of delivering a emotional message to other users through the actions of his/her avatar (e.g. WoW's /mad command makes your avatar to raise its fist in anger). These actions contribute to build an image on how a player is seen by others in the game world. In a way, trust is tied to risk associated to every single user's action, which normally provokes a reaction. This action-reaction is an abstraction of what we call interaction. Trust is fundamental in interactions involving trading, cooperation to kill a monster, participation in a quest, advice from other player on how to perform or fulfill a task, and so forth, simply because user's experience and knowledge may be not enough to excel on any sort of interactions.

In fact, as suggested above, trust on someone or something may be risky. For example, the reputation systems based on user's feedback can be used to promote or demote players artificially, as it has been seen in reputation-based online services. This happens because malicious players may also complain on a player that they want to expel directly from the game or virtual world. Mimicking the reality in virtual worlds has other flavors. For example, homophily is also present in VW/MMOGs [AKW⁺11], that is, the tendency that many individuals have in identifying and associating themselves with others who are similar to them. This common identity reveals in many ways, namely: age, race, gender, dress code, social class, status, expertise and organizational role. Therefore, trust may originate from analyzing features like user avatar dress code and behavior, and also from user data made available from in-world statistics.

4.3.4 Trust Data Sources

Acquiring trust data from diverse sources existing in a virtual world is hampered by the difficulty in transposing real life trust mechanisms to any new interactive medium. VW/MMOGs present several challenges to trust representation, modeling, and management, namely:

- How to find adequate computational replacements for the traditional trust, fairness, recommendation, and reputation cues used in the physical world [JIB07].
- Which data sources to use to derive reliable measures for trust and reputation in VW/MMOGs [RCS⁺10].
- How to identify within the existing solutions, which have been proposed and validated in other knowledge areas, the ones that could be transposed and adapted to VW/MMOGs.

It is clear that cognitive and behavior data inputs extracted from our interactions in the virtual world can be used to provide a set of features susceptible to be employed in a trust model. This is the ground of current recommendation and reputation systems.

Tracking user's behavior has been used as a way to improve performance, adaptability and resilience of VW/MMOGs systems [SM12b]. But, user's behavior data can be also used to identify and trace bots [CLPC08] and gold farming users [BBC⁺08]. Other user's trust data are dependent on the model of computing. For example, in a client-server architecture, client side data includes user location, avatar's look, items and skills, while server side data comprises authentication data, logs, and so on. In a peer-to-peer architecture, the existence of trustable data is more compelling for the users because there is not central entity as a server to regulate as much as possible the data exchange between users or players.

In general, we can say that computational counterparts of fairness, recommendation, and reputation systems can also work as data sources for trust systems. Reputation systems have been used in electronic commerce and auction sites like Ebay, well as in other computer-mediated services, enabling users to forward feedback on transactions. However, these systems provide limited functionalities and its outputs can be easily tampered. In some VW/MMOGs, this sort of system is also rather limited as it simply calculates the accumulated sum of positive and negative feedbacks of users in virtual banks and auction houses. Recommendation systems are not usual in VW/MMOGs. To mitigate these problems users use complementary sources or develop add-ons and middleware solutions [BHRS09]. Fairness systems are also unusual in VW/MMOGs either, or at least are not perceived as such by users. Current approaches include profiling players from their behavior for detecting cheaters, bots and gold farmers. Usually the adopted solutions are limited to ban users. It is not accurate and could lead in many cases to false positives and unfair decisions [YK13]. Existing security and trust mechanisms are not coping with the VW/MMOGs needs [BBC⁺08, MMG⁺08]. From a business perspective the developments made in electronic transactions only thrived when the secure sockets layer (SSL) was incorporated in browsers, and in this way it was possible to assure the privacy and security of a transaction to the user, in spite of the overall medium being insecure. It also provided a way to guarantee the authenticity of the other entity by validation certificates from a certification authority (CA). These features have not been transposed to VW/MMOGs yet.

4.4 Trust framework

Let us now outline a conceptual framework for VW/MMOGs in order to address in-world trust as it is perceived by users. The novelty of the proposed framework lies not only in the trust-based interactions occurring inside a virtual world, but also in multi-dimensional trust models that help in-world users (i.e., avatars) to take decisions in specific situations. In a way, this framework is an attempt to mimic the interactions

between individuals in the real world, where we have trustors and trustees in specific circumstances. Trust is an individual manifest about trustability, while reputation is a collective manifest about trustability.

Thus, the approach we have followed in the design of our framework focuses on the user perception about the surrounding virtual world, and on his/her interactions with other in-world entities, no matter they are trustor or trustee entities. Trust will be referred as a trustor's manifest about the trustee in regards to a specific goal; for instance, "I trust him to trade!" Note that most of computational trust models do not target to be used as human aids in taking decisions; instead, they try to transpose human trust relevant features to non-human scenarios in which there is not a human direct intervention like in MAS and P2P networks or even MANETs.

The framework includes three major components: inputs, engine, and outputs (Figure 4.1). The *input* component is responsible by inputting as much as possible data (not necessarily only trust data) into the engine. This data is mainly about users/avatars' data. The *engine* via its trust kernel feeds trust model-based system with specific user's data retrieved from a database, which produces manifold trust results about a user/avatar that are then forwarded to the decision system, which in turn decides about the trustability of the user. Taken a decision, it is delivered to *output* module, being it then forwarded to the trustor avatar who takes the final decision about the trustee avatar.

4.4.1 Input

The input data is manifold and includes contextual data, external data, and user profiling data. This data is collected from different sources and stored within the VW/MMOG, what is in a way related to the variety of trust models we have embedded in the engine. Trust data can be collected from a number of sources, namely: attitudes, behaviors, and experiences. Attitudes result from the information gathered from a user's interactions like expressing a opinion about someone or entity. Behaviors correspond to observed behavioral aspects of other users. Experiences include explicit and implicit experiences; explicit experiences are direct first-hand interactions with others, while implicit experiences are those that are vehiculated through others, regardless of whether they are friends, feedback mechanisms or anything else.

The inputs considered in our framework conceptual approach are obtained from three different types of information sources, as illustrated in Figure 4.1. The first, the *contextual* sources denotes the information on user actions in specific contexts of interaction with other avatars in the virtual world. The *external* sources correspond to inputs obtained from external data sources (e.g., list of friends, trust networks, as well as inputs from reputation system if available). The *user profile* corresponds to data specific to each user in accordance to his/her own trust specifications; for instance, "I always trust others at beginning".

Engine. The trust engine comprises various systems: kernel, trust model-based system,

storage database, update system and decision system.

Kernel. The *kernel* is the central element of the trust framework (TFW). The kernel is responsible for determining which data sources and trust models are to be used in each user's trust assessment, but has also the function of collecting trust results produced by the trust model-based system and to forward them to the update and decision systems.

Update system. The *update system* is necessary because the perception about an user's trustability may change over time. A trust change in the user profile occurs when he/she interacts with another user for the first time or when his/her behavior has changed. That is, a trust change is the result of interactions between users inside the virtual world, and leads to a change in the storage database.

Storage database. The *storage database* is designed to house data for each user/avatar profile, his/her trustability, well as his/her inter-relationships and interactions within a VW/MMOG, what results in a trust graph or network.

Trust model-based system. Currently, *trust model-based system* houses the following computational models:

- *Trust Network Analysis with Subjective Logic (TNA-SL)*. This model incorporates trust networks representing the transitive trust relationships between entities (e.g., people, organizations or software agents), taking advantage of the subjective logic to calculate trust between arbitrary nodes in the trust network [JIB07], which is represented as a directed series-parallel graph (DSPG). The subjective logic generalizes binary logic and probability calculus, which includes degrees of uncertainty. In VW/MMOGs, these nodes are users/avatars and TNA-SL is used to assess trust from the existing transitive trust relationships represented by the edges of the trust graph. Interestingly, subjective logic is able to derive a level of trust between any two nodes of a trust network, even when no explicit trust paths between them exist.

- *Regret*. This model has a multidimensional perspective on trust as it aggregates three dimensions: individual based on direct interactions, social from past interactions of group members, and also a dimension represented by a hierarchical ontology structure to address different types of complex concepts [SS01]. It allows for subjectivity in trust assessments as well as a temporal-effect factor giving more relevance to recent data [MP10]. In addition, in the presence of conflicting information, it is able to still provide methods for calculating degrees of trust [AG07]. The model strengths lie in the compositional approach that successfully deal with many of the issues of trust and reputation in virtual communities [Pat07]. But, a functional update mechanism is missing [WHS11], and it does not allow anonymity as referred in [MP10]. By examining truthfulness of information, it does not distinguish between dishonest and just incompetent [Med12]. The subjectivity, flexibility, temporal effect and multidimensional characteristics present in Regret are important features to take into account in the design of the TFW for VW/MMOGs.

— *Eigentrust*. This model enables to choose peers of a P2P file-sharing network with reference to their history of reliable downloads [KSGM03] according to a PageRank [BP98] approach. Each peer is assigned a unique global trust value that accounts for the experiences of all peers with such a peer. For that purpose, each peer ranks its downloads from other peer nodes, and this information is placed in a trust matrix. The concept of transitive trust is at the core of this model; consequently, one assumes that a peer will have a high-ranked opinion of those peers from whom it has downloaded authentic files, so that such a peer is likely to trust those peers because they presumably will be honest in also reporting their local trust values. This notion of transitive trust leads to a system where global trust values of peers are related to the left principal eigenvector of a matrix of normalized local trust values. The normalization of these local trust values ensures that malicious or untrusted peers can be excluded from the trust network. In VW/MMOGs it can be used for identifying misbehaved avatars or to identify the trustworthier avatar in a specific context situation.

— *Stereotrust*. In general, trust models make usage of past behavior information of any entity that is being evaluated, but this information is not always available simply because there is not any historical information when one faces a stranger. In this case, one uses the “instinct”, which is nothing more than a number of stereotypes developed from our interactions experienced in the past with someone that looks “similar”. Therefore, Stereotrust is a computational trust model that was inspired by real life stereotypes [LDRL09]. Therefore, features like profile data, past behavior and types of interactions/transactions of a specific entity with others are used to build its own stereotype. As a generic model, Stereotrust can be easily, not to say desirably, applied in VW/MMOGs because user’s behavior in the virtual world tends to be similar to user’s behavior in the real world.

— *Trust Ant Colony System (TACS)* is a model developed in the context of P2P networks. It uses an ant (or agent) colony optimization algorithm for finding good and reliable peers. More specifically, it uses probabilistic techniques to find trust paths to trustworthier nodes in a P2P network [GMMPGS09a]. Due to the dynamics of P2P networks topology (e.g., nodes can leave or enter the network at any time) it was later improved using genetic algorithms to tune and optimize TACS working parameters. Without having prior information about the existing peers, TACS showed high accuracy in detecting the most reliable peer, although on static networks its results were only satisfactory and in highly dynamic networks, they weren’t conclusive [GMMPGS09a]. In relation to VW/MMOGs TACS can be employed to identify the most trustworthy avatar regarding a specific situation (e.g., the best content developer offering services in-world).

Summing up, the *trust model-based system* is scalable in the sense that it is designed to house more computational trust models if needed. However, for the time being, we believe that the trust models approached above are more than enough to support trust judgments of a user/avatar about any other user/avatar he/she may meet somewhere in the virtual world.

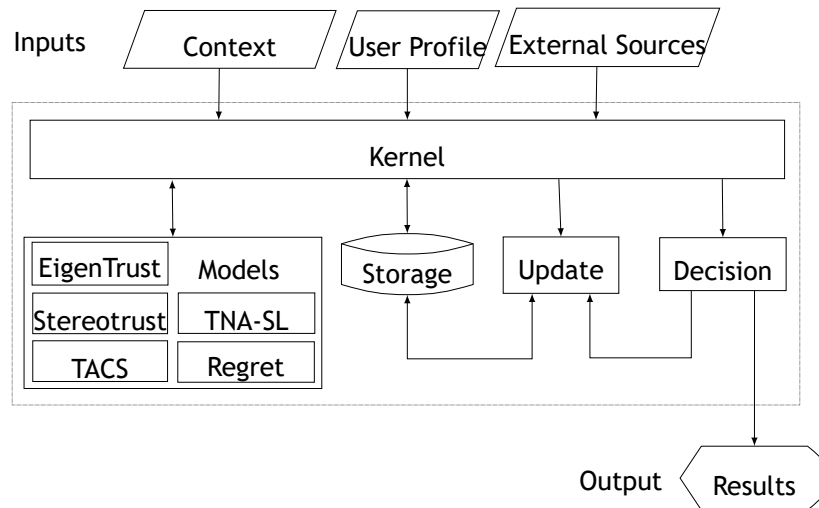


Figure 4.1: Outline of the Trust Framework (TFW).

Decision system. This is the last module of the trust framework (TFW) shown in Figure 4.1. This module is in charge of producing a computational decision about the trustworthiness of an trustee (e.g., user or avatar) based on the trustee data available in the database and on the most appropriate trust models embedded in the trust engine. This trust judgment is then forwarded to the trustor who takes a final decision about the trustee, acting then accordingly in the virtual world with the trustee. It is clear that trustor’s final decision will be also sent to the database via the kernel component in order to update the trustee profile.

4.4.2 Output

The output is the judgment produced by the trust decision system, which is forwarded to the user through the client interface. The framework output should be intuitive to users. We also intent to use the framework in real time in a preemptive constant evaluation of the avatars in avatar’s Aol (Area of Interest); for instance, if an avatar is going to an auction house, we assume that he/she has the intent of trading something, so it would be advisable to notify the auctioneers about that because a number of transactions/interactions are going to take place likely therein.

4.5 Discussion

In practice, trust in immersive worlds has not been accomplished yet, although virtual worlds present a more familiar representation to users than online services. In a way this comes from the fact that trust in VW/MMOGs cannot be evaluated from a single point of view. A trust framework for a VW/MMOG must be multidimensional and flexible enough in order to enable adjustments to the aggregated final value for trust; hence, the trust models incorporated in our TFW. For example, stereotypes of the Stereotrust

model allow for judgements on trusting someone or something without any prior data, while other models require a historical trust data as it the case of trust networks can be processed also by TNA-SL, Eigentrust and TACS, so that we end up having means to improve the global assessment.

In fact, users of VW/MMOGs do not have access to relevant information that is being generated in the VW/MMOG, preventing them from being able to judge other users before initiating any interactions with them. These limitations are overcome by users with the use of external sources (e.g., WoW Armory), or with the development of these capabilities as middleware as seen in MMOGs in [BHRS09], or with the implementation of alternative sharing data solutions like SecondLife *trustnet* (i.e., an alternative rating system) and *banlink* (i.e., a system for sharing ban list between users). On the other hand, the industry acts by banning malicious users by inducing scarcity of items and by promoting those users who participate in the development of the in-world [BL12].

Trust plays a key role because if users do not trust in the VW/MMOG capabilities to provide satisfaction fairness, security and privacy they start to flee. Unlike the current state-of-the art in VW/MMOGs, the FWT is relevant because it supports each user in his/her judgment about other users in the virtual worlds. The proposed models in the FWT present a way to represent and maintain trust data relevant to each user. An effort was made in order to have a broader representation of the available data, together with the required tools to aggregate and rate the different inputs to an overall trust value.

4.6 Summary

Trust concepts in VW/MMOGs have not been addressed in the past from a integrated perspective. In this chapter we have presented an introductory view on existing problems related to trust in VW/MMOGs. A special effort was made in order to identify trust models susceptible to be integrated in a VW/MMOGs trust framework. An effort was also made in order to analyze the adaptability of well established solutions or models to this specific scenario of VW/MMOGs. Future developments include to achieve reliable trust metrics as features for enhancing management and usage of trust mechanisms by users of these environments.

Chapter 5

Trust Representation

In virtual worlds (including computer games), users develop trust relationships from their in-world interactions with others. However, these trust relationships end up not being represented in the data structures (or databases) of such virtual worlds, though they sometimes appear associated to reputation and recommendation systems. In addition, as far as we know, the user is not provided with a personal trust tool to sustain his/her decision making while he/she interacts with other users in the virtual or game world. In order to come up with a computational formal representation of these personal trust relationships, we need to succeed in converting in-world interactions into reliable sources of trust-related data. In this chapter, we develop the required formalisms to collect, aggregate and represent in-world interactions – which are based on the activity theory –, as well as a method to convert in-world interactions into trust networks. In the chapter 6, we use these trust networks to produce a computational trust decision based on subjective logic. This solution aims at supporting in-world user (or avatar) decisions about others in the game world.

5.1 Introduction

The fact of Internet is more and more ubiquitous, with an increasingly number of users having access to broad-band networks, together with a sustainable rise in power and graphics capabilities of client compute devices has led to an increasing interest in virtual worlds (also known as multi-user virtual environments or VW/MMOGs) [Bel08, Bar03]. This is largely due to their applications in domains that are far beyond entertainment and gaming industry [DF11, BL12], including online business and commerce [MMG⁺08], research and education [BL12, DC07], military training (e.g., OLIVE) [Mac07], as well as industrial training (e.g., aircraft maintenance procedures), pilot training, and medical procedures [DF11].

Trust stems from the interactions that avatars (i.e., virtual representations of users, also called in-world users) end up setting with other avatars, places or objects. That is, trust is at the heart of all user's activities taking place within a virtual world. Similar to real life, users socialize somehow through interactions, whose trustworthiness has much to do with first impressions, opinions of others, and past experience. The grand challenge is then how to represent and operate on impressions, opinions, and user experience in virtual worlds, in order to help the user in decision-making in respect to the trust value of in-world interactions.

Trust elements can be identified in several aspects of virtual worlds. For example, in World of Warcraft (WoW), color is used to differentiate the *Alliance* from the *Hord*. The *friends list* of an in-world user (or avatar) gives also insights on the trustability and reliability of other users, as friends are considered more reliable and trustworthy than other users. Also the user-perceived behavior contributes to develop trust/distrust opinions about him/her by other users.

As noted in user behavior studies in massively multi-player online games (MMOGs) [RCS⁺10, SSM11], in-world users develop their knowledge from how they perceive the environment and from how the environment responds to their actions. The way how the user (inter)acts within the virtual world results in vast amounts of data about interactions, which are usually discarded because they are not systematically stored or are not made available to users.

The principal issue regarding trust usability (i.e., trust from user's point of view) lies in the fact that the knowledge that results from user interactions is not well represented in the virtual world, limiting so user's experience [BL12, MMG⁺08]. What we know is that part of these data is retained by the owner (or seller) company of the virtual world, which controls the management and governance of the overall virtual world platform [Hum08], mainly for user profiling and to predict user behavior. Therefore, only a small part of the data is made available to users, usually in aggregated statistics.

In other words, users are not provided with trust mechanisms in virtual worlds, what results in important constraints on the interactions that users establish with each another. For example, when a user is about to make a transaction with an unknown user (i.e., without any previous contact), the user tends to refrain from interacting with the unknown user when a relevant/important asset or goal is at stake.

To address this issue, we introduce an innovative trust approach that allows us to collect, aggregate, and represent existing trust-related data into a unifying trust model. The principal difference with other approaches is that a trust model is created for each in-world user, i.e., a user trust model that features how an individual perceives and interacts with others in the virtual world. For that purpose, current and past experiences of each in-world user contributes to enhance his/her current and future trust decisions on how interact with others. Also relevant it is the contribution that each user can bring to the overall system if his/her trust decisions were disseminated and used to enhance decisions of others, something that has not been feasible with current virtual worlds.

Thus, in this chapter, we address trust in terms of its computational representation and usability [Mar94, SS05, MMH02] in virtual worlds, taking advantage of its sociological perspective [DH08], in order to create a user-centric trust system to assist the user in his/her decision-making in respect to interactions with others. At the best knowledge of the authors, this kind of personal trust system is inexistent in the game-related literature, and far less in virtual worlds like the OpenSimulator [Lop07], which has been used in our research work.

5.1.1 Research Questions

In the present chapter, the grand challenge we are facing is to answer the following research question (Q):

Q – Assuming that interaction data are available, how can in-world users (i.e., avatars) benefit from the data generated in the virtual world to sustain their trust decisions?

To properly respond to this question, we propose a bottom-up methodology to *collect/aggregate* (first stage), *represent* (second stage) trust-related data, on which we operate to produce a *trust recommendation* (third stage) about a given in-world user. Such methodology leads us to the following subsidiary research questions:

Q1 – What kind of in-world data are available and how can they be collected?

Q2 – Can we turn in-world data gathered in the environment into a persistent computational trust representation?

Q3 – How can we derive the trust to evaluate the trustability of an avatar even when no previous direct interaction with it took place in the past?

Q4 – Can we demonstrate the validity of our proposal?

The first two questions are addressed in the present chapter, while the last two research questions concerning the trust assessment procedure and its validation will be approached in the next chapter (Chapter 6[CGF16b]).

5.1.2 Methodology

To answer to Q1, it is necessary to be aware of the resources provided by the virtual world in use. We have used the OpenSimulator [Lop07] as our virtual world, in largely because it is open-source, but more importantly because we are allowed to access to system-generated events directly. So, unlike proprietary virtual worlds like WoW (World of Warcraft), we can easily filter out those events related with avatar-avatar interactions. As explained further ahead in Section 5.3, these interactions are those in which we are interested, because they will allow us to establish trust relationships between avatars.

Regarding Q2, we can indeed turn avatar-avatar interactions into trust relationships (Section 5.4), which express positive and negative outcomes of past interactions between two avatars. A graph of avatars (i.e., nodes) and their trust relationships (i.e., edges) is thus formed into what we call trust network. Then, as described in Section 5.5, we can use the subjective logic to convert trust relationships into trust opinions [JHP06]. These trust network and opinions will be used in the next chapter (Chapter 6) to evaluate the trustability of a given avatar from a personal point of view (cf. Section 5.7).

Q3 is addressed in the chapter 6[CGF16b]. We will employ the concept of user trust

network, as the result of assembling direct trust trees (i.e., a tree per user) in order to establish a trust path between two avatars, the trustor (start node) and the trustee (goal node). After finding such trust path, we use subjective logic operators to calculate the trustability value (of the trustee) along the path connecting the trustor to the trustee, so that the trustor will act accordingly making then a decision. This is briefly approached in Section 5.7, and detailed in the next chapter [CGF16b].

Q4 is also addressed in chapter 6[CGF16b]. For that purpose, we built up various scenarios within OpenSimulator with a varying number of users and behaviors (i.e. honest, malicious, pure malicious, and sybil users), a varying number of interactions between users, as well as the impact of trust processing in the overall system performance.

5.1.3 Organization of the Chapter

The remainder of this chapter is structured as follows. In Section 5.2, we briefly review the work related to VW/MMOGs, together with trust studies carried out in other fields of knowledge. Section 5.3 characterizes the concept of interaction as the source of events from which trust-related information will be obtained. Sections 5.4-5.6 describe the process of aggregating trust relationships into trust opinions and trust networks. Section 5.7 advances with some insights on the trust inference process detailed in chapter 6. Section 5.8 puts the personal trust system in context of the research questions mentioned above, with a discussion on trust representations and operators as mechanisms of inference and reasoning. Finally, Section 5.9 draws important conclusions to bear in mind, together with some clues for future work.

5.2 Related Work

Trust has been a research topic in social sciences for a long time [Luh79, McL11]. In computing, only recently trust has attracted a lot of attention, though its roots date back to the seminal work of Marsh [Mar94], in 1994. The driving force of this interest in trust computing has been the Internet, more specifically social networks [ZKB11, SNP13, Bhu10, Gol09, CZDB11, ZDB11, CSC11].

Currently, trust pervades many fields of computing, including networking and security [CG12], critical infrastructure (CI) services [CSM⁺11], cloud computing [vLAV05, DPJX12], service virtualization [DPJX12], artificial intelligence [Mar94], human-computer interaction (HCI) [BRDM11], just to mention a few. For example, in networking, trust is employed to pre-assess nodes reliability in an attempt to ensure that there are not rogue nodes tampering data or altering its content, as observed in mobile ad hoc networks (MANETs), wireless sensor networks (WSNs) and peer-to-peer (P2P) [WE05, CSC11], not to mention the authentication procedures via certificates, public key infrastructure (PKI), and others [YWS03]. In artificial intelligence, more specifically in agents and

multi-agent systems (MAS), trust is used as a framework tool to enhance reliability in agent interactions [Mar94]. In human-computer interaction, trust plays a vital role in interactions with online services, what has to do with trust usability [BRDM11]. Yet another example is the assessment of trustability in software and hardware development, as it was identified in the industry through the Trustworthy Computing Initiative [TCG11].

Altogether, trust-related contributions have been mostly focused on addressing platform technical issues [CC13], like infrastructures (e.g., hardware and software), networking [SM12a], load balancing, world state consistency, data replication control, digital rights management (DRM) [ZPMY09], privacy, etc., and not that much on users/avatars and their behavior in the immersive world [SSM11], or the assessment of security and privacy risks in virtual worlds [BBC⁺08]. However, a few works have approached the concepts of fairness [CLPC08], reputation [HHJ08], recommendation [HSRF95] as data sources or vehicles for in-world trust management in VW/MMOGs, as well as for user behavior profiling [SM12b] and in-world governance [Hum08]. We find also works of the same sort in online services [Gol09, Tav12] and in social networks [Bhu10, SNP13]. In short, although there are many studies directly focused on trust in computing [Mar94, You07, KSGM03], only a few of them address virtual worlds and games [RCS⁺10, CG14].

In this chapter, we are interested in approaching trust in virtual worlds (including MMOGs), and the same applies to fairness, reputation, recommendation, and other types of judgments and opinions that result from human-like interactions. As observed by Ratan et al. [RCS⁺10], MMOG players tend to interact with those having good looking, to fear high rank players and gold farmers, and also to consider their in-game friends and guild members more reliable than others, with whom they tend to use voice channels more frequently. In a way, humans interact with each other developing trust/distrust relations that evolve over time, existing thus a need to adopt new trust vehicles in new scenarios, in particular for a society that is increasingly dependent on digital media.

In the following sections we intend to bridge the gap of trust in virtual worlds (including those of games) by developing a process to collect and store trust relevant information, which feeds a computational trust representation that supports in-world users (or avatars) in their decision-making processes during transactions and interactions with others. In principle, this would help in-world users to develop relationships with others, as well as to develop their own assessment and risk management capabilities.

5.3 Interactions

Interactions play a pivotal role in virtual worlds. In a way, users develop their knowledge from their interactions with and within the world, in the sense that more interactions likely mean more knowledge about the environment, objects, and other users. The interactions are conditioned by various factors, namely: user perception about the en-

vironment, user perception about the behavior of others, immersion, presence, avatar embodiment, and time. In fact, the environment looks more appealing to the user when he/she identifies himself/herself with the surrounding virtual world; the user adheres more easily to others when they belong to the same guild or member list. Immersion into virtual world has to do with a perception of being physically present therein, while presence refers to the sense of others in his/her vicinity [BCRT08]. Finally, virtual embodiment has to do with endowing an avatar (i.e., a virtual body) with the same appearance and sensations as for the user body [BCRT08, KGS12]. Also, time represents a relevant asset to assess user's commitment to virtual worlds, and also to enhance his/her knowledge about the in-world environment characteristics and the behavior of other users.

5.3.1 Activities

Within a virtual world, one may develop one or more activities over time. Trading is a sort of activity that features, for example, the selling and buying of in-world items. Other types of activities commonly found in VW/MMOGs are listed in Table 5.1. An activity involves at least an avatar; for example, the avatar's action of creating an in-world artifact is a representative of the activity of building. Also, when two guilds face themselves in a battle ground, they are developing a fighting activity; more specifically, a battle-playing activity. Furthermore, according to the activity theory [BM14], every single activity develops towards a goal. For example, in a PvP (Player vs Player) fight, the goal is to win the opponent and increase its in-world ranking/status.

In the context of virtual worlds, a (virtual) activity can be defined as follows:

Definition 1 *An **activity** denotes an exercise of a specific function by one or more avatars (or users) to achieve a specific goal (or objective) within a given time frame, being thus represented by the triple*

$$A = (s, g, t) \quad (5.1)$$

where s denotes the scope or type of activity, g the goal of the activity, and t the time frame that lasts the activity.

It is clear that distinct virtual worlds may foster different activities with specific goals and time frames. For example, WoW promotes role playing and competition, while in SecondLife socialization is a key feature.

A human agent (subject) undertakes an activity in order to solve a problem or purpose (object), being that such an activity is mediated by tools [Fre95] (artifacts) in collaboration with others (community). Note that an activity undertaken in nature by animals is typically unmediated, i.e., it is an instinct-guided activity. Even humans perform unmediated activities; for example, when an individual picks up berries in the wild and directly eats them is an activity without mediation. But, collecting a mushroom in the

Table 5.1: Types of users activities in VW/MMOGs.

Type	Description
<i>Exploring</i>	Movement of the avatar in-world.
<i>Building</i>	Create items in the virtual world.
<i>Socializing</i>	Interactions with other in-world users that resemble face-to-face human interactions.
<i>Trading</i>	Commercial activity that an in-world user has with others.
<i>Cooperation</i>	Activity involving at least two in-world users in order to achieve a goal.
<i>Role playing</i>	MMOG's activity that aims to rise the user prestige and status by earning items and virtual currency as user play a role.
<i>Fighting</i>	MMOG's activity concerning fights with non-player characters (NPCs), other users in PvP, and also fights with multiple in-world users like in battles and raids.

wild and eating it is an activity that is ill-advised without some kind of mediation, i.e., without the direct advice of an experienced mushroom forager [Lur81]. That is, many human activities, independently of whether they are real or virtual, are mediated in some extent. Mediation means *interaction* with others more experienced and with more skills in respect to a specific activity. Thus, an activity is seen as a set of interactions, each of them encompasses multiple actions that trigger in-world events as illustrated in Fig. 5.1.

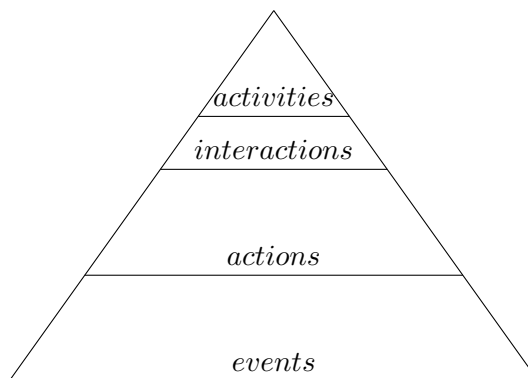


Figure 5.1: Hierarchical structure of data gathering.

5.3.2 Interactions

Informally speaking, an *action* is what an entity can do, no matter whether such entity is a human being, a machine, an agent, an avatar, etc. In turn, an *interaction* is defined as an action between two entities. In this chapter we extend this notion of interaction to a sequence of actions between two or more entities within the scope of a given activity, so that an action of the first entity usually triggers a reaction of the second entity, and vice-versa. For example, an interaction between avatars could involve multiple actions (e.g., avatar motion, behavior commands and a chat session).

In general, we classify interactions in respect to the types of interacting entities, as



Figure 5.2: Interaction process within an OpenSimulator's client window.

follows:

- *Avatar-Avatar Interaction.* This sort of interaction involves two avatars (or users); for example, two avatars are trading a single in-world virtual item (e.g., a sword).
- *Avatar-Environment Interaction.* In this case, only an avatar is involved in the interaction; for example, an avatar is opening a door to get in a building.
- *Avatar-System Interaction.* Similar to previous interaction, this interaction involves only a single avatar; for example, the avatar is interacting with a VW/MMOG reputation system in order to retrieve data about a specific user for assessing purposes. Another example is when an avatar accesses a VW/MMOG service to get a profile statistics on a user, or to make a complaint, or to report a flaw.
- *User-Service Interaction.* In this case the service is external to the VW/MMOG, so that the idea is to get additional information about other users; for example, such an information can be obtained by querying for WoW ranks in the Armory online service.

In this chapter, we are limited to in-world avatar-avatar interactions because we are approaching trust between users immersed in a VW/MMOG, not anything else.

5.3.3 Avatar-Avatar Interactions

As seen above, every single in-world interaction between two users are mediated by their avatar alter egos. As in real life interactions, we have the following:

Definition 2 An *interaction* γ_B^A between two avatars, A and B , can be represented as

follows:

$$\Upsilon_B^A = (i, s, g, t, r, d, o) \quad (5.2)$$

where i stands for the identifier of the interaction, s the scope of the interaction, also called activity (e.g., a trading activity), g the goal to achieve to fulfill with the interaction, t the timeline of the interaction, r the risk associated with the interaction (e.g., “I would lend him my special sword during a ride event in WoW in the expectation that he will return it to me”), d the decay factor associated to the interaction (i.e., the importance or strength of an interaction decays over time), and o the interaction outcome as seen by each interacting user.

The interaction outcome takes on a binary value, 0 (unsuccessful) or 1 (successful), and is thus similar to the ‘like’ system used in social networks. This interaction outcome is of paramount importance as input for the subjective logic-based trust network to be approached in Section 5.5. As shown in Section 5.4 onwards, from the 7-tuple representation (5.2) for avatar-avatar interactions, we are able to derive the trustworthiness of any user from the point of view of his/her interacting partner.

```

00 --- A starts the interaction
01 --- A seeks others in her vicinity
02 --- A starts a chat, asking others for the item x
03 --- B replies positively, but only trades x for z
04 --- C also replies positively for sharing x
05 --- A sends a IM to C asking for x
06 --- C replies saying she will drop x for sharing
07 --- A moves towards C
08 --- C drops the item x
09 --- A picks up the item x
10 --- A thanks C in the chat
11 --- A ends the in-world interaction
12 --- A rates the interaction with C
13 --- A stores the interaction with C
14 --- A ends the interaction
    
```

Figure 5.3: Actions performed within an interaction between A , B , and C (cf. Fig. 5.4 for the corresponding action types).

Example 1 A in-world scenario involving three avatars is shown in Fig. 5.2, where an avatar A (Anna) interacts with B (Beth) and C (Charlotte) in her Aol (area of influence). The avatar A intends to obtain a special item x for her inventory. To achieve that goal, A starts an interaction with B and C who are nearby. This interaction between A , B , and C comprises the actions shown in Fig. 5.3. In this interaction scenario, A ends up obtaining the item x from C in the context of a trading activity.

As illustrated in Fig. 5.4, this avatar-avatar interaction involved a number of actions over time, namely: *movement/seeking*, *chat*, *instant messaging*, *drop* and *pick* from inventory. As a result, the state of A (and also of C) has changed.

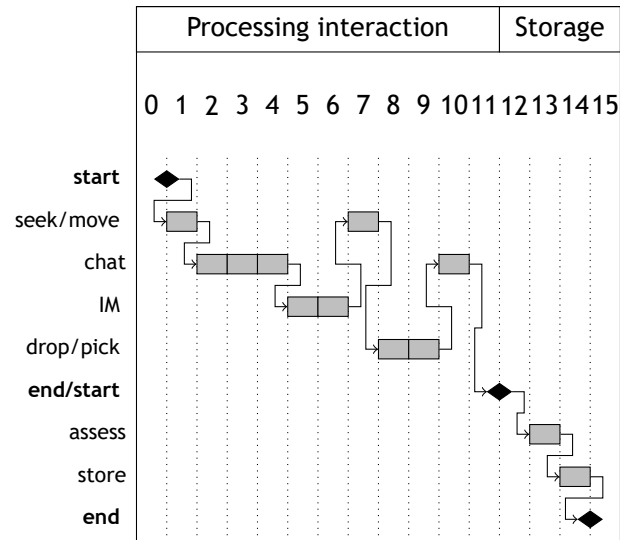


Figure 5.4: Action types of the interaction between A , B , and C over time illustrated in Fig. 5.3.




5.3.4 Actions and Events

An avatar's action takes place when the user types in keyboard or moves the mouse of his/her compute device (e.g., laptop or smartphone). Thus, avatar's actions have to do with user inputs. The OpenSimulator translates the keyboard and mouse inputs of the user into actions of the respective avatar.

Definition 3 An *action* \mathbf{a} of an avatar A is a process of doing something with a specific aim, and is characterized by the following tuple representation

$$\mathbf{a} = (id, A, t, \alpha, i) \quad (5.3)$$

where id is the identifier of the action \mathbf{a} , t stands for the time of the occurrence of the action, α denotes the action type, and i the type of input employed in the action.

Fig. 5.5 shows different types of actions (α) commonly found in virtual worlds when avatars interact with each other on behalf of their users. Note that each type of action is associated to a few input devices (keyboard , mouse , and microphone .

Events describe the state changes caused by avatar actions [HSS⁺12, Heg13]. Therefore, an action triggers one or more events.

Definition 4 An *event* is an occurrence of an action.

That is, an event is an identifiable occurrence that something has happened within the VW/MMOG. The VW/MMOG engine global state is managed through events. In OpenSimulator, these events are employed in multiple areas of the platform architecture and services, as illustrated in Fig. 5.6. Table 5.2 lists the events concerning the actions of the interaction between the avatars A , B , and C in Figs. 5.3-5.4. Accessing events of a VW/MMOG like OpenSimulator is made possible because it is open source [Lop07, HMB03]. Some events are triggered automatically by OpenSimulator platform

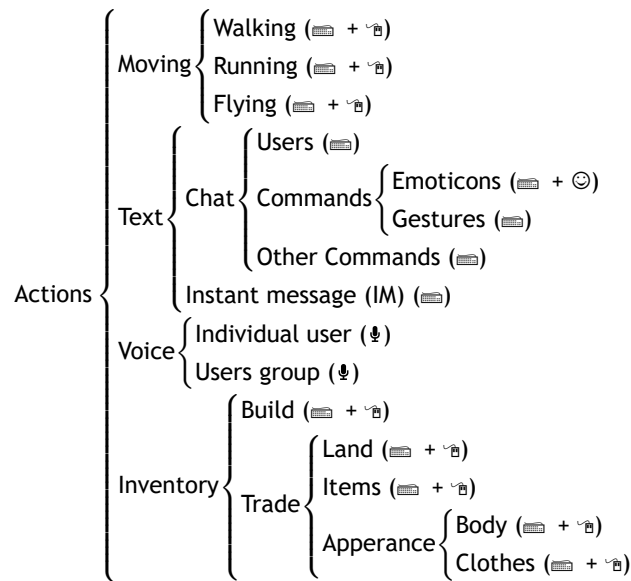


Figure 5.5: Classification of avatar actions.

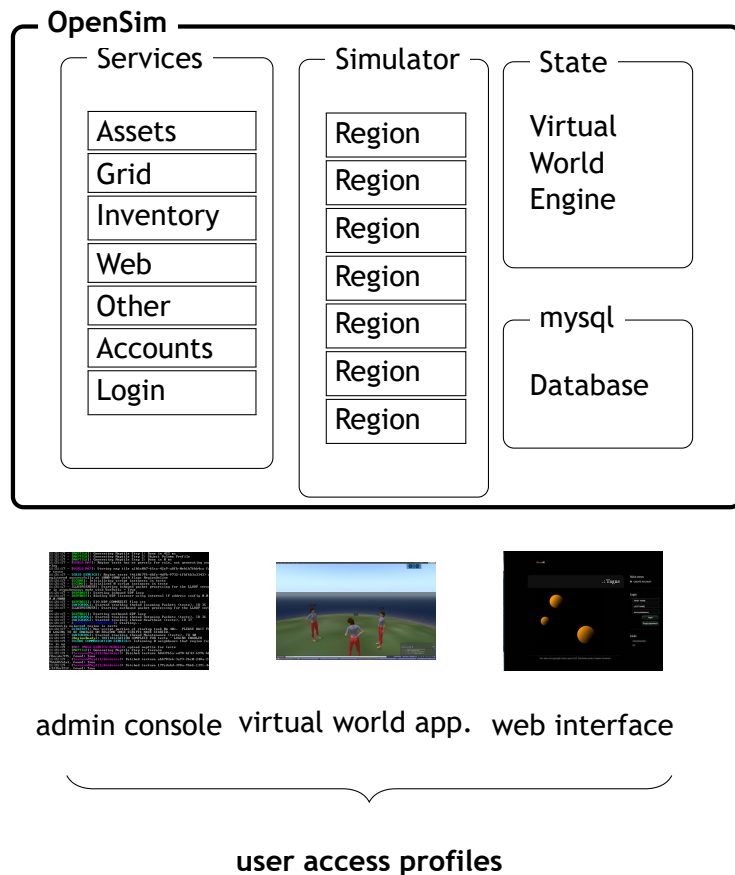


Figure 5.6: OpenSimulator architecture and services.

server when a preset condition or conditions occur, while others are initiated from the client side.

Typically, a message is issued either from user-generated events (e.g., keystrokes and mouse clicks, among others), in-world events triggered from interactions (e.g., a door

opens in response to avatar movement), or even system events (e.g., lack of memory). As already suggested, we are only interested in in-world events triggered from avatar-avatar interactions, because these interactions are the ones from which avatars develop the feeling of trust in others.

Table 5.2: Deployed Events.

Id	Events
00	<i>A starts the interaction</i> <pre>public UserEvent(UUID userId, string userName, string eventType, string gridId, string regionName, DateTime datetime)</pre>
01	<i>A seeks others in her vicinity</i> <pre>public void TriggerOnClientMovement(ScenePresence avatar)</pre>
02	<i>A starts a chat, asking others for the item x</i> <pre>public UserChatEvent(UUID userId, string userName, Vector3 origin, ChatTypeEnum chatType, string text, int channel, string gridId, string regionName, DateTime datetime): base(userId, userName, "chat", gridId, regionName, datetime)</pre>
03	<i>B replies positively, but only trades x for z</i> <pre>public UserChatEvent(UUID userId, string userName, Vector3 origin, ChatTypeEnum chatType, string text, int channel, string gridId, string regionName, DateTime datetime): base(userId, userName, "chat", gridId, regionName, datetime)</pre>
04	<i>C also replies positively for sharing x</i> <pre>public UserChatEvent(UUID userId, string userName, Vector3 origin, ChatTypeEnum chatType, string text, int channel, string gridId, string regionName, DateTime datetime)</pre>
05	<i>A sends a IM to C asking for x</i> <pre>public UserImEvent(UUID userId, string userName, UUID receiverId, string receiverName, bool isReceiverGroup, string text, string gridId, string regionName)</pre>
06	<i>C replies saying she will drop x for sharing</i> <pre>public UserImEvent(UUID userId, string userName, UUID receiverId, string receiverName, bool isReceiverGroup, string text, string gridId, string regionName)</pre>
07	<i>A moves towards C</i> <pre>public void TriggerOnClientMovement(ScenePresence avatar)</pre>
08	<i>C drops the item x</i> <pre>public void TriggerOnNewInventoryItemUpdate(UUID agentID, UUID AssetID, int userlevel)</pre>
09	<i>A picks up the item x</i> <pre>public void TriggerObjectGrab(uint localID, uint originalID, Vector3 offsetPos, IClientAPI remoteClient, SurfaceTouchEventArgs surfaceArgs) public void TriggerOnNewInventoryItemUploadComplete (UUID agentID, UUID AssetID, String AssetName, int userlevel)</pre>
10	<i>A thanks C in the chat</i> <pre>public UserChatEvent(UUID userId, string userName, Vector3 origin, ChatTypeEnum chatType, string text, int channel, string gridId, string regionName, DateTime datetime)</pre>
11	<i>A ends the in-world interaction with C</i> <pre>public UserEvent(UUID userId, string userName, string eventType, string gridId, string regionName, DateTime datetime)</pre>
12	<i>A rates the interaction with C</i> <p>Loads $P(u_A)$; $\alpha=1$;</p>
13	<i>A stores the interaction with C</i> <pre>\$insertquery = insert into interactions(i, trustor, trustee, s, g, t, r, d, o) values (2341,'A','C','trade','obtain item',2014-04-27 12:44:40 168, 'low',0.5,1);</pre>
14	<i>A ends the interaction</i> <pre>public UserEvent(UUID userId, string userName, string eventType, string gridId, string regionName, DateTime datetime)</pre>

5.3.5 Collecting Interaction Data from Events

Events are registered and handled through the *EventManager* of OpenSimulator. The pre-defined events of OpenSimulator have a global (the entire world), regional (a world region), or local (a scene or avatar's area of interest) coverage.

The avatar-avatar interactions taking place within OpenSimulator fires off events. To illustrate a type of events considered in the interaction we describe instant messaging (IM) events in OpenSimulator's format as follows:

$$\varepsilon_B^A = (i_A, n_A, i_B, n_B, b, m, G, R, t) \quad (5.4)$$

where i_A and n_A stand for the id and name of the trustor A (who sends the message), i_B and n_B are the id and name of the trustee B (who receives the message), b is a boolean flag that indicates whether the receiver is a group or not, m is the text message, G the virtual world grid identifier, R the virtual world region identifier, and t the time of the occurrence.

In fact, OpenSimulator is here used for avatar behavior analysis, in which chat sessions and IM events serve the purpose of tracking user behaviors [ORMCB12]. For example, as the interaction activity develops, the actions performed by the participant avatars described in Fig. 5.3 trigger the events described in Table 5.2. Initially, the event *ClientMovement* was triggered (action 01) when A started the interaction. Next, the event *UserChatEvent* was generated (action 02) when A opened the chat window. It is clear that subsequent actions continued to generate other events. The collected events are those associated with the chat and IM actions, movement and picking objects, as well as those associated to inventory state updates. The interaction is concluded when A rates C , and the interaction γ_C^A (cf. Eq. (5.2)) is stored in OpenSimulator's MySQL database as an entry $(i, \text{trustor}, \text{trustee}, s, g, t, r, d, o)$ of the interactions table. For additional details on OpenSimulator events and storage formats, the reader is referred to [Lop07].

Automatic gathering Interactions between avatars usually occur when they are within reach of one another, i.e. when an avatar crosses the Aol of another avatar. In order to automate the data gathering process, the decision taken to start and end each avatar-avatar interaction is based on events that detect when an avatar enters or leaves the Aol of another avatar. For example, we have five avatars A, B, C, D and E in Fig. 5.7, where the Aol of A is structured into three concentric circles: *shout* (outer circle in light green), *speak* (middle circle in green), and *whisper* (inner circle in dark green); the remaining avatars appear depicted with their Aol's speak circles. Fig. 5.7 shows four speak interactions, namely: γ_B^A and γ_C^A because B and C get in the Aol of A , γ_A^B because A gets in the Aol of B , and γ_A^C because A gets in the Aol of C . Also, Fig. 5.7

exhibits the shout interaction γ_E^A because E is in the Aol of A .

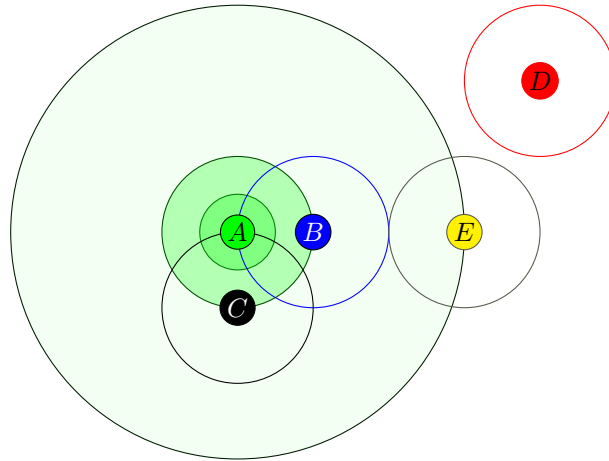


Figure 5.7: A records an interaction with B and another interaction with C , and vice-versa, because B and C are inside the Aol of A .

Rating process Every single avatar-avatar interaction is rated as either positive or negative automatically. The key features relevant for an avatar to automatically rate his/her interaction with another avatar are the following:

- Member of *friends list*.
- Amount of time within the Aol.
- Number of chat messages.
- Number of words/expressions employed within the chat considered offensive (e.g., compared with a list of bad expression/words from the user).
- Number of words/expressions employed within the chat considered helpful and kind (e.g., compared with a list of good expression/words from the user).
- Number of IM messages exchanged (sent and replied by the trustor avatar).
- Change on the number of items in the *inventory*.
- Voice communication.
- Gathering in-world statistical information about the avatar.
- Adding the avatar to user friends list.
- Adding avatar to the avatar blocking list.
- Social distance (e.g., time within *whisper* Aol).
- Avatar dress code (e.g. if similar to mine it is more trustworthy).
- In-world cues (e.g., like race or guild identifiers in WoW).
- Avatar behavior (e.g., gestures like dance).
- Avatar address directly in the chat.

- It dropped an item (e.g., that I picked).
- Location (e.g., if avatar is in a dungeon it is likely to be hostile, in opposition if it is within its home location.)
- Access user statistics (e.g., amount of time connected, ranking).

For example, if the avatar is added to the user blocking list of the first avatar, then such a membership feature is rated as negative; otherwise it is rated as positive. The rating is done for all the features automatically. Note that the type and amount of rateable features are susceptible of being set up or changed by each user. Therefore, the process by which each feature is rated is subjective and susceptible to be tuned by each user.

Interaction aggregation The interaction aggregation mechanism proposed is based on a two-layer approach. All features are aggregated and averaged by type, after which the different collections of features are rated by relevance according to the user parameterizations. The resulting rate value is then compared with a predefined threshold in order to determine the outcome of the interaction as either positive or negative (cf. event 12 in Table 5.2).

As illustrated in Algorithm 1, the process of collecting interaction data is initiated by the loading of user preferences (e.g., the events and activities to track) $P(u_A)$ of the trustor u_A from the database. Then, if an event ε involves the trustor u_A and the trustee u_B , we have then to check whether the scope s of the activity is in the preferences of u_A , setting then the remaining parameters of the interaction, including the assessment outcome o of the trustor about the trustee.

5.4 Trust Relationships

In the previous section, we have seen how to gather and aggregate actions/events into in-world interactions. We intend now to show how to generate trust relationships from such interactions. As much as we know, this trust inference from interactions has not been tried and achieved before, in particular in online games and virtual worlds. Nevertheless, this inference mechanism may be also applicable to social networks, P2P networks, online services like auction sites because they have commonalities with online games and virtual worlds, in particular as socialization spaces [DIG13, SNP13].

5.4.1 Trust Relationships

In general terms, a trust relationship between two avatars, a trustor (A) and a trustee (B), is formulated from the set of past interactions between them, which are maintained in some database. More formally, we have the following definition:

Algorithm 1: Collecting data into interactions.

Data:

u_A : in-world user id for truster (sender)
 u_B : in-world user id for trustee (receiver)
 s : scope of the activity
 o : assessment outcome of the truster about trustee

Result:

$\Upsilon_B^A(i, s, g, t, r, d, o)$: interaction

```

1 begin
2   Load preferences  $P(u_A)$  from database;
   /* automatic gathering */
3   begin
4     while  $u_B$  in  $u_A$  Aol do
5       Read and store event  $\varepsilon_i$  in  $u_A$  Aol;
6        $i \leftarrow i + 1$ ;
   /* rating process */
7   begin
8     for all  $\varepsilon_i$  do
9       Rate of the collect data  $\varepsilon_i$  based on the  $feature_j$  detected;
10       $i \leftarrow i + 1$ ;
11       $j \leftarrow j + 1$ ;
12      return  $rate(i, j)_B^A$ ;
   /* aggregate ratings by feature and by relevance */
13  begin
14    for all  $j$  do
15      for all  $i$  do
16         $sumrate(j) = rate(i, j)_B^A$ ;
17         $i \leftarrow i + 1$ ;
18        return  $sumrate(j)_B^A$ ;
19         $j \leftarrow j + 1$ ;
20        return  $sumrate_B^A$ ;
   /* calculating interaction outcome */
21  begin
22    Calculate  $o$  from  $sumrate(j)_B^A$  ponderation;
23    if  $o > preset - threshold$  then
24       $o = 1$ ;
25    else
26       $o = 0$ ;
   /* storing interaction */
27  begin
28     $A = u_A$ ;
29     $B = u_B$ ;
30     $s(\Upsilon_B^A) = s$ ;
31     $t(\Upsilon_B^A) = now$ ;
32     $i(\Upsilon_B^A) = i(\Upsilon_B^A) + 1$ ;
33     $g(\Upsilon_B^A) = g(P(u_A))$ ;
34     $d(\Upsilon_B^A) = d(P(u_A))$ ;
35     $o(\Upsilon_B^A) = o$ ;
36    Store  $\Upsilon_B^A(i, s, g, t, r, d, o)$  in database;

```

Definition 5 A *trust relationship* Γ_B^A between two avatars, A (trustor) and B (trustee) is given by

$$\Gamma_B^A = (i, s, g, t, r, d, a, p, n) \quad (5.5)$$

where, i stands for its id, s the scope of the activity, g the goal to be achieved, t the time instant of the assessment of A about B , r the risk for the trustor, d the decay factor over time, a the base rate obtained from trustor parameterizations $P(u_A)$, p is the sum of positive outcomes (i.e., $o = 1$) of past interactions, and n is the sum of negative outcomes (i.e., $o = 0$) of past interactions of A with B .

In the present implementation, we opted not to include the risk r and the decay factor d in the computations of the trust relationships for simplicity sake. Therefore, all interactions share the same risk and the same relevance. Otherwise, we would have to give more or less relevance to the outcome o of each interaction, depending on the risk r is lower or higher, respectively. The fact that we do not use the decay factor d in our computations means that we are not discarding any interactions behind in time (e.g., interactions that occurred 5 days ago or more). This also means that we are not considering when such interactions occurred in the past; as a consequence, if the time of occurrence of any interaction were considered, the decay d would allow us to reinforce recent interactions in detriment of old interactions. Therefore, we end up using the following simplified version trust relationship:

Definition 6 A *simplified trust relationship* Γ_B^A between two avatars, A (trustor) and B (trustee) is given by

$$\Gamma_B^A = (i, a, p, n) \quad (5.6)$$

where, i represents its id, a the base rate obtained from trustor parameterizations $P(u_A)$, p is the sum of positive outcomes (i.e., $o = 1$) of past interactions, and n is the sum of negative outcomes (i.e., $o = 0$) of past interactions of A with B .

As illustrated in Algorithm 2, in-world trust relationships (Γ) are build from stored interactions. Therefore, representing a trust relationship between A and B within a scope or activity requires the aggregation of positive (p) and negative (n) interactions between A and B in the vector o of outcomes (cf. Eq. (5.2)).

5.4.2 Plain Trust Networks

The trust relationship Γ_B^A denotes how much A trusts in B , while the trust relationship Γ_A^B denotes how much B trusts in A . Therefore, trust relationships essentially are unidirectional. This means that a trust network can be conceptualized as directed graph (or digraph) as follows:

Definition 7 A *plain trust network* \top of a virtual world is a directed graph (\mathbf{A}, Γ) ,

Algorithm 2: Creating and storing trust relationships (Γ).

Data:
 u_A : in-world user id for truster (sender)

 u_B : in-world user id for trustee (receiver)

 s : scope of the activity

 $\Upsilon_B^A(i, s, g, t, r, d, o)$: data from A interaction with B
Result:
 Γ_B^A : trust relationship of A with B

```

1 begin
2   Load  $s$ ;
3   while  $\Upsilon_B^A(i)$  exist do
4     if  $o(\Upsilon_B^A(i)) = 1$  then
5        $p(\Gamma_B^A) = p + 1$ ;
6     if  $o(\Upsilon_B^A(i)) = 0$  then
7        $n(\Gamma_B^A) = n + 1$ ;
8     adjust  $\Gamma_B^A(i, a, p, n)$  with decay  $d$ ;
9     adjust  $\Gamma_B^A(i, a, p, n)$  with risk  $r$ ;
10     $i++$ ;
11  store  $\Gamma_B^A$ ;
    
```

where $\mathbf{A} = \{A_1, \dots, A_n\}$ stands for the set of avatars (or nodes), and $\Gamma = \{\Gamma_1, \dots, \Gamma_m\}$ the set of trust relationships (or directed edges) established between avatars in the virtual world.

Recall that we are only considering trust relationships associated to avatar-avatar interactions, though other types of trust could be used if necessary. Besides, we are assuming that such interactions occur within the same scope s , but we also might consider other scopes in the assessment of trust of a given avatar by other avatar.

5.4.3 A Case Study Example

As seen above, a plain trust network essentially is a network of avatars, whose avatar-avatar interactions are enhanced with trust data. Thus, the generation of a plain trust network is straightforward from avatar-avatar interactions and their trust relationships. An example of a plain trust network is shown in Fig. 5.8, where we have 7 avatars (nodes) and 18 trust relationships (directed edges).

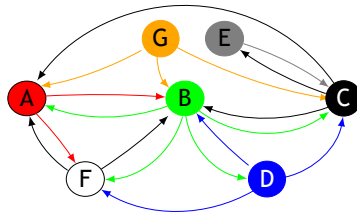


Figure 5.8: A plain trust network \mathbb{T} concerning 7 avatars interacting within an OpenSimulator region.

The trust network (\mathbb{T}) in Fig. 5.8 was built up from the aggregation of the individual trust networks(\mathbb{T}_i) of the seven avatars present regarding the same specific scope and represented as: $\mathbb{T}_i^A = \{B, F\}$, $\mathbb{T}_i^B = \{A, C, D, F\}$, $\mathbb{T}_i^C = \{A, B, E\}$, $\mathbb{T}_i^D = \{B, C, F\}$, $\mathbb{T}_i^E = \{C\}$, $\mathbb{T}_i^F = \{A, B\}$ and $\mathbb{T}_i^G = \{A, B, C\}$. Note that an individual trust network (\mathbb{T}_i) represents the direct interactions of a single avatar with others, as illustrated in Fig. 5.9. For the sake of trust reasoning, later approached in the context of subjective

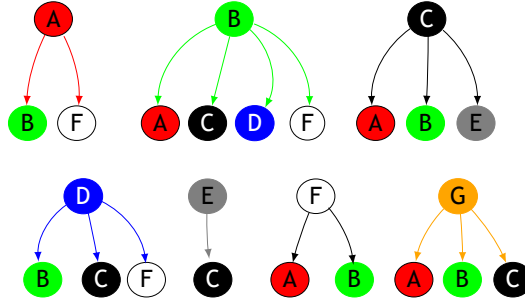


Figure 5.9: Individual trust networks (\mathbb{T}_i) of 7 avatars interacting in a game scenario.

logic, the trust network digraph in Fig. 5.8 can be represented in the matrix form as follows:

$$\mathbb{T} = \begin{matrix} & \text{users} & A & B & C & D & E & F & G \\ \begin{matrix} A \\ B \\ C \\ D \\ E \\ F \\ G \end{matrix} & & \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (5.7)$$

The matrix \mathbb{T} represents the 49 (7x7) possible trust relationships of the scenario, but only 18 correspond to existent interaction relationships; in particular, ‘1’ denotes the existence of interaction relationships, while ‘0’ indicates the inexistence of interaction relationships.

However, the matrix \mathbb{T} does not incorporate the trust relationships \mathbb{T}_i explicitly, but only their existence. To do so, we collect their aggregated outcomes $\mathcal{Y}(o)$ from previous interactions as positive p and negative n , replacing each entry ‘1’ by the corresponding

vector of outcomes as follows:

$$\mathbb{T} = \begin{array}{c} \text{users} \\ \begin{array}{c} A \\ B \\ C \\ D \\ E \\ F \\ G \end{array} \end{array} \begin{bmatrix} A & B & C & D & E & F & G \\ 0 & \begin{bmatrix} 12 \\ 1 \end{bmatrix} & 0 & 0 & 0 & \begin{bmatrix} 7 \\ 3 \end{bmatrix} & 0 \\ \begin{bmatrix} 6 \\ 2 \end{bmatrix} & 0 & \begin{bmatrix} 1 \\ 4 \end{bmatrix} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} & 0 & \begin{bmatrix} 13 \\ 1 \end{bmatrix} & 0 \\ \begin{bmatrix} 5 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & 0 & 0 & \begin{bmatrix} 3 \\ 1 \end{bmatrix} & 0 & 0 \\ 0 & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & 0 & 0 & \begin{bmatrix} 3 \\ 2 \end{bmatrix} & 0 \\ 0 & 0 & \begin{bmatrix} 4 \\ 1 \end{bmatrix} & 0 & 0 & 0 & 0 \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 2 \end{bmatrix} & 0 & 0 & 0 & 0 & 0 \\ \begin{bmatrix} 3 \\ 0 \end{bmatrix} & \begin{bmatrix} 8 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5.8)$$

For example, the trust relationship Γ_B^A is a result of 13 previous interactions between A and B , twelve of which were positive ($p = 12$) and one was negative ($n = 1$); another example is Γ_F^D , which consists of 3 positive interactions and 2 negative interactions. Altogether, we count 89 interactions in this plain trust network involving 7 avatars acting within an in-world region of OpenSimulator.

Of course, the plain trust matrix \mathbb{T} is not enough for an avatar to formulate a trust opinion about another avatar while they do not interact with one another. In order to formulate such opinion at first sight, i.e., before any interaction, we need to use some kind of logical inference. In this chapter and in chapter 6, we use the subjective logic as our opinion engine.

In the context of online games, a trust network can be defined as a plain trust network (cf. Definition 7) whose connections (or edges) are endowed with trust opinions, that is, a directed graph of avatars whose edges denote the opinions (and their underlying trust relationships) they establish with each other.

5.5 Trust Opinions

Our opinions on others are subjective in some way, and this is determined by the human condition itself. That is, an opinion is a belief built on trust, but not sustained on any proof. The subjective logic is particularly adequate for modeling and analyzing situations involving uncertainty and incomplete knowledge. In these circumstances, subjective logic can be seen as a probabilistic logic for uncertain probabilities.

In this chapter, we will use a model of subjective logic, here called subjective algebra, which consists of a pair of opinions and subjective operators. For the time being, we are only interested in the representation of trust opinions across trust networks. In respect to subjective operators, which are necessary for reasoning and inference, they will be approached in the next chapter (Chapter 6; see [CGF16b] for further details).

5.5.1 Opinions and Subjective Logic

In order to build up a *trust opinion network* (or, simply, a *trust network*) for avatars within the game world, we first need to convert trust relationships into trust opinions (or, simply, opinions). This conversion is accomplished using subjective logic [JHP06, Jøs13].

In subjective logic, the notion of opinion is as follows:

Definition 8 Let x be a proposition. An **opinion** ω_x^A of the belief owner A about the proposition x is denoted by an ordered quadruple

$$\omega_x^A = (b, d, u, a) \quad (5.9)$$

where $b, d, u, a \in [0, 1]$ stand for *belief* (belief that x is true), *disbelief* (belief that x is false), and *uncertainty* (the amount of uncommitted belief), respectively, such that $b + d + u = 1$, while a is the *base rate* defined as the *a priori* probability in the absence of evidence.

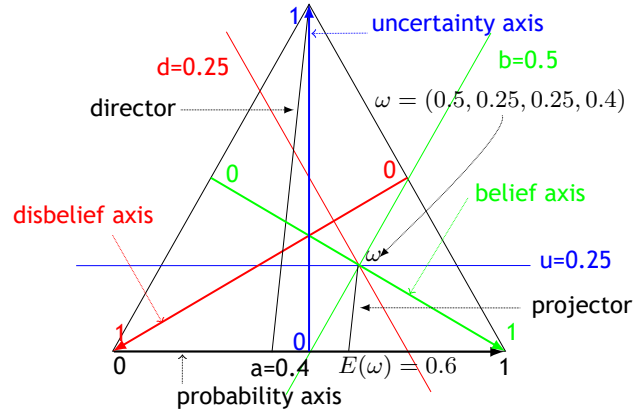


Figure 5.10: Example of the representation of a trust opinion in the subjective logic space triangle.

From the previous definition of opinion, we can state that the variables b , d , and u define a barycentric coordinate system, in which the location of a point is specified as the center of mass (or barycenter) of the values of b , d , and u (see Fig. 5.10), so that the **certainty** c of a proposition x can be formulated as follows:

$$c = (1 - u) = (b + d) \quad (5.10)$$

This means that the opinion space is an equilateral triangle. Equivalently, an opinion is represented by a point of such triangle, which is specified as the center of mass (or barycenter) of the values of b , d , and $u \in [0, 1]$ (see Fig. 5.10). For example, the

opinion $w = (0.5, 0.25, 0.25, 0.4)$ is found as the point of intersection between the lines perpendicular to axes at $b = 0.5$, $d = 0.25$, and $u = 0.25$. Note that each axis is perpendicular to each triangle side. As said before, the fourth component a of an opinion stands for the a priori probability (or a priori trust) assigned to any individual of a given community. The value of a in the probability axis (i.e., bottom side of the triangle) and the top vertex u of the triangle define a director line. This director line is important because it allows us to compute the opinion's probability expectation value as follows:

$$E(\omega_x^A) = b + a u \quad (5.11)$$

which is the result of the projection of the opinion point onto the probability axis along a line parallel to the director line.

Similar to Kleene logic [Fit91], the subjective logic is a three-valued logic [JHP06, Jøs13]. However, Kleene logic lacks from the concept of base rate, so that probability expectation values can not be determined at all. Additionally, depending on the values of b, d, u , we end up having distinct classes of opinions as follows:

- *Class of True Opinions.* In this case, we have opinions with $b = 1$, being this equivalent to the binary logic 'true'.
- *Class of False Opinions.* In this case, we have opinions with $d = 1$, being this equivalent to the binary logic 'false'.
- *Class of Certain Opinions.* In this case, we have opinions with $u = 0$ or, equivalently, $b + d = 1$, being this equivalent to the traditional probability.
- *Class of Uncertain Opinions.* In this case, we have opinions with $u \in]0, 1[$ or, equivalently, $b + d < 1$, opinions with some degree of uncertainty.
- *Class of Totally Uncertain Opinions.* In this case, we have opinions with $u = 1$ or, equivalently, $b + d = 0$, being this equivalent to total uncertainty.

In a way, subjective logic generalizes the standard logic because part of the propositions are considered to be either true or false. Also, subjective logic constitutes a generalization of the probabilistic logic because the propositions can be expressed as a probability in the range $[0, 1]$. But, more than that, it is fact the subjective logic makes it possible to express propositions with uncertainty. Remarkably, as shown later, this allows us to formulate an opinion about someone who we never found before.

In the context of trust computing, the proposition x mentioned above in the context of subjective logic synthesized as " A trusts on B ", that is, the belief owner A is the trustor, and B is the trustee. Therefore, apart the abuse of language, we can express ω_B^A as a trust opinion of A on B . In these circumstances, the value of c given by Eq. (5.10) denotes the **confidence degree** of a trust opinion ω_B^A . On the other hand, the value of $E(\omega_B^A)$ given by Eq. (5.11) denotes the **trust predicted value** (i.e., the probability

expected value) of a trust opinion ω_B^A , that is, it represents trustability as a quantifiable value.

5.5.2 Trust Relationship-Opinion Conversion

Converting a trust relationship (i.e., a set of avatar-avatar interactions) Γ_B^A into an opinion ω_B^A involves two steps. First, we express the probability density over the space of binary outcomes (i.e. positive p and negative n) resulting from avatar-avatar interactions as beta probability density functions, which are denoted by $\text{Beta}(\alpha, \beta)$. Recall that a beta distribution is a family of continuous probability distributions defined on the interval $[0, 1]$, which are parametrized by two positive shape parameters, denoted by α and β . Let p and n stand for the number of positive and negative past interactions of A with B , and let a express the a priori or base rate, then α and β can be determined as follows:

$$\alpha = p + 2a \quad \text{and} \quad \beta = n + 2(1 - a) \quad (5.12)$$

Second, by using the bijective mapping between the opinion parameters and the beta parameters [JHP06, Jøs13], we can express the opinion parameters in terms of positive and negative past interactions of A with B , and vice-versa as follows:

$$\begin{cases} b = \frac{p}{p+n+2} \\ d = \frac{n}{p+n+2} \\ u = \frac{2}{p+n+2} \\ a = \text{base rate of } x \end{cases} \Leftrightarrow \begin{cases} p = \frac{2b}{u} \\ n = \frac{2d}{u} \\ 1 = b + d + u \\ a = \text{base rate of } x \end{cases} \quad (5.13)$$

Thus, we use the set of equations on the left hand side of Eq. (6.9) to express an opinion $\omega_B^A(b, d, u, a)$ of the avatar A on the avatar B in terms of the positive p and negative n outcomes of their past interactions.

5.5.3 Abstract Case Study: A Revisited Example

In the context of online games, a trust network can be defined as a plain trust network (cf. Definition 7) whose connections (or directed edges) are endowed with trust opinions, that is, a directed graph of avatars whose edges denote the trust relationships and opinions they establish with each other. For example, recall the trust network involving 7 avatars interacting within an in-world region of OpenSimulator, as illustrated in Fig. 5.8, where 18 different trust relationships were set from 89 interactions between avatars (cf. Eq. (5.8)).

By applying subjective logic, in particular the equalities on the left hand side of Eq. (6.9), it is straightforward to convert the trust relationships into opinions; equivalently, it is an easy task to convert the trust matrix (cf. Eq. (5.8)) into an opinion matrix as follows:

$$\omega = \begin{matrix} \text{users} & \begin{matrix} A & B & C & D & E & F & G \end{matrix} \\ \begin{matrix} A \\ B \\ C \\ D \\ E \\ F \\ G \end{matrix} & \begin{bmatrix} 0 & \omega_B^A & 0 & 0 & 0 & \omega_F^A & 0 \\ \omega_A^B & 0 & \omega_C^B & \omega_D^B & 0 & \omega_F^B & 0 \\ \omega_A^C & \omega_B^C & 0 & 0 & \omega_F^C & 0 & 0 \\ 0 & \omega_B^D & \omega_C^D & 0 & 0 & \omega_F^D & 0 \\ 0 & 0 & \omega_C^E & 0 & 0 & 0 & 0 \\ \omega_A^F & \omega_B^F & 0 & 0 & 0 & 0 & 0 \\ \omega_A^G & \omega_B^G & \omega_C^G & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (5.14)$$

5.6 Assembling Trust Networks

As seen above, we have shown how to derive a trust network from avatar-avatar interactions, aggregated into trust relationships, from which we derive trust opinions. In order to allow an avatar to formulate an opinion about another avatar without any previous direct interaction, we have been led to the concept of *extended individual trust network* \mathbb{T}_e , which is built up by assembling a tree of individual trust networks \mathbb{T}_i . Therefore, the concept of extended individual trust network is the key mechanism behind the inference engine detailed in chapter 6. This is illustrated in Fig. 5.11, which shows the extended individual trust network of the avatar A . For example, despite the inexistence of any previous interaction between A and C , A is able to formulate an opinion about C because C belongs to its extended individual trust network.

As shown in Fig. 5.11, assembling individual trust networks into an extended trust network \mathbb{T}_e^A of the avatar A is a procedure of attaching individual trust trees as subtrees of \mathbb{T}_i^A recursively; more specifically, A had interacted with B and F , so we attach the trees of B and F to the nodes B and F of A , and repeat the procedure for each of their nodes. The stopping condition for attaching a tree is when it already exists in the tree. As illustrated in Fig. 5.11, the \mathbb{T}_e^A building process initiated in A follows a Breadth First Search (BFS) process that results in the following edges:

1. $A \rightarrow B$ (obtained from \mathbb{T}_i^A)
2. $A \rightarrow F$ (obtained from \mathbb{T}_i^A)
3. $B \rightarrow C$ (obtained from \mathbb{T}_i^B)
4. $B \rightarrow D$ (obtained from \mathbb{T}_i^B)
5. $C \rightarrow E$ (obtained from \mathbb{T}_i^C)

For inference reasoning purposes, we encode this extended individual trust network \mathbb{T}_e^A

in the matrix form as follows:

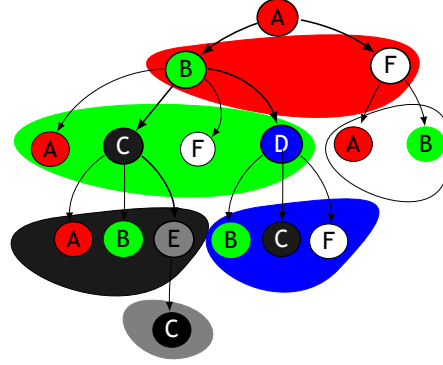


Figure 5.11: Example of an extended trust network \mathbb{T}_e^A for A .

$$\mathbb{T}_e^A = \begin{matrix} & \text{users} & A & B & C & D & E & F & G \\ A & \left[\begin{array}{cccccc} \Gamma_B^A & \Gamma_B^A & \Gamma_B^A & \Gamma_B^A & \Gamma_F^A \\ & \Gamma_C^B & \Gamma_D^B & \Gamma_C^B & \\ & & \Gamma_E^C & & \end{array} \right] \end{matrix} \quad (5.15)$$

This process can be employed as a personal trust assessment mechanism that any user/avatar can use to assess others.

5.7 User's Trust Inference System

As shown in Fig. 5.12, the personalized trust inference system is structured as a trust pipeline with three stages: *collecting*, *representing*, and *reasoning*. This chapter has detailed the first two stages, while the third stage is approached in the next chapter (Chapter 6).

5.7.1 First Stage: Collecting Avatar-Avatar Interactions

In the first stage, events (ϵ) and actions (A) are gathered and handled in order to construct and represent avatar-avatar interactions (\mathcal{I}). This is achieved by conversion of in-world occurrences from user/avatar actions and events into interactions as VW/MMOG permanent storage representations (e.g., a MySQL database in OpenSimulator is employed for data storage). This was detailed in Section 5.3.

5.7.2 Second Stage: Storing Trust Relationships and Opinions

The second stage is the core of the personalized trust inference system. Herein, interactions (\mathcal{I}) are aggregated by scope into trust relationships (\mathcal{I}), which in turn are

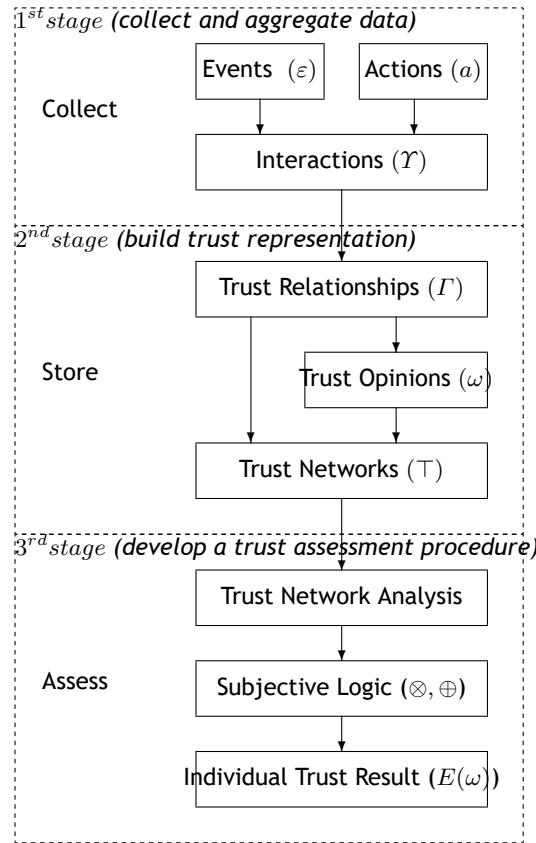


Figure 5.12: Trust inference system.

converted into subjective logic trust opinions (ω) and trust networks (T). Thus, this stage corresponds to the construction of trust and opinion networks, in particular the extended individual trust/opinion networks, which constitute the fulcrum of the personalized trust inference system proposed in this chapter and the next (Chapter 6). Note that subjective logic is here used to derive trust opinions (ω) from trust relationships, so that the resulting opinion network is basically a trust network enhanced with the representation of opinions.

5.7.3 Third Stage: Trust Assessment

The last stage is where trust inference and reasoning take place, and will be detailed in chapter 6. For this purpose, we apply subjective logic (SL) operators to paths linking trustor and trustee in the individual trust network of the trustor, even when there was not any interaction between them in the past. As described in chapter 6, these subjective logic operators are the discount (\otimes) and consensus (\oplus) operators. As a result, the trustor does obtain a trust opinion on the trustee, which is expressed as a probability expectation value.

The assessment across each personalized trust network (i.e., the trust network of each avatar) will be addressed using three different methods in order to obtain a representative trust path or paths linking trustor and trustee. In the first method, we will consider Jøsang TNA-SL [JHP06] and Optimal TNA-SL [JB08b, Bhu11]. In the second method, we

employ SL directly to the \mathcal{T} without any simplification as in West [WKLS09]. Finally, the third method will use breath-first search and depth-first search (BFS/DFS) in the assessment of (\mathcal{T}) to obtain the representative paths linking trustor and trustee, and further processed with subjective logic.

5.8 Discussion

The bottom-up methodology used in this chapter and the following (Chapter 6) aims to demonstrate the applicability and usability of trust mechanisms in virtual worlds. In the current chapter, the focus is on collecting and aggregating data generated by avatar-avatar interactions in the virtual world (first stage of the trust inference system), from which we construct trust relationships and trust networks (second stage of the trust inference system). In the next chapter (Chapter 6), we will discuss how trust is calculated from those trust networks (third stage of the trust inference system).

At this point, we are in position of responding to the first two research questions put forward in the first section of the current chapter:

Q1 – What kind of in-world data are available and how can they be collected?

Taking into consideration that OpenSimulator is open-source, we have direct access to system-generated events. Therefore, we had only to devise a way of intercepting and filtering its actions/events related to avatar-avatar interactions. See Section 5.3 for further details.

Q2 – Can we turn in-world data gathered in the environment into a persistent computational trust representation?

In Section 5.3, it was shown how collected data in the form of avatar-avatar interactions could be stored in OpenSimulator database. In Section 5.4, we demonstrated how to derive trust relationships from avatar-avatar interactions. Recall that trust relationships express positive and negative interactions between avatars. A graph of avatars (nodes) and their trust relationships (edges) form what we call a trust network.

We have also shown in Section 5.5 how to derive trust opinions from trust relationships using the barycentric coordinate system of subjective logic. These opinions will be used in the following chapter (Chapter 6) to compute the trustability of a given avatar from a personal point of view (cf. Section 5.7). This computation will be performed using subjective logic operators. Thus, the third (Q3) and fourth (Q4) questions will be addressed in due time in the next chapter (Chapter 6).

5.9 Summary

In this chapter, we have introduced a bottom-up methodology to build up a 3-tier personal trust inference system for virtual worlds, in particular for OpenSimulator. The collecting and aggregating of data generated by actions and events associated to avatar-avatar interactions are performed in the first tier. The second tier includes a procedure to derive trust relationships from avatar-avatar interactions in order to make it possible to determine trust opinions and build up trust networks. The third tier incorporates an inference mechanism based on graph search algorithms and subjective logic operators to compute the trustworthiness of a given avatar-impersonating user. Thus, the main contribution of the chapter is the formalization of trust as a usable concept for virtual worlds, which translates itself into a personal trust system that each in-world user may enjoy during his/her interactions with others.

Chapter 6

Trust Inference

Representing, manipulating, and inferring trust from the user point of view certainly is a grand challenge in virtual worlds, including online games. When someone meets an unknown individual, the question is “Can I trust him/her or not?”. This requires the user to have access to a representation of trust about others, as well as a set of operators to undertake inference about the trustability of other users/players. In this chapter, we employ a trust representation generated from in-world data in order to feed individual trust decisions. To achieve that purpose, we assume that such a representation of trust already exists; in fact, it was proposed in another paper of ours cf. [CGF16a], as described previously in chapter 5. Thus, the focus here is on the trust mechanisms required to infer trustability of other users/players. More specifically, we use an individual trust representation deployed as a trust network as base to the inference mechanism that employs two subjective logic operators (consensus and discount) to automatically derive trust decisions. The proposed trust inference system has been validated through OpenSimulator scenarios, which has led to a 5% increase on trustability of avatars in relation to the reference scenario (without trust).

6.1 Introduction

Human relationships rely on trust. The idea of trust computing is to emulate such trust relationships on computer. The question is then that “believe or not believe” on someone depends on user’s experience, and how the user perceives others and the context. Personal experience is the result of a knowledge gathering process about others, their behavior similarities and differences, and so forth, as a result of the prior interactions with others and surrounding world. When we say that humans are social beings, we are also saying that they are interactive entities who change and refine themselves over time and with experience, i.e., they learn in response to their senses.

Thus, the grand challenge advanced by the authors in the previous chapter cf. [CGF16a] was how to gather data from avatar-avatar interactions and transform them into *direct* trust data. The previous chapter succeeded in gathering and representing such direct trust data. Now, what remains to know is how to infer *indirect* trust data from direct trust data embedded in a network of avatars. As Jøsang argued in [Jøs13], we need to assess if anyone else is trustworthy enough to interact with. This is particularly important when someone intends to interact with an unknown someone else. In short, chapter 5 was about the data gathering from avatar-avatar interactions and their trust

representations, while this chapter is about trust inference and reasoning, i.e., this chapter details how to reason about those trust data and decide accordingly.

6.1.1 Motivation

Trust is profusely used in everyday life decision making process. In games and virtual worlds, we need to find a way of mimicking trust between avatars as humans do in their daily lives. In order to achieve that, we need to consolidate the three stages of the trust pipeline: *collecting*, *representing*, and *reasoning* on avatar-avatar interactions. The first two were dealt with in the previous chapter, while the third will be approached throughout the current chapter.

Obviously, this requires the framework of a trust model in games and virtual worlds, as we find in specific fields such as social networks [SNP13], work-flows [VM12], MANETs [CSC11, GM12] and online auctions [WJDW10]. In fact, VW/MMOGs have some similarities with other areas in which trust models were already employed. For example, the socialization process promoted by social networks [SNP13] is similar in virtual worlds [DIG13] and online games. But, as far as we know, trust models have never been used in the context of games and virtual worlds. In a way, this is the *raison d'être* of these two chapters, the current and its predecessor (Chapter 5).

6.1.2 Contributions

The main contributions of this chapter are the following:

- We propose a *personal trust model* that allows to assist any avatar-impersonated user in its decision-making about others *within* the virtual world, as humans do in their daily lives. This is in contrast with current approaches based on centralized reputation systems that makes statistical data partially available to users, though the most common process of passing information from user to user in virtual worlds and games is word of mouth.
- We propose a trust inference engine sustained on path-finding algorithms and subjective logic (SL) operators. In fact, we use BFS (breadth-first search) and DFS (depth-first search) pathfinders to extend the TNA-SL (trust network analysis with subjective logic) previously used in other contexts, other than games and virtual worlds.

6.1.3 Organization of the Chapter

The remainder of this chapter is organized as follows. Sec. 6.2 provides a brief overview of trust representation developed in the previous chapter, as illustrated in Fig. 6.1. Sec. 6.3 shows how to assembly avatar trees to path the way between a trustor and a

trustee, from which we are able to find BFS (breath-first search) and DFS (depth-first search) paths between two avatars. This is particularly important when the trustor had no idea about the trustee, simply because they have never met before. Sec. 6.4 shows us how to apply subjective logic operators to the BFS and DFS paths, as a way of a trustor evaluating the trustability of the trustee. Sec. 6.5 describes a number of experiments in order to validate the benefits of using our BFSDFS-SL trust engine in virtual worlds and games. Sec. 6.6 elaborates on the research questions put forward in chapter 5, highlighting the advantages of using trust modeling in virtual worlds as humans do in their real lifes. Sec. 6.7 concludes the chapter with some hints for future work.

6.2 Personal Trust System: an Overview

As mentioned above, our individual trust system is based on a pipeline of three stages: collecting, representing (or storing), and assessing. This three-stage system is shown in Fig. 3. The first two stages (collecting and representing) were described in the previous chapter [CGF16a], while the third stage (assessing) is detailed in the present chapter. Before proceeding any further, let us then briefly approach each of them separately.

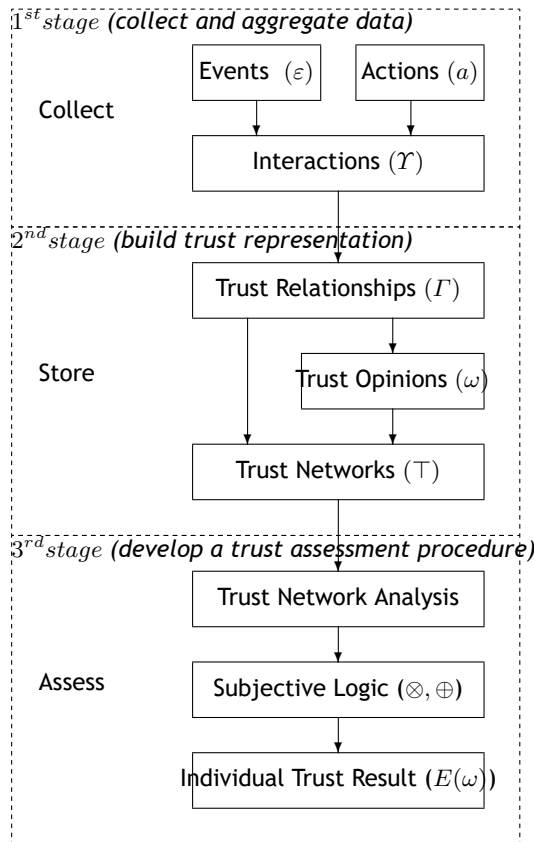


Figure 6.1: Pipeline of our personal trust system.

Table 6.1: Data formats.

Type	Representation
User parameterizations	$P = (i, s, g, t, r, d, a)$
Event	$\varepsilon_B^A = (u_A, n_A, u_B, n_B, b, m, G, R, t)$
Action	$a = (i, A, t, c, p)$
Interaction	$\Upsilon = (i, s, g, t, r, d, o)$
Trust Relationships	$\Gamma = (i, s, g, t, r, d, a, p, n)$ $\Gamma = (i, a, p, n)$
Trust Opinions	$\omega = (i, s, b, d, u, a)$ $\omega = (b, d, u, a)$
Trust Networks	$\top = (\Gamma, A)$ $\top_i = (\Gamma, A)$ $\top_e = (\Gamma, A)$
Trust result value	$E(\omega)$

6.2.1 Collecting (1st stage)

Considering that we intend to have an individual trust system to help each avatar (user) in its trust decision-making about others, we start collecting data with reference to its own parameters (cf. user parameterizations in Table 6.1).

Collecting consists in gathering event/action data generated from in-world user activities, which will be used to characterize, to represent, and to store avatar-avatar interactions. That is, events and actions (in the formats shown in Table 6.1) are converted into representations of avatar-avatar interactions (see also Table 6.1), in a format adequate for permanent storage; for example, OpenSimulator uses a MySQL database for permanent data storage.

6.2.2 Representing (2nd stage)

The second stage represents the process by which the stored avatar-avatar interactions (Υ) are used to derive trust relationship representations (Γ), which in turn are later converted into subjective logic trust opinions (ω) and trust networks (\top), as illustrated in Fig. 6.1.

6.2.2.1 Trust relationships

The avatar-avatar interactions are at the heart of our personal trust system. From the point of view of each avatar, such interactions are classified as either ‘successful’ (1) or ‘unsuccessful’ (0), which are then aggregated by scope in order to produce trust relationships. Recall that an avatar-avatar interaction γ_B^A between two avatars A and B originates two **trust relationships**, Γ_B^A and Γ_A^B ; in Γ_B^A , A is the *trustor* and B is the *trustee*, but they swap their roles in Γ_A^B . A trust relationship is unidirectional and not reflexive, so that a trustor cannot be a trustee, other than in another trust relationship; that is, it is not feasible to have Γ^A nor Γ^B . In order to elucidate this point, let us consider we have the transitive path $A \rightarrow B \rightarrow C \rightarrow A$ of trust relationships, where A appears as a trustor in Γ_B^A and a trustee in Γ_A^C , but not in the same trust relationship.

In a more formal setting, a trust relationship between a trustor A and a trustee B is represented by the tuple $\Gamma_B^A = (i, s, g, t, r, d, a, p, n)$, where i is its integer identifier, s the scope of the activity, g the goal to be achieved, t the time of the assessment, r the risk taken by the trustor, a the base rate taken from trustor (user) parameterizations, d the decay factor also taken from trustor (user) parameterizations, and p and n is the number of positive and negative outcomes, i.e., $o = 1$ and $o = 0$, respectively. In practice, we use the simplified form $\Gamma_B^A = (i, a, p, n)$ for trust relationships.

6.2.2.2 Trust networks

By aggregating all the individual trust relationships of a trustor avatar, we obtain a height-1 tree called **individual trust tree**. In turn, recursively appending the individual trust trees of the trustee avatars to the individual trust tree of a trustor avatar, we end up obtaining what we call the **personal trust tree** of a given (trustor) avatar.

In a more general setting, a **trust network** $\mathbb{T} = (\Gamma, \mathbf{A})$ is a digraph representation of all trust relationships $\Gamma = \{\Gamma_1, \dots, \Gamma_m\}$ established between avatars $\mathbf{A} = \{A_1, \dots, A_n\}$. Therefore, both individual trust tree and its expanded version, called personal trust tree, of an avatar (as a trustor) are subsets of the trust network of the entire game world.

6.2.2.3 Trust opinions

Trust relationships are used not only to build up trust networks, but also to derive trust opinions (ω) using subjective logic. In practice, each trust relationship of a trust network is enhanced with a subjective logic opinion. This is a requirement for those interested in carrying out reasoning and inference across the trust network, as explained below.

6.2.3 Assessing (3rd stage)

The final stage of the trust pipeline in Fig. 6.1 ends up at calculating the trust value associated to the trustee, as required by the trustor. The idea is to support the trustor on its judgment about the trustee. To a large extent, this constitutes the *raison d'être* of this thesis as detailed in this chapter and in chapter 5 (cf. [CGF16a]). For that purpose, we have to devise a way to reason on the trust network in order to find a trust path (or paths) between trustor and trustee.

In this chapter, we employ three different methods to obtain a representative trust path or paths linking *trustor* with *trustee*, namely:

- *Jøsang method*. This method is due Jøsang [JHP06], and is known as TNA-SL. This method had a follow-up named *optimal* TNA-SL [JB08b, Bhu11].
- *West method*. This is a variant of the Jøsang method, with the particularity of not owning any simplification [WKLS09].
- *BFS/DFS method*. This method uses graph search techniques to find a set of representative paths between two nodes of the trust network, the start node (trustor) and the goal node (trustee). As far as we know, these graph search techniques have never been used in the context of trust computing in games.

These methods correspond to the *trust network analysis* (TNA) module depicted in Fig. 6.1. Having found paths linking *trustor* and *trustee*, we apply subjective logic operators (\otimes and \oplus) to such paths, as indicated in Fig. 6.1 and described in Algorithm 3. These operators are those originally introduced by Jøsang in [JHP06]. From the application of those operators to trust paths results a trust opinion (ω) that a trustor has developed on the *trustee*, which is then used to obtain a quantifiable trust assessment as a probability expectation value ($E(\omega)$), represented in the final block of Fig. 6.1.

6.3 Finding Trust Paths

Before calculating a quantifiable trust value of the *trustee* by the *trustor*, we need to find at least one path connecting them in the graph underlying the trust network. Recall that, in the literature, we find mainly two techniques to determine those paths, namely: trust network analysis (TNA) due to Jøsang [JHP06, JB08b] and Bhuiyan [Bhu11] and the modified TNA proposed by West et al. [WKLS09].

TNA has proved to be applied to several types of networks, namely: social networks [ZXL⁺12], multi-agent systems (MAS) [WHS11], P2P [WAC⁺09], and reputation systems [PSA12]. But, it finds all paths between the trustor and the trustee, so that it tends to cover the entire search space. This means that TNA is very time consuming, but worse it is the fact that we very likely get paths with cycles or paths with edges repeated multiple times. In order to get canonical paths, i.e., paths without cycles and edge

Algorithm 3: Modeling algorithm.**Data:** u_A : in-world user id for truster (sender) u_B : in-world user id for trustee (receiver) s : scope of the activity**Result:** $E(\omega_B^A)$: quantifiable trust assessment of u_B by u_A

```

/* First Stage */
1 begin
    /* loads  $u_A$  parameterizations */
2    Load  $P(u_A) = (i, s, g, t, r, d, a)$  from database;
    /* collect/store  $(A)/(\varepsilon)$  into  $(\mathcal{Y})$  */
3    while  $(A)/(\varepsilon)$  occur in-world do
        /* algorithm described in [CGF16a] */
4        Execute CollectAlgorithm ;
5        return  $\mathcal{Y}_B^A$ ;

/* Second Stage */
6 begin
    /* define trust relationships  $(\Gamma)$  */
7    for all  $\mathcal{Y}(i, s)$  do
        /* algorithm described in [CGF16a] */
8        Execute GatherStoreAlgorithm;
9        return  $\Gamma_B^A$ ;

    /* determine trust opinions  $(\omega)$  */
10   read  $\Gamma(i)$ ;
11   repeat
12       read  $\Gamma(i)$ ;
13       Convert  $(\Gamma)$  into  $(\omega)$ ;
14       i-;
15   until  $\Gamma(i) = 0$ ;

    /* determine trust network  $(\mathcal{T})$  */
16   Build  $(\mathcal{T})$  from  $(\Gamma)$ ;

/* Third Stage */
17 begin
    /* trust network analysis on  $(\mathcal{T})$  */
18   Execute Algorithm 2;
19   return  $\mathcal{T}_B^A$ ; /* subjective logic application */
20   Apply SL operators to  $(\mathcal{T}_B^A)$ ;
    /* convert  $\mathcal{T}_B^A$  into  $\omega_B^A$  */
21   Determine  $\omega_B^A$ ;
    /* determine a trust value  $E(\omega_B^A)$  */
22   Uses  $\omega_B^A$  to determine  $E(\omega_B^A)$ ;
    /* present results to user */
23   return  $E(\omega_B^A)$ ;

```

repetitions, we have to simplify the trust network. Therefore, simplification aims at eliminating eventual cycles and edge repetitions along each path between trustor and trustee. This simplification generates a directed series-parallel graph (DSPG) between the trustor and the trustee. However, because of the computational complexity and time processing required to achieve the optimal DSPG [JHP06], only trust paths with a level of confidence over a given threshold are filtered out. The downside of this approach is that it may exclude relevant paths that could provide a more accurate final outcome.

The problem of finding all the DSPG paths was considered impractical and computationally unfeasible for fully connected networks representing therefore an exponential number of possible paths to consider; hence West et al. [WAC⁺09, WKLS09] proposed a different strategy for the TNA-SL model, called *modified* TNA-SL. This modified method does not require the graph analysis of the trust network, i.e., there is no need to determine all paths between trustor and trustee. Instead, one uses a $n \times n$ connectivity matrix for n users to derive a preliminary opinion matrix, which is iteratively updated by applying the discount (\otimes) and consensus (\oplus) subjective operators, getting so an opinion matrix with the most certainty of the trust relationships.

Algorithm 4: BFS/DFS trust network assessment .

Data:

u_A : in-world user id for truster (sender)
 u_x : in-world user id for trustee (receiver)
 s : scope of the activity
 \mathbb{T} : scenario trust network

Result:

\mathbb{T}_x^A : Trust network paths linking A with x

```

1 begin
2   Execute procedure BFS( $\mathbb{T}, A$ );
3   Execute procedure DFS( $\mathbb{T}, A$ );
4   Aggregates  $BFS/DFS_x^A$  results as  $\mathbb{T}_{bfsdfs}^A = \mathbb{T}_{bfs}^A + \mathbb{T}_{dfs}^A$ ;
   /* Result BFSDFS paths from  $A$  to  $x$  */
5 begin
6   Parse  $\mathbb{T}_{bfsdfs}^A$  to find paths from  $A$  to  $x$ ;
7    $\mathbb{T}_x^A = BFSDFSpaths\ found$ ;
```

Our method was inspired in the trust model introduced by Golbeck [Gol05], which was designed for social networks. Golbeck's trust model uses a modified breadth first search (BFS) to find a path between trustor and trustee, so that it is efficient and fast to reach all users within the shortest path distance from the trustor (i.e., source user). More specifically, Golbeck [Gol05] employed a BFS-based minimal path solution in order to minimize the number of transitive hops interactions in the trust network. Therefore, the graph search of Golbeck's trust model does not produce an overall trust assessment, simply because the search ends up being limited to a localized region of the search space, following the observed feature that shorter paths and higher trust values lead to

better accuracy in trust assessment [Gol05].

In contrast, we propose here a new method based on breath first search (BFS) and depth first search (DFS), as described in Algorithm 4. The use of these two path-finding algorithms to find two alternative paths between trustor and trustee was motivated by the following observations:

- *Bounded search space.* Unlike Jøsang's trust model [JHP06], we do not consider all the possible paths between trustor and trustee; instead, we use two path finders, BFS and DFS, that operate on a part of the search space. This agrees with the fact that, in virtual worlds and online games (VW/MMOGs), each user interacts with those within its Aol (area of interest), or at most within the *instantiated region*, so that the number of users to take into account in finding paths between trustor and trustee is limited, yet the total number of users present in the virtual world may be thousands or millions. Note that, similar to Jøsang's trust model [JHP06], the trust solution proposed by West et al. [WAC⁺09] is also global, yet it is much more efficient in time performance.
- *Trust Assessment Accuracy.* This depends on the length of the paths found. The trust value degrades with the distance (i.e., number of intermediate graph nodes or users) from the trustor towards the trustee, so that shorter paths are in principle more accurate than longer paths, what is in conformity with what happens in the real life when individuals express opinions about others in a chained manner.

It is true that the BFS pathfinder used by Golbeck does not allow for cycles and repeated edges in the found path, but it has the drawback of using a single path between trustor and trustee. Instead, we use two-path approach that combines BSF and DFS pathfinding. The leading idea is to have an intermediate solution between the Jøsang's solution [JHP06] —that tends to cover the entire search space— and the single path solution proposed by Golbeck [Gol05]. As explained further ahead, this two-path solution ends up being a more balanced solution in the computation of the trust value when trustor and trustee never met before.

6.3.1 Finding Paths using BFS

As seen in the previous chapter [CGF16a], a plain trust network \mathbb{T} basically is a network (or graph) of avatars and their direct interactions. This is illustrated in Fig. 6.2, where we have a graph of 7 nodes (avatars) and 18 directed edges (trust relationships). Recall that the trust relationships are unidirectional.

The trust network shown in Fig. 6.2 is the result of combining the individual trust networks (T_i) of those seven avatars as follows: $T_A = \{B, F\}$, $T_B = \{A, C, D, F\}$, $T_C = \{A, B, E\}$, $T_D = \{B, C, F\}$, $T_E = \{C\}$, $T_F = \{A, B\}$ and $T_G = \{A, B, C\}$. Recall that an individual trust network is a representation of the direct interactions that of an avatar have already established with others so far, which are shown in Fig. 6.3 for our

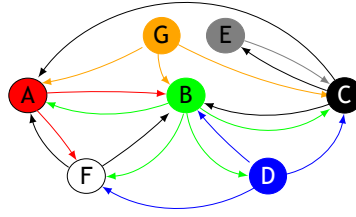


Figure 6.2: A trust network T from avatar interactions in OpenSimulator.

convenience.

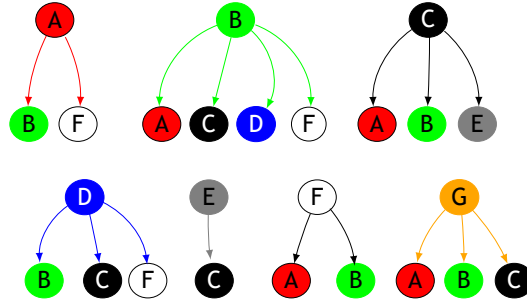


Figure 6.3: Individual trust networks (T_i) of 7 avatars.

In order to allow an avatar to formulate an opinion about another avatar without any previous direct interaction, we have been led to the concept of *extended individual trust network* T_i , which is built up by assembling a tree of individual trust networks T_i . Therefore, the concept of extended individual trust network is the key mechanism behind our inference engine, as detailed from here on. This is illustrated in Fig. 6.4, which shows the extended individual trust network of the avatar A . For example, despite the inexistence of any previous interaction between A and C , A is able to formulate an opinion about C because C belongs to its extended individual trust network.

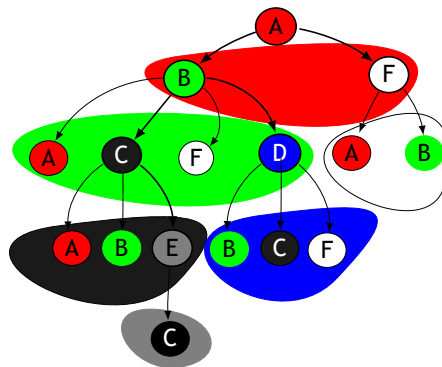


Figure 6.4: Extended individual trust network T_A for A .

As shown in Fig. 6.4, assembling individual trust networks into an extended trust network T_A of the avatar A is a procedure of attaching individual trust trees as subtrees of T_A recursively; more specifically, A had interacted with B and F , so we attach the trees of B and F to the nodes B and F of A , and repeat the procedure for each of their

nodes. The stopping condition for attaching a tree is when it already exists in the tree. As illustrated in Fig. 6.4, the assembling of individual trust networks into T_A follows a Breadth First Search (BFS) process that results in the following edges:

1. $A \rightarrow B$ (obtained from T_A)
2. $A \rightarrow F$ (obtained from T_A)
3. $B \rightarrow C$ (obtained from T_B)
4. $B \rightarrow D$ (obtained from T_B)
5. $C \rightarrow E$ (obtained from T_C)

These edges are the constituents of all paths from A to any other node in the graph. These paths are given by the paths of T_A (cf. Fig. 6.4), after excluding the terminal nodes of the tree, and are as listed in Fig. 6.5. The digraph representation of the BSF paths obtained in Fig. 6.5 is shown in Fig. 6.6. This digraph is a subgraph of the original plain trust network in Fig. 6.2.

```

BFS applied to (A)
A to B (B): A->B
A to C (C): A->B->C
A to D (C): A->B->D
A to E (D): A->B->C->E
A to F (B): A->F
A to G (-): not connected
    
```

Figure 6.5: Breath First Search process initiated from avatar A .

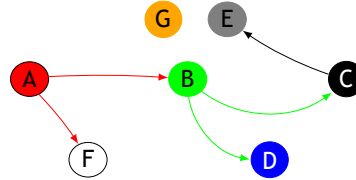


Figure 6.6: Digraph of BFS paths from trustor A .

For inference reasoning purposes, we encode this extended individual trust network T_e^A in the matrix form as follows:

$$T_e^A = \begin{matrix} & \text{users} \\ & A & B & C & D & E & F & G \\ A & \begin{bmatrix} \Gamma_B^A & \Gamma_B^A & \Gamma_B^A & \Gamma_B^A & \Gamma_B^A & \Gamma_F^A \\ & \Gamma_C^B & \Gamma_D^B & \Gamma_C^B & \Gamma_E^C \\ & & & & \Gamma_E^C \end{bmatrix} \end{matrix} \quad (6.1)$$

This process can be employed as a personal trust assessment mechanism that any user/avatar can use to assess others.

6.3.2 Finding Paths using DFS

Finding paths starting at the trustor using DFS is similar to BFS. The difference lies in that the direct trust tree of each user is attached to the extended trust tree of the trustor in a different manner. BFS grows the extended trust tree first in width and in depth afterwards, while DFS does the opposite, i.e., DFS prioritizes the depth in relation to width. This is illustrated in Fig. 6.7, where the expansion of the tree of A goes firstly down by the way of F ; after completing the sub-tree of F , one comes back to B linked to A , but the tree expansion stops because B had already been dealt with in the sub-tree of F . The digraph representation of the DSF paths obtained in Fig. 6.8 is shown in Fig. 6.9. Obviously, this digraph is also a subgraph of the original plain trust network in Fig. 6.2.

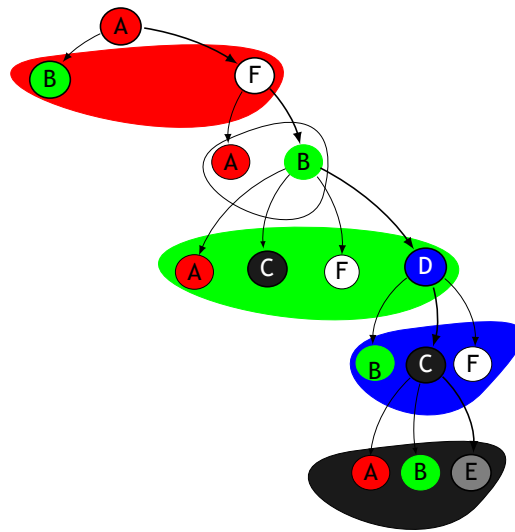


Figure 6.7: Extended individual trust network T_A for A .

```
DFS applied to (A)
A to B (B): A->F->B
A to C (C): A->F->B->D->C
A to D (D): A->F->B->D
A to E (E): A->F->B->D->C->E
A to F (F): A->F
A to G (G): not connected
```

Figure 6.8: Depth First Search initiated from A .

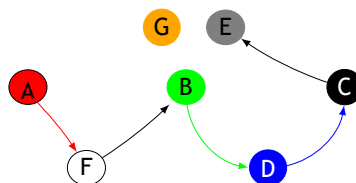
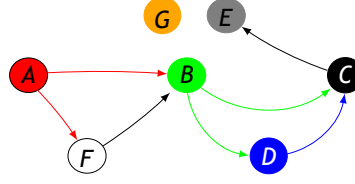


Figure 6.9: DFS paths from trustor A .


 Figure 6.10: Aggregated results of the BFS/DFS paths linking *trustor* and *trustee*.

6.4 Subjective Logic - based Trust Operators

Subjective logic provides means to produce a quantifiable trust assessment as a probability expectation, as suitable for analysis of situations with significant uncertainty [Jø97, Jøs13], and is the basis behind the TNA-SL model [JHP06, JB08b, LLJ⁺11, JHJ10]. Our interest in the subjective logic stems from the fact that it is able to emulate and evaluate trust as humans do in real world scenarios [CKN⁺15, TLHT09, ZDB11, GM12, PAS13]. This section describes how trust is calculated from BFS and DFS paths between trustor and trustee.

6.4.1 Trust Opinions

As explained in the previous chapter [CGF16a], a *trust opinion* entails a trust value that a trustor A has on another in-world user B within a given activity at a given time. More formally, a trust opinion of A on B is represented by the following 4-tuple:

$$\omega_B^A = (b, d, u, a) \quad (6.2)$$

with $(b, d, u, a) \in [0, 1]$ and $b + d + u = 1$, where b represents the amount of belief A as on B , d stands for the disbelief (i.e., the opposite of b) that A assigns to B , u is the value that amounts the uncertainty of the opinion, and a is the base-rate or the preset value in the model parameterization settings, or in the user individual profile, that establishes the influence that uncertainty has in the *trust predicted value*, also called *trust opinion probability expectedated value*, E of ω_B^A , which is as follows:

$$E(\omega_B^A) = b + au \quad (6.3)$$

Recall that this trust value applies to direct trust relationships, being the 4-tuples (b, d, u, a) calculated from the positive (p) and negative (n) outcomes of the past interactions between A and B . If there were not any interactions in the past between A and B , we have to calculate the trust value by applying subjective logic operators (i.e., discount and consensus) along paths connecting A and B in the search graph underlying the trust network.

6.4.2 Discount Operator

The discount operator (\otimes) is used to compute trust along a chain of trust relationship edges in a transitive path [JHP06, JIB07, Bhu11]. Its specific features contribute to increase uncertainty as confidence decreases along the chain [JB08b].

In order to realize how this operator works after all, let us consider an activity involving three users A , B and C , where we already have two direct trust relationships, namely A is linked to B and B with C , i.e., we assume that we already have two trust opinions, ω_B^A and ω_C^B . Let also assume that there was not any interaction between A and C in the past. In order to allow A building an opinion on C via B , A has to resort to the discount operator (\otimes) as follows:

$$\omega_C^{A:B} = \omega_B^A \otimes \omega_C^B \quad (6.4)$$

with its four components given by:

$$\begin{cases} b_C^A = b_B^A b_C^B \\ d_C^A = b_B^A d_C^B \\ u_C^A = d_B^A + u_B^A + b_B^A u_C^B \\ a_C^A = a_C^B \end{cases} \quad (6.5)$$

The discount operator is graphically displayed in Fig. 6.11, where the transitive path between A and C through B is replaced by a new edge representing the discount opinion, as calculated using Eq. (6.5).

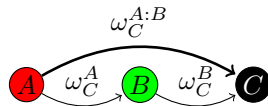


Figure 6.11: Transitive trust derivation with operator discount (\otimes).

6.4.3 Consensus Operator

BFS and DSF generate two canonical paths, i.e., paths without cycles and repeated edges. However, these paths may share intermediate nodes. These intermediate nodes work as confluence nodes of two distinct paths. The consensus operator (\oplus) enables us to fuse two opinions into a single one as a result of the confluence of two edges of distinct paths into a shared node, as shown in Fig. 6.12.

The consensus operator works as an trust update operation. In fact, it performs a similar operation to a bayesian network update [JB08b]. Applying the consensus operator results in a reduction of uncertainty. When uncertainty is absent ($u = 0$), an opinion (ω) can be seen as a weighted average of probabilities [JHP06]. To illustrate how the

consensus operator works, let us consider that the users A and B have an opinion on C ; these opinions are represented by ω_C^A and ω_C^B . The consensus operator \oplus fuses these two opinions about C as follows:

$$\omega_C^{A \diamond B} = \omega_C^A \oplus \omega_C^B \quad (6.6)$$

with its 4-tuple components given by the following expressions:

$$\begin{cases} b_C^{A \diamond B} = \frac{b_C^A u_C^B + b_C^B u_C^A}{u_C^A + u_C^B - u_C^A u_C^B} \\ d_C^{A \diamond B} = \frac{d_C^A u_C^B + d_C^B u_C^A}{u_C^A + u_C^B - u_C^A u_C^B} \\ u_C^{A \diamond B} = \frac{u_C^A u_C^B}{u_C^A + u_C^B - u_C^A u_C^B} \\ a_C^{A \diamond B} = a_C^A = a_C^B \end{cases} \quad (6.7)$$

and $u_C^A + u_C^B \neq u_C^A u_C^B$. Thus, this operator creates an opinion that represents the aggregated opinion from A and B on C .

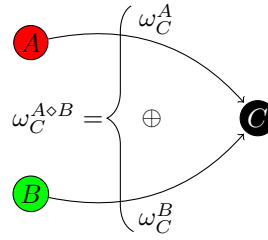


Figure 6.12: Trust aggregation with operator consensus (\oplus).

Before proceeding any further, let us recall that the subjective logic operators are applied to the trust network paths linking *trustor* and *trustee*, in order to obtain a unique trust opinion representing the *trustor* opinion on the *trustee*.

6.4.4 Trust Inference Scenario

Now, we are in the position of carrying out trust inference on a trust network. Let us the network depicted in Fig. 6.2, whose scenario represents a snapshot of an in-world region at a specific time, where we have seven avatars moving around.

6.4.4.1 Trust pipeline: 1st stage

Let assume that there were 89 previous avatar-avatar interactions (\mathcal{I}), all performed within the same activity, with each avatar-avatar interaction scored with one out of two different outcomes values, either positive ($p = 1$) or negative ($n = 0$). These avatar-avatar interactions are then aggregated as 18 trust relationships $\Gamma = (i, p, n, a)$, with i

standing for the identifier of each trust relationship and a the base rate, as shown in Eq. 6.8:

$$\mathbb{T} = \begin{matrix} & \begin{matrix} u & A & B & C & D & E & F & G \end{matrix} \\ \begin{matrix} A \\ B \\ C \\ D \\ E \\ F \\ G \end{matrix} & \begin{bmatrix} 0 & \begin{bmatrix} 12 \\ 1 \\ 0.5 \end{bmatrix} & 0 & 0 & 0 & \begin{bmatrix} 7 \\ 3 \\ 0.5 \end{bmatrix} & 0 \\ \begin{bmatrix} 6 \\ 2 \\ 0.5 \end{bmatrix} & 0 & \begin{bmatrix} 1 \\ 4 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 0 \\ 2 \\ 0.5 \end{bmatrix} & 0 & \begin{bmatrix} 13 \\ 1 \\ 0.5 \end{bmatrix} & 0 \\ \begin{bmatrix} 5 \\ 0 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 0.5 \end{bmatrix} & 0 & 0 & \begin{bmatrix} 3 \\ 1 \\ 0.5 \end{bmatrix} & 0 & 0 \\ 0 & \begin{bmatrix} 1 \\ 0 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 0.5 \end{bmatrix} & 0 & 0 & \begin{bmatrix} 3 \\ 2 \\ 0.5 \end{bmatrix} & 0 \\ 0 & 0 & \begin{bmatrix} 4 \\ 1 \\ 0.5 \end{bmatrix} & 0 & 0 & 0 & 0 \\ \begin{bmatrix} 1 \\ 0 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 0 \\ 2 \\ 0.5 \end{bmatrix} & 0 & 0 & 0 & 0 & 0 \\ \begin{bmatrix} 3 \\ 0 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 8 \\ 0 \\ 0.5 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \\ 0.5 \end{bmatrix} & 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \quad (6.8)$$

Note that we considered the predefined base rate $a = 0.5$. The trust network matrix given by Eq. 6.8 is the output of first stage of the trust pipeline. It represents the direct individual trust representation between trustors and trustees; the value 0 denotes the absence of avatar-avatar interactions.

6.4.4.2 Trust pipeline: 2nd stage

As explained in chapter 6 [CGF16a], the second stage of the trust pipeline converts trust relationships $\Gamma_B^A = (i, p, n, a)$ into trust opinions $\omega_B^A = (b, d, u, a)$ of trustor A on trustee B as follows:

$$\begin{cases} b = \frac{p}{p+n+2} \\ d = \frac{n}{p+n+2} \\ u = \frac{2}{p+n+2} \\ a = \text{base rate} \end{cases} \quad (6.9)$$

so that, from the matrix in Eq. (6.8) we obtain the following opinion matrix:

$$\omega = \begin{matrix} & \text{users} & A & B & C & D & E & F & G \\ \begin{matrix} A \\ B \\ C \\ D \\ E \\ F \\ G \end{matrix} & \left[\begin{array}{ccccccc} 0 & \omega_B^A & 0 & 0 & 0 & \omega_F^A & 0 \\ \omega_A^B & 0 & \omega_C^B & \omega_D^B & 0 & \omega_F^B & 0 \\ \omega_A^C & \omega_B^C & 0 & 0 & \omega_E^C & 0 & 0 \\ 0 & \omega_B^D & \omega_C^D & 0 & 0 & \omega_F^D & 0 \\ 0 & 0 & \omega_C^E & 0 & 0 & 0 & 0 \\ \omega_A^F & \omega_B^F & 0 & 0 & 0 & 0 & 0 \\ \omega_A^G & \omega_B^G & \omega_C^G & 0 & 0 & 0 & 0 \end{array} \right] \end{matrix} \quad (6.10)$$

with

$$\left\{ \begin{array}{l} \omega_B^A = (0.8, 0.067, 0.133, 0.5) \\ \omega_F^A = (0.583, 0.25, 0.167, 0.5) \\ \omega_A^B = (0.6, 0.2, 0.2, 0.5) \\ \omega_C^B = (0.143, 0.571, 0.286, 0.5) \\ \omega_D^B = (0.0, 0.5, 0.5, 0.5) \\ \omega_F^B = (0.8125, 0.0625, 0.125, 0.5) \\ \omega_A^C = (0.7142, 0.0, 0.2857, 0.5) \\ \omega_B^C = (0.3333, 0.0, 0.6667, 0.5) \\ \omega_E^C = (0.5, 0.1667, 0.333, 0.5) \\ \omega_B^D = (0.3333, 0.0, 0.6667, 0.5) \\ \omega_C^D = (0.333, 0.0, 0.667, 0.5) \\ \omega_F^D = (0.4285, 0.2857, 0.2857, 0.5) \\ \omega_C^E = (0.5714, 0.1428, 0.2857, 0.5) \\ \omega_A^F = (0.3333, 0.0, 0.6667, 0.5) \\ \omega_B^F = (0.0, 0.5, 0.5, 0.5) \\ \omega_A^G = (0.6, 0.0, 0.4, 0.5) \\ \omega_B^G = (0.8, 0.0, 0.2, 0.5) \\ \omega_C^G = (0.3333, 0.0, 0.6667, 0.5) \end{array} \right. \quad (6.11)$$

6.4.4.3 Trust pipeline: 3rd stage

Let us now assume that the trustor A is about interacting with E , but they never met before. In order to A having *a priori* opinion about E , we first find BFS and DFS paths between them, as explained in Section 6.3. As shown in Figs. 6.6 and 6.9, these BFS and DFS paths are $A \rightarrow B \rightarrow C \rightarrow E$ and $A \rightarrow F \rightarrow B \rightarrow D \rightarrow C \rightarrow E$, respectively.

The union of these BFS and DFS graphs results in the digraph shown in Fig. 6.10 and also in Fig. 6.13(a) in a simplified manner. So, now we are in the position of applying the subjective logic operators discount (\otimes) and consensus (\oplus) in order to aggregate and fuse the opinions associated to the edges of the digraph depicted in Fig. 6.13 into a single trust opinion ω_E^A , which represents the trust opinion of A on E .

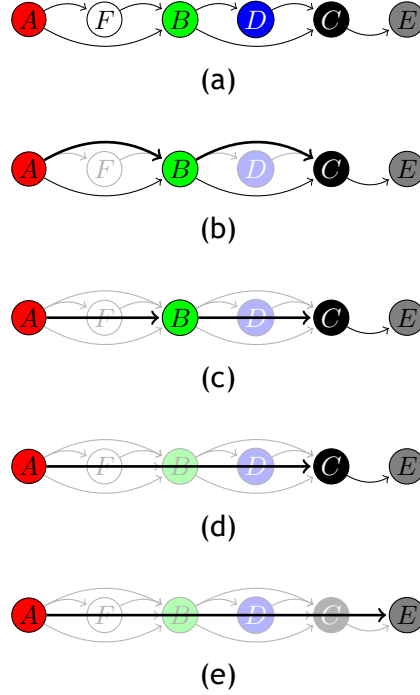


Figure 6.13: Digraph representing the trust network \mathbb{T}_E^A .

The application of the subjective logic discount operator to the transitive paths $A \rightarrow F \rightarrow B$ and $B \rightarrow D \rightarrow C$ results in a simplification of the initial digraph, as shown in Fig. 6.13(b). Basically, the trust opinions that A has on F and F on B , as well as the ones that B has on D and D on C are aggregated as $\omega_B^{A:F} = \omega_F^A \otimes \omega_B^F$ and $\omega_C^{B:D} = \omega_D^B \otimes \omega_C^D$. So, taking into account the values of the direct opinions in (6.9), we obtain the following:

$$\omega_B^{A:F} = (0, 0.292, 0.708, 0.5) \quad (6.12)$$

$$\omega_C^{B:D} = (0, 0, 1, 0.5) \quad (6.13)$$

Then, as illustrated in Fig. 6.13(c), the subjective logic consensus operator \oplus is used to merge the trust opinion ω_B^A represented by path $A \rightarrow B$ with the transitive trust opinion $\omega_B^{A:F}$, that is, $\omega_B^{(A:F) \odot A} = \omega_B^{A:F} \oplus \omega_B^A$ yields

$$\omega_B^{(A:F) \odot A} = (0.758, 0.115, 0.127, 0.5). \quad (6.14)$$

Analogously, the trust opinion ω_C^B represented by path $B \rightarrow C$ merges with the transitive trust opinion $\omega_C^{B:D}$, that is, $\omega_C^{(B:D) \diamond B} = \omega_C^{B:D} \oplus \omega_C^B$ yields

$$\omega_C^{(B:D) \diamond B} = (0.143, 0.571, 0.286, 0.5). \quad (6.15)$$

Once again, by combining $\omega_B^{(A:F) \diamond A}$ (cf. Eq. (6.14)) and $\omega_C^{(B:D) \diamond B}$ (cf. Eq. (6.15)) in a transitive manner, we obtain the graph simplification shown in Fig. 6.13(d), that is,

$$\omega_B^{(A:F) \diamond A} \otimes \omega_C^{(B:D) \diamond B} = (0.108, 0.433, 0.459, 0.5) \quad (6.16)$$

Finally, as illustrated in Fig. 6.13(e), we are able to express the subjective trust opinion of A on E as follows:

$$\begin{aligned} \omega_E^A &= (\omega_B^{(A:F) \diamond A} \otimes \omega_C^{(B:D) \diamond B}) \otimes \omega_E^C \\ &= (0.054, 0.018, 0.928, 0.5) \end{aligned} \quad (6.17)$$

Summing up, although initially avatar A did not possess any information on E , by using our BFSDFS-SL model to obtain a DAG linking A to E , we can provide a mean to assess the trustability of other avatars even without prior direct knowledge about them. Nevertheless, it should be borne in mind that the transitivity inherent to the discount operator tends to degrade an opinion as a path increases.

On the other hand, the consensus operator decreases uncertainty by averaging belief and disbelief in a fair and equal way. The quantifiable value representing the degree of trustability of avatar E from the assessment performed by A is obtained from Eq. (6.3), and is as follows:

$$E(\omega_B^A) = 0.054 + 0.5 \times 0.928 = 0.581 \quad (6.18)$$

Note that this trust value may change over time because of the dynamics of the avatar-avatar interactions taking place in the game virtual world.

6.5 Simulation Experiments and Discussion

6.5.1 Simulation Scenarios and Experiments Settings

In MMOGs or virtual worlds like OpenSimulator/SecondLife, the virtual world is partitioned in multiple regions (usually 256mx256m or 512mx512m regions). Essentially, we are interested in a simulation scenario (i.e., the trust network of avatars) that involves only a virtual region (i.e., a server), where several avatars interact with each other, and continuously assess the trust that nourish by others over time. With this scenario we intend to demonstrate the advantage of using trust-generated data to assist in-world users or avatars to take decisions as a result of their interactions with others. Therefore, key features to trust management in other areas like the node dynamics, communication overload, data integrity and security, which are addressed in P2P networks [GMMPGS09b, TLHT09], are not directly addressed here in our simulation.

6.5.1.1 Settings

The experiments were performed on a HP ProLiant DL160 G6 server, a quad-core Intel(R) Xeon(R) E5504 2.00GHz processor with 4 GB of RAM and a 160 GB disk drive. The operating system used was a Ubuntu 12.04.4 LTS with 64-bit kernel version 3.5.0-44-generic. All the results of the simulation were produced by a C-based applications and compiled by gcc version 4.6.3.

6.5.1.2 Behavior-based classification of users

To be able to reason about the advantages of trust usage in the simulation, we considered different types of user behaviors:

- *Honest* – This is the default behavior of in-world users who share items and interact honestly with others.
- *Pure malicious* – This represents users that lie to others in their interactions and on the items they possess.
- *Malicious* – This behavior represents users that although being trustful in their interactions lie about the items they possess.
- *Sybil* – This behavior has to do with forging different identities. By leaving and reentering the virtual world with new identity each time, he/she misbehaves to maintain a positive trust value. Because in the simulation settings, experienced users are preferred (e.g. users with more interactions) this type of behavior represents a challenge to detect.

The behavioral characteristics of each user that we have used in our simulation tests were those described by West et al. [WAC⁺09] and Pranata et al. [PAS13], and are as

indicated in Table 6.2 with reference to honesty. For example, honest users are 100% honest in their interactions with others, but not completely honest (>90% of honesty) in respect to their shared items of their inventories; in contrast, despite malicious users are also 100% honest in their interactions, they lie quite a lot in respect to their items (<10% of honesty). It is worthy noting that the behavior of each user remains unchanged during the simulation. Each avatar is either honest (or good) or misbehaved (or bad) as shown in Fig. 6.14 as green dots and red dots, respectively.

Table 6.2: Honesty-based behavior models.

	Honest	Pure Malicious	Malicious	Sybil
Interactions	100%	0%	100%	n.a.
Shared Items	> 90%	< 10%	< 10%	< 10%

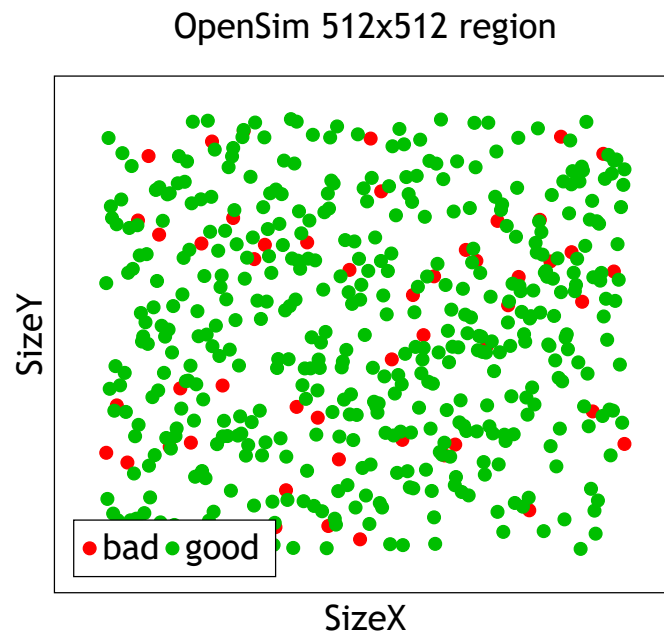


Figure 6.14: Snapshot of a OpenSim region with 500 avatars with a rate of 10% misbehaved (bad users in red).

6.5.1.3 BFSDFS-SL trust engine

Our simulation experiments described further below were carried out on our BFSDFS-SL trust engine. The BFSDFS-SL trust engine was designed as an extension to QTM (quantitative trust management), which is the quantitative trust model simulator developed at Pennsylvania University [Wes09]. QTM initially aimed to trust in P2P scenarios [Wes09], but it was also used in other areas like reputation systems [PAS13, YZCZ11, LTW10]. Although there are other trust modeling testbeds solutions [JHSMT13], we choose QTM because of its extended functionalities, in particular its user behavior modeling functionalities.

Enhancing Trustability in MMOGs Environments

The BFSDFS-SL trust engine comprises two stages: *dataset generator* and *construction of the trust network*. The input data consist of three parameters: number of user-impersonating avatars, percentage of each type of user behavior (i.e., honest, malicious, pure malicious, and sybil), and number of items to trade.

From the input data, the dataset generator produces a dataset into an ASCII file with the following data:

- A set of user-*behavior* pairs that describes how each user supposedly behaves. The association of behaviours to users is randomly generated using a Zipf distribution [Zip49].
- A set of user-*item* pairs that describes the inventory of each user. The distribution of items by avatars was modeled by a Zipf distribution [Zip49, WAC⁺09, KSGM03, PSA12], and represented with a value 0.9 as an attempt to reflect real life data patterns [PSA12]. The number of available item types to be distributed among users were limited to 25 to induce scarcity and in this way to increase the number of require interactions.
- A set of user-*query* pairs that describes the queries that each user put forward by each user to others users in the same region. The queries associated to each user are randomly generated taking into consideration its own items. Basically, a user may put forward a query to others in its region like “who has the item #5?” since the item #5 does not belong to its inventory. In order to obtain specific items, each user must interact with others in an attempt of obtaining items from them.

After generating the dataset into an ASCII file, we are in position of constructing the trust network incrementally from the avatar-avatar interactions, which in meanwhile have been generated from the aforementioned queries of the dataset. The number of interactions was limited to the range [1000,10000]. The edges connecting avatar nodes of the network denote direct trust relationships, many of them generated from indirect trust relationships through our BFSDFS-SL trust model.

6.5.1.4 Metrics

In the experiments described further below, we used two metrics to characterize and evaluate the simulation results: the performance metric (W) due to West et al. [WAC⁺09] and the time metric (t). The metric W denotes the performance of honest users as the ratio of the number of successfully traded items to the amount of interactions as follows:

$$W = \frac{v}{i} \quad (6.19)$$

where v stands for the number of valid items that have been traded between users, while i is the number of interactions that have taken place in a given region of the virtual world.

The time t plays an important role in the simulation because the avatar-avatar interactions supposedly occur in real-time. In particular, we are interested in evaluating the upper bound of the number of users that ensure a real-time performance. Recall that MMOGs and FPSs are particularly vulnerable to lag issues (e.g., a latency time above 200 ms would make a FPS game unplayable), what may negatively affect their trust usability.

6.5.1.5 Experiments

In order to validate our BFSDFS-SL trust model, we performed the following six experiments:

- *Exp. 1* – Here, we used scenario without trust, against a set of different misbehavior users. Thus, it is the reference scenario against which we will evaluate our model proposal.
- *Exp. 2* – This uses a scenario with trust. We use the same misbehavior users as in Exp. 1. Exp. 2 represents an attempt to validate the usage of trust in virtual worlds and games.
- *Exp. 3* – This experiment carries out a comparison of different misbehaviors. Each misbehavior is compared with two settings: with and without trust. For that purpose, we used results from Exps. 1 and 2.
- *Exp. 4* – This experiment addresses the impact of an increasingly crowded region (with users) and an increasingly number of interactions has on the simulation results.
- *Exp. 5* – In this experiment, we have a more realistic scenario with a population that is a mix of users of the four profiles (i.e., honest, pure malicious, malicious, and sybil).
- *Exp. 6* – Finally, this experiment addresses the time issue. One intends to evaluate the impact of the trust model on the processing time of the virtual world performance.

6.5.2 Experiment 1: Absence of Trust Modeling

6.5.2.1 Description

In this experiment, we first intend to assess the impact of misbehaved users in a virtual world without trust, which will work as the ground truth for the next two experiments.

For this purpose, we use a population of users of all types, including those behaving maliciously.

6.5.2.2 Settings

The graph in Fig. 6.15 was produced from a setting without trust mechanisms for three datasets generated for the different behaviors considered in accordance with the initial settings and parameterizations for 100 users, 25 items and 1000 interactions. The y-axis represents the metric defined by Eq. (6.19), i.e., the success rate of honest users. The x-axis features the percentage of each type of misbehaved users in the total amount of users considered in the parameterization. For example, in Fig. 6.15, a value of 0.8 of sybils stands for 80% of sybil users (i.e., just 20 honest users present in a total number of 100). For this percentage of sybil users, we have an honest for four sybils.

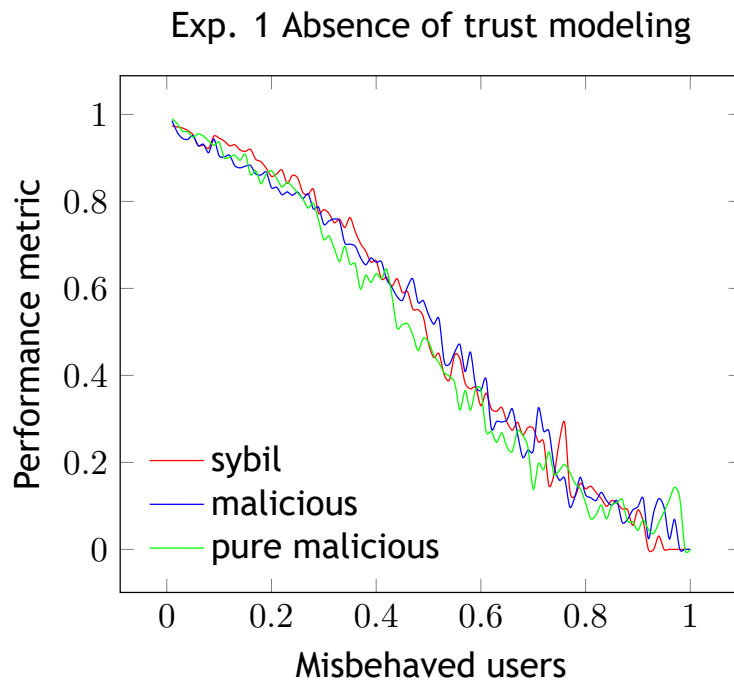


Figure 6.15: Impact on the honest user performance from rising the number of misbehaved users to saturation for three different behaviors in an absence of trust.

6.5.2.3 Discussion

Interesting conclusions can be drawn from the analysis of the results in Fig. 6.15. All misbehaviors are consistent with a Gaussian-like regression curve. The success rate given by Eq. (6.19) decreases with the number of misbehaved users. Regarding the results of the three different misbehaved user profiles, we see that there are no significant differences between them. Also, a population with less than 20% of misbehaved users still has a success rate higher than 80%, while, in the opposite situation, for a population with 60% of misbehaved users or higher, 60% the success rate of honest users

decays to less than 30%.

6.5.3 Experiment 2: Existence of Trust Modeling

6.5.3.1 Description

With this simulation we intend to analyze how our trust model embedded in a virtual world copes with different categories of misbehaved users separately, and at the same time to observe how they compare to each other. We also intend to compare the results obtained in this experiment with those produced by Exp. 1 in order to validate whether our BFSDFS-SL-based trust model is adequate for virtual worlds or not.

6.5.3.2 Settings

This experiment uses the same datasets of Exp. 1, i.e., files generated from the parameterizations concerning 100 users, 25 items, and 1000 interactions, with each file representing a specific integer percentage of misbehaved in-world users relative to the population of users, as expressed by the x-axis of Fig. 6.16. Again, the y-axis represents the success rate of honest in-world users, as expressed by the metric given by Eq. (6.19).

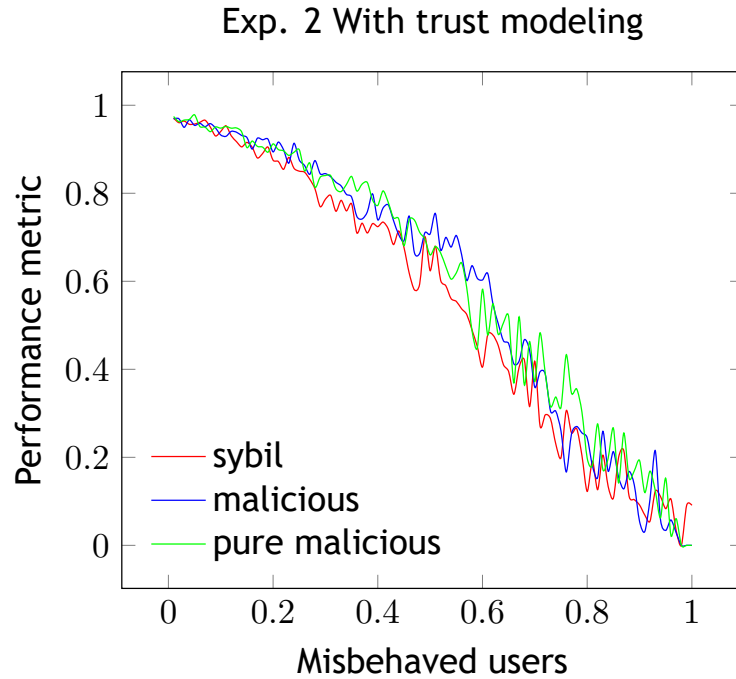


Figure 6.16: Effect on the performance of honest users from the rising number of misbehaved users until saturation for the three behaviors.

6.5.3.3 Discussion

The results depicted in Fig. 6.16 clearly show that using trust mechanisms is beneficial in terms of valid interactions from the honest user point of view. In fact, in a population having 20% to 80% of misbehaved users, honest users got more 5% to 10% of valid interactions in comparison with the results obtained in Exp. 1, i.e., the mean rate of successful interactions increases when one uses trust embedded in virtual worlds. Although the three user behaviors present similar results, the malicious and pure malicious behaviors show slightly better results than sybil in the range [30%,50%] of misbehaved users. For populations with less than 20% or greater than 80% of misbehaved users the differences are even smaller in relation to the scenario without trust of Exp. 1.

6.5.4 Experiment 3: Trust Modeling per User Category

6.5.4.1 Description

Now, we aim at checking the validity of the our trust model for each category of misbehaved users within a virtual world. For this purpose, we considered each type of misbehaved users separately, without and with trust, as shown in Figs. 6.17-6.19.

6.5.4.2 Settings

The input data and datasets (i.e., files with distinct percentages of misbehaved users) used in this experiment were the same as those used in the first two experiments. Figs. 6.17-6.19 show the impact of using trust mechanisms (curves in blue) in respect to a setting without trust (curves in red); once again, we used the West metric given by Eq. (6.19).

6.5.4.3 Discussion

Fig. 6.17 shows that there is a clear advantage in using trust mechanisms when the percentage of sybil users in the population is in the range [40%,70%]. Using trust seems to be even more advantageous for malicious (Fig. 6.18) and purely malicious (Fig. 6.19) users, being this more noticeable for a population with 30% or more of pure malicious users. Note that trust mechanisms have no significant impact for populations with more than 90% of misbehaved users, but this situation is not plausible because honest users would stop interacting with others, and probably would abandon the virtual world rapidly because of the increasing lack of trust. Anyway, it seems that trust mechanisms are slightly more advantageous in a population with pure malicious users than with other misbehaved users because the corresponding red and blue curves are more far away from each other (cf. Fig. 6.19).

Exp. 3 Sybil behavior impact on performance

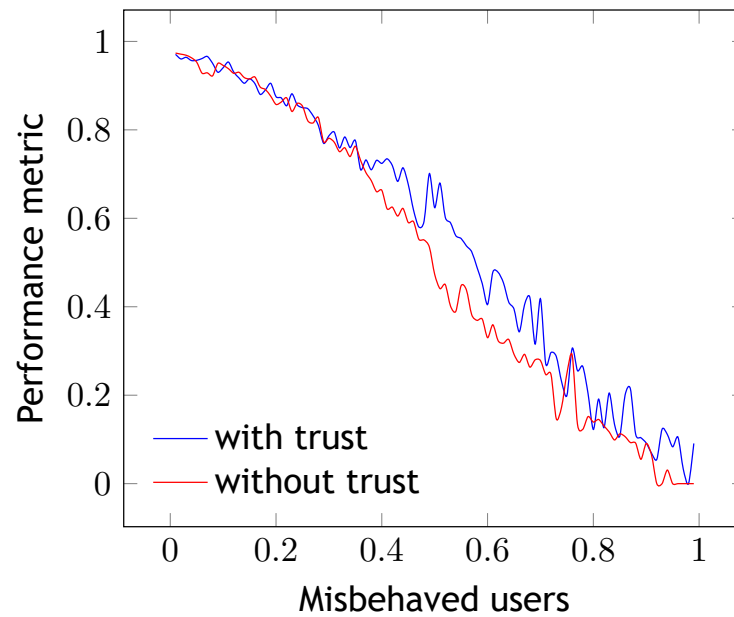


Figure 6.17: Effect on the performance of honest users from a rising number of sybil users in two scenarios, with and without trust.

6.5.5 Experiment 4: Trust Modeling with Data of Higher Orders of Magnitude for a Population with 4% of Malicious Users

6.5.5.1 Description

To address the impact of overcrowding the virtual space we performed some experiments with a varying number of users (from 50 to 500).

This experiment aims at evaluating the trust model in scenarios overcrowding the virtual region (or world). For that purpose, we have considered an increasing amount of the data (i.e., avatars and avatar-avatar interactions) associated to a region, for a population with a constant percentage of 4% of malicious users. In particular, we have a ten-fold increase in the number of users and the number of interactions; more specifically, the number of users increases from 50 to 500, whereas the amount of interactions increases from 1000 (or 1x) to 10000 (or 10x), as shown in Fig. 6.20.

In other words, we intend to assess the impact that the number of users and interactions have on our trust model. Nevertheless, in practice, we reckon that the amount of possible users interacting through their avatars is limited for two reasons. First, any region of the virtual world has a limited area and, consequently, a limited capacity in terms of physical space occupancy of their avatars. Second, even in a crowded region, a user is only capable of directly interacting with those located in his/her vicinity.

Exp. 3 Malicious behavior impact on performance

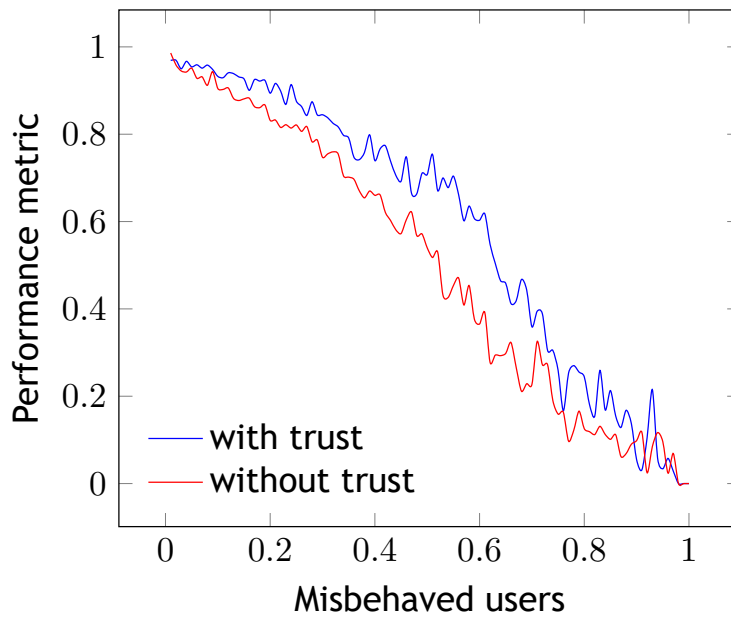


Figure 6.18: Effect on the performance of honest users from a rising number of malicious users in two scenarios, with and without trust.

Exp. 3 Purely malicious impact on performance

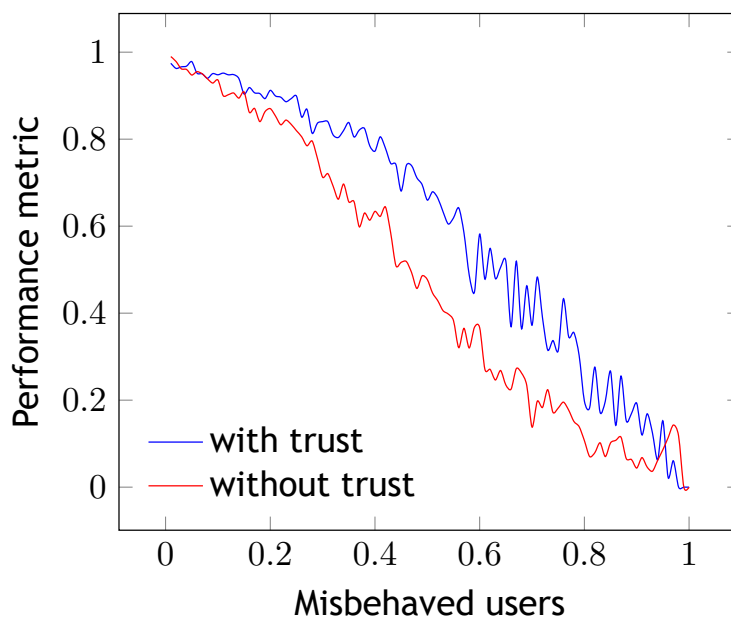


Figure 6.19: Effect on the performance of honest users from a rising number of purely malicious users in two scenarios, with and without trust.

6.5.5.2 Settings

In this experiment, we used a 512x512 region, with the number of users to increase from 50 to 500, what means that such region progressively gets more crowded; as a consequence, the corresponding server ends up getting overstretched, in particular in the case of OpenSimulator.

Taking into consideration that the number of interactions would increase from 1000 to 10000 (i.e., 1000 interactions per each 50 users), we end up having an average rate of 20 interactions per user over time. It was also assumed that the population inside the region had 4% of malicious users, but no other misbehaved users. This percentage of 4% of malicious users (i.e., 4 out of 100) is an attempt of representing the reality. The choice of malicious users is justified by the more consistent trust results obtained in the previous experiments.

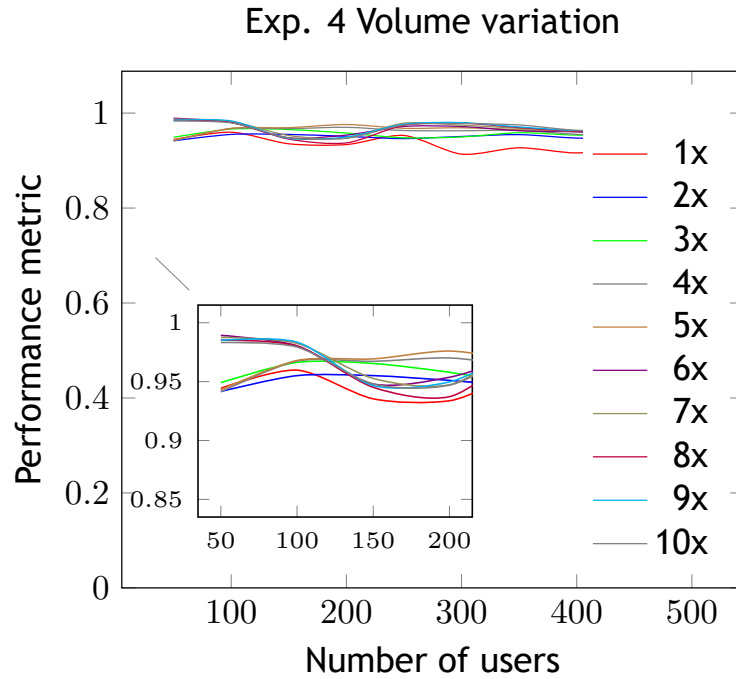


Figure 6.20: Effect on the performance of honest users from a rising number of users and interactions while keeping a 4% misbehaved presence.

6.5.5.3 Discussion

The graph pictured in Fig. 6.20 was produced from 100 datasets (u, i) (i.e., 100 files), where the number of users $u \in [50, 500]$ varies with increments of 50, and the number of interactions $i \in [1000, 10000]$ varies with increments of 1000. The results in Fig. 6.20 show that with 4% of malicious users, the West rate of success of honest users (cf. metric given by Eq. (6.19)) in their interactions with the entire population in the region is not directly affected by the volume of data considered. In fact, the results obtained are consistently above a success rate of 94%.

It is observed a higher fluctuation among results concerning the initial 5 scenarios (until 5000 interactions), but from there on there is no noticeable fluctuations in the obtained results. In short, the success rate ranges between 92% and 99% for a constant rate of 4% malicious users, no matter the size of the population in the region and the number of avatar-avatar interactions.

6.5.6 Experiment 5: Trust Modeling with Data of Higher Orders of Magnitude for a Population with Mixed Misbehaved Users

6.5.6.1 Description

This experiment is a more realistic variant of Exp. 4 because the population includes misbehaved users of different categories. In fact, in a virtual world, the probability of different users with different behaviors coexist is high. Therefore, the current experiment considers a population having a mix of misbehaved users, namely: malicious users, pure malicious users, and sybil users.

6.5.6.2 Settings

As in Exp. 4, we also used a 512x512 region populated with an increasing number of users in the range [50, 500], and an increasing number of interactions in the range [1000, 10000]. It was still assumed that the population inside the region had 4% of malicious users, 4% of pure malicious users, and 2% of sybil users.

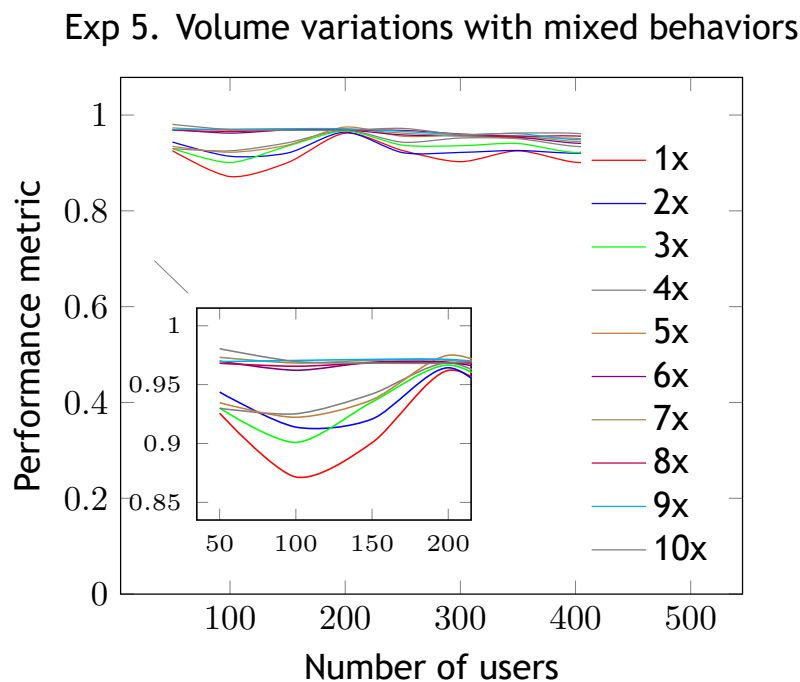


Figure 6.21: Impact of the volume variation in the performance of honest users keeping 10% of mixed misbehaved users.

6.5.6.3 Discussion

The results shown in Fig. 6.21 corroborate our expectations. They are similar to, but slightly worse than, the ones produced by Exp. 4. The upper bound of success rate in Exp. 5 (approx. 98%) is slightly lower than in Exp. 4 (approx. 99%), while the corresponding lower bound in Exp. 5 (approx. 85%) is clearly lower than the corresponding lower bound in Exp. 4 (approx. 92%). This is valid for populations with up to 500 users, but for populations with a higher number of users the lower bound tends to converge to the upper bound of success rate. This suggests that, in spite of a user directly interacts with a reduced number of other users in its AOI (area of interest), it is recommended that a user takes advantage of the entire population of its world game region to take decisions about the interactions established with others.

6.5.7 Experiment 6: Impact of Trust Computing Time

6.5.7.1 Description

In this experiment we address the impact of processing time on the usability of the trust model. More specifically, we address the implications of the delay incurred in evaluating the trust model on computer, i.e., the time necessary to get an opinion (or recommendation) from the trust network, in order to then support the trustor in its decision-making about the trustee.

It is clear that the admissible lag depends on the type of virtual world in question. For example, in a player-to-player fight taking place in WoW, a lag of 0.2 secs may be the admissible maximum, but a lag of 3 secs in SecondLife for trading activities seems to be reasonable for many. Thus, in Exp. 6, we use a time metric to assess the viability of the BFSDFS-SL trust model to cope with avatar-avatar interactions in real-time (i.e., in conformity with the pace of the virtual world).

6.5.7.2 Settings

In Exp. 6, we used the same setting as the one utilized in Exp. 4. That is, we used 10 populations in the range [50,500] that differ in 50 users from one to another, as well as a number of interactions between 1000 and 10000. As in Exp. 4, the percentage of malicious users was 4% for any population, though no other misbehaved have been considered in the simulation. As for the previous experiments, we used BFSDFS-SL trust model to evaluate trust in the interactions among users.

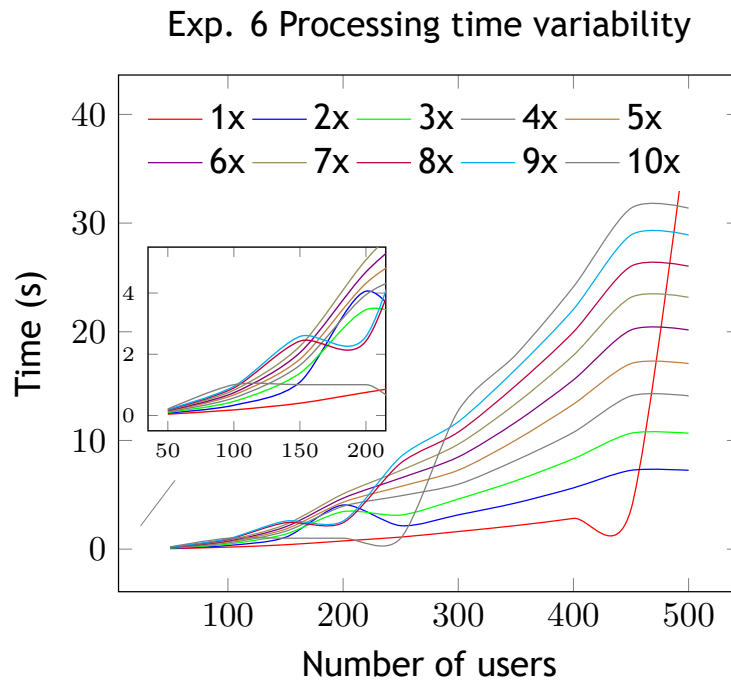


Figure 6.22: Effect of the trust computing time under different volume of interactions and users with a %4 constant rate of misbehaved users.

6.5.7.3 Discussion

A brief glance at Fig. 6.22 shows that, for a population with less than 100 users, it is feasible to embed trust in the decision-making of in-world users when they interact with each other, since trust system latency is less than a 1 second, that is, the time period used as reference for interactions without lagging, also called time window of usability.

For bigger populations, it is impracticable to use the BFSDFS-SL trust model, unless one uses parallel computing facilities and tools to speed up trust computations, or eventually other trust models [CG14], like EigenTrust [KSGM03], Travos [TPJL06] or [LDRL09]. Nevertheless, there seems more reasonable to only consider the avatars within the small area of each user Aol for interactions with boundaries determined by the `\shout` command used in virtual worlds.

6.6 Discussion

Let us now revisit the main research question put forward in the previous chapter[CGF16a]:

Q – Assuming that interaction data is available, how can in-world users (i.e., avatars) benefit from the data generated in the virtual world to sustain their trust decisions?

In order to respond to this grand question, we agreed that we had first to respond to the following five subsidiary questions:

Q1 – What kind of in-world data are available and how can they be collected?

Q2 – Can we turn in-world data gathered in the environment into a persistent computational trust representation?

Q3 – How can we derive trust to evaluate the trustability of an avatar even when no previous direct interaction with it took place in the past?

This question can be further detailed in two follow-up questions:

Q3.1 – How to derive a set of paths linking trustor and trustee from the existing trust network representation?

Q3.2 – How to determine a quantifiable trust value for a path linking trustor and trustee?

Q4 – Can we demonstrate the validity of our proposal?

Recall that in chapter 5 [CGF16a], we only addressed the main research question partially, because only the first two subsidiary research questions were responded properly. Those first two research questions have to do with collecting data tied to avatar-avatar interactions, and how they can be converted into a graph-based trust representation.

The methodology employed to address the first research question (Q1) was based on avatar-avatar interaction data collected from OpenSimulator actions/events. In regard to the second research question (Q2), we showed how to store collected data into OpenSimulator database, and afterwards processed and converted into a trust network representation, as necessary to be latter dealt with by our BFSDFS-SL model. In fact, it was demonstrated that avatar-avatar interaction data can be then converted into relevant trust information in the form of unidirectional, direct trust relationships between trustor and trustee. Recall that the conversion of trust relationships into trust opinions is accomplished in the triangle domain of subjective logic, and in conformity with the Eq. (6.9).

The purpose of the present chapter is to show how to reason on personal trust trees in order to allow a trustor come up with trust result about a given trustee in an automated manner. Such trust inference engine is based on subjective logic operators. To achieve that goal, we adopted specific methodologies to respond to the third, fourth and fifth research questions.

In respect to the third research question (Q3), we used BFS/DFS pathfinding together with subjective logic operators (i.e., discount and consensus operators) to derive indirect trust opinions from direct trust opinions, being thus it possible to combine individual trust networks into a personal trust tree, from which an user-impersonating avatar is able to formulate an opinion about another avatar even when they have not met or interacted before. Summing up, we used a BFSDFS-SL model at the core of our inference trust engine.

In order to address the fifth research question (Q4), we produced various scenarios within OpenSimulator with unequally-sized populations of avatars, distinct avatar behaviors (i.e., *honest*, *malicious*, *pure malicious*, and *sybil*), a varying number of interactions between avatars, as well as the impact of trust processing in the overall system performance. The results have shown that the trust model has a positive impact in the increasing of trustability among avatar-impersonated users within the virtual world. Note that the data privacy is *a priori* ensured by each user settings. That is, information concerning email, real name, address, and so forth is not shared in any way amongst users in our system. The only shared information is the trust network, but even so that depends on the user settings.

6.7 Summary

In this chapter we have shown that it is feasible to embed a trust model based on subjective logic in virtual worlds, as commonly humans do in their lives. For that purpose, we have used Opensim as a proof of concept and validation platform to confirm that direct trust relationships stored as trust networks can be used to help a trustor to build a trust assessment value about a trustee, in particular when they have never met before.

To achieve this objective, we had to win three challenges. Firstly, we had to manage a way of gathering avatar-avatar interaction data, and find a proper representation for them. Secondly, we had then to find a way to convert interactions into direct trust opinions, what was done using subjective logic. Thirdly, we had to use pathfinding techniques as a vehicle to trust inference, as needed when trustor has to make a trust decision about a trustee, no matter they have met before or not.

In the near future, we intend to improve the data gathering process in respect to avatar-avatar interactions, as well as relatively to interactions between other kind of entities (e.g., avatar-bank interactions, assuming that we have banks in the virtual world). Additionally, we intend to develop alternative pathfinding algorithms as a support for a better trust inference. We have also the idea that investigating further the user profiles (behaviors) may contribute to improve our BFSDFS-SL trust engine. Moreover, we intend to test the trust system with human users in order to make sure about its efficiency.

Chapter 7

Conclusions

This thesis sustains on the research work carried out in trust models for virtual worlds and massively multiplayer online games (VW/MMOGs). Briefly speaking, we can say that its main contribution lies in the design and development of a trust model for immersive environments, where avatars interact with each other in a similar way as humans in real life, using potentially their five senses: sight, hearing, touching, smell, and taste.

7.1 Context of the Research Work

It is important to recall that the research work underlying this thesis started after getting the understanding that VW/MMOGs lacked trust mechanisms in order to help users/players to make trust decisions about others. In fact, we noted that we can organize trust in layers and in conformity with the history of trust systems, namely infrastructure, services, and ultimately community. In modern terms, infrastructure trust has much to do with reliability of and trust in network nodes, while service trust is intimately related with online services as it is the case of eBay e-commerce system. On the other hand, community trust concerns social trust we may find in social networks and e-communities, including VW/MMOGs.

However, VW/MMOGs differ from other social networks, in that they are immersive worlds where avatars impersonating users/players tend to mimic humans in real life. That is, virtual trust in immersive worlds attempts to reproduce how humans trust in other humans. The challenge was then how to model trust (i.e., trust representation and its operators) for immersive virtual worlds, when there is no known computable trust model for humans in real life. Recall that such human trust model, in principle, has to take into consideration the five human senses, each one of which triggers very personal emotions that affect decision-making.

Obviously, we opted by a simplified trust model that mimics how humans behave during social interactions. In fact, we opted by considering two out of five senses (sight and hearing) in the avatar-avatar interactions, though the touch is always present in the interaction of each avatar with the environment; for example, when an avatar opens a door or picks up an object, the collision detection-based touch enters in action, i.e., we can say that there is an avatar-environment interaction. It is clear that touching may be considered in avatar-avatar interactions, but we decided not to use it in this research stage.

7.2 Research Questions

In order to validate the thesis statement expressed in Chapter 1, let us recall the main and subsidiary research questions put forward in Chapters 5 and 6.

Q – Assuming that interaction data is available, how can in-world users (i.e., avatars) benefit from the data generated in the virtual environment to sustain their trust decisions?

In order to respond to this main question, we use a bottom-up methodology that enables the collecting, aggregation and representation of trust-related information, from which a small set of operators produce a trust recommendation about any in-world user. Therefore, the stages of this bottom-up methodology lead us to subsidiary questions related to data collection, data aggregation, trust representation, and trust assessment, which are as follows:

Q1 – What kind of in-world data are available and how can they be collected?

Obviously, such data depend on the VW/MMOG at hand. Recall that OpenSimulator [Lop07] is open-source, so that we access to system-generated events directly. So, unlike to proprietary VW/MMOGs like WoW (World of Warcraft), we can easily filter out those events related with avatar-avatar interactions. As explained further ahead in Section 5.3, these interactions are those in which we are interested in, because they will allow us to establish trust relationships between avatars.

Q2 – Can we turn the in-world data gathered in the environment into a persistent computational trust representation?

We can respond positively to this question because we were able to build individual trust networks from avatar-avatar relationships (Section 5.4). These individual networks can be then combined together in order to build trusted opinions (Section 5.5) and trust networks (Section 5.6), which are later used to evaluate the trustworthiness of avatars from a personal point of view (Section 5.7).

Q3 – How can we derive trust to evaluate the trustability of an avatar even when no previous direct interaction with it took place in the past?

To respond to Q3, we employed the concept of extended individual trust network, which, as explained in Section 5.6, allows us to assemble successive individual trust networks as subtrees of a tree of trust in order to establish a trust path to the trustee avatar, no matter whether it is unknown or not for the trustor avatar. After finding such trust path using graph search methods, we use subjective logic operators to come up with a final trust value about the trustee.

Q4 – Can we demonstrate the validity of our proposal?

Q4 is addressed in Chapter 6. For that purpose, we built up various scenarios within OpenSimulator with a varying number of users and behaviors (i.e. honest, malicious, pure malicious, and sybil users), a varying number of interactions between users, as well

as the impact of trust processing in the overall system performance. These experiments show that embedding a trust system into a VW/MMOG brings us gains in trust evaluation accuracy, helping avatars/players to make better decisions in relation to others.

Summing up, and recalling the thesis statement:

Assuming that in-world data generated from avatar-avatar interactions can be employed to derive a trust representation for each individual user, will it be feasible to have an in-world trust assessment mechanism suitable to support and enhance users' trust decisions?

we can say the research work described in thesis responds positively to and validates the thesis statement above, in respect to the aforementioned research questions.

7.3 Contributions

The main achievements that have resulted from this research work are the following:

- a trust framework that consists of three layers, data sources, trust engine, and avatar-avatar interactions;
- a trust model based on the activity theory;
- a trust representation built upon a bottom-up methodology for collecting and aggregating data generated by avatar-avatar interactions;
- a real-time trust inference based on subjective logic operators and graph search algorithms.

The latter three contributions (i.e., interaction representation, trust representation, and trust inference) correspond to the three tiers of the trust engine.

7.4 Research Limitations and Future Work

In the research work carried out during the doctoral program, we have identified a number of research limitations that open a window for future work:

- *Data gathering.* Although other types of information sources could be used, we only collected/gathered data from in-world avatar-avatar interactions. Therefore, the gathering process does not take into consideration other types of interactions or additional information sources (e.g., reputation systems).
- *Trust representation.* The trust representation was built upon collected data, i.e., avatar-avatar interactions via chat and messaging, though other communication media (e.g., voice and facial expressions and micro expressions of avatars) might be used.

Enhancing Trustability in MMOGs Environments

- *Inference solution.* We used BFS/DFS graph search methods to construct the trust trees, largely because of real-time requirements in interactive MMOGs. We have not tried other solutions as the search was limited to the game region where the trustor stood, although we could consider other solutions (e.g., Dijkstra's, A*, and Floyd-Warshall search) for solving the *shortest path problem* between the trustor and trustee.
- *Preset behaviors.* We only considered preset behaviors to emulate/simulate human behaviors. Nevertheless, the experiments would benefit from a deployment consisting of human data generated from avatar-avatar interactions.

It is clear that these limitations will be instrumental for further research, in particular those concerning facial expressions, which are related to sight sensing.

Bibliography

- [AB16] Pallavi Agarwal and Neha Bhardwaj. A review on trust model in vehicular ad hoc network. *International Journal of Grid and Distributed Computing*, 9(4):325-334, 2016.
- [ABC⁺15] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. *Frontiers of Computer Science*, 9(2):280-296, 2015.
- [AD01] Christopher Alberts and Audrey Dorofee. An introduction to the octave method. *Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University*, 2001.
- [Adr] A. Adrian. Social engineering fundamentals. Available from: <http://www.symantec.com/connect/articles/social-engi-neering-fundamentals-part-ii-combat-strategies>.
- [Adr10] A. Adrian. Beyond grieving: Virtual crime. *Computer Law & Security Report*, 26:640-648, 2010.
- [AEG⁺10] Sibel Adali, Robert Escriva, Mark K Goldberg, Mykola Hayvanovych, Malik Magdon-Ismael, Boleslaw K Szymanski, William A Wallace, and Gregory Williams. Measuring behavioral trust in social networks. In *Proceedings of the Conference on Intelligence and Security Informatics (ISI)*, pages 150-152, Vancouver, BC Canada, 2010. IEEE, IEEE.
- [AG07] Donovan Artz and Yolanda Gil. A survey of trust in computer science and the semantic web. *Web Semantic*, 5(2):58-71, June 2007. Available from: <http://portal.acm.org/citation.cfm?id=1265608.1265746>.
- [AHC13] Do-sik An, Byong-lae Ha, and Gi-hwan Cho. A robust trust management scheme against the Malicious nodes in distributed P2P network. *International Journal of Security & Its Applications*, 7(3):317-326, 2013.
- [AK02] Paul S Adler and Seok-Woo Kwon. Social capital: Prospects for a new concept. *Academy of management review*, 27(1):17-40, 2002.
- [AKW⁺11] Muhammad Ahmad, Brian Keegan, Dmitri Williams, Jaideep Srivastava, and Noshir Contractor. Trust amongst rogues? a hypergraph approach for comparing clandestine trust networks in mmogs. In *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media ICWSM*, pages 8-pp, Barcelona, Spain, 2011. AAAI.
- [Ali97] Daniel G Aliaga. Virtual objects in the real world. *Communications of the ACM*, 40(3):49-54, 1997.
- [AP11] Stephen Atlas and Louis Putterman. Trust among the avatars: A virtual

- world experiment, with and without textual and visual cues. *Southern Economic Journal*, 78(1):63-86, 2011.
- [APS08] Leigh Achterbosch, Robyn Pierce, and Gregory Simmons. Massively multiplayer online role-playing games: the past, present, and future. *Computers in Entertainment (CIE)*, 5(4):9, 2008.
- [ARH00] Alfarez Abdul-Rahman and Stephen Hailes. Supporting trust in virtual communities. In *Proceedings of the 33rd Hawaii International Conference on System Sciences*, pages 9-pp, Hawaii, 2000. IEEE. Available from: <http://dl.acm.org/citation.cfm?id=820262.820322>.
- [ARJ09] Najwa Aaraj, Anand Raghunathan, and Niraj K. Jha. Analysis and design of a hardware/software trusted platform module for embedded systems. *Transactions in Embeded Computer Systems*, 8(1):81-831, January 2009.
- [Bai86] Annette Baier. Trust and antitrust. *Ethics*, 96(2):231-260, 1986.
- [Bai02] T. Bailey. On trust and philosophy. <http://137.108.238.28/trust/downloads/docs/ontrust.pdf>, 2002. Available from: http://www.open2.net/trust/on_trust/on_trust1.htm.
- [Bar03] Richard .A. Bartle. *Designing Virtual Worlds*. New Riders, San Francisco, California US, 2003.
- [BB04] S. Buchegger and J.-Y. Boudec. A robust reputation system for P2P and mobile ad-hoc networks. In *Proceedings of the 2nd Workshop on Economics of P2P Systems*, pages 1-6, Boston, MA, USA, June 2004. MIT Press.
- [BBC⁺08] D. Barosso, R. Bartle, C. Chazeran, M. de Zwart, J.M. Doumen, S. Gorniak, M. Kaźmierczak, M. Kaskenmaa, D. Benavente López, A. Martin, I. Naumann, R. Reynolds, J. Richardson, C. Rossow, A. Rywczyoska, and M. Thumann. Security and privacy in massively-multiplayer online games and social and corporate virtual worlds. Technical Report 1, European Union Agency for Network and Information Security (ENISA), Crete, November 2008.
- [BCRT08] Stephen C Bronack, Amy L Cheney, Richard E Riedl, and John H Tashner. Designing virtual worlds to facilitate meaningful communication. *Technical Communication*, 55(3):261-269, August 2008.
- [Bel08] Mark W. Bell. Toward a definition of virtual worlds. *Journal of Virtual Worlds Research*, 1(1):1-5, 2008.
- [Bew08] Glenn R. Bewsell. Online trust mechanisms: a domain study of on-line auctions. *Australasian Journal of Information Systems*, 15 (2):5-22, 2008.
- [BFL96] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Sympo-*

- sium on*, SP '96, pages 164-173, Washington, DC, USA, 1996. IEEE, IEEE Computer Society. Available from: <http://dl.acm.org/citation.cfm?id=525080.884248>.
- [BGRP01] Steve Benford, Chris Greenhalgh, Tom Rodden, and James Pycock. Collaborative virtual environments. *Communications of the ACM*, 44(7):79-85, 2001.
- [BHRS09] Sonja Bergsträber, Tomas Hildebrandt, Christoph Rensing, and Ralf Steinmetz. Virtual context based services for multiplayer online games to facilitate community participation. *Multimedia Tools Appl.*, 45(1-3):347-367, October 2009.
- [Bhu10] T. Bhuiyan. A survey on the relationship between trust and interest similarity in online social networks. *Journal of Emerging Technologies in Web Intelligence*, 2(4):291-299, 2010. Available from: <http://www.ojs.academypublisher.com/index.php/jetwi/article/viewArticle/0204291299>.
- [Bhu11] Touhid Bhuiyan. *Trust-based Automated Recommendation Making*. PhD thesis, Queensland University of Technology, Brisbane, Australia, 2011.
- [BJB⁺07] Jeffrey Bardzell, Markus Jakobsson, Shaowen Bardzell, Tyler Pace, Will Odom, and Aaron Houssian. Virtual worlds and fraud: Approaching cybersecurity in massively multiplayer online games. In *proceedings of the 2007 DiGRA International Conference: Situated Play*, pages 451-742, Tokyo, Japan, September 2007. The University of Tokyo.
- [BL12] Pierre Baldi and Crista Lopes. The universal campus: An open virtual 3-D world infrastructure for research and education. *ACM eLearn Magazine*, 2012(4):6, 2012.
- [BM07] Shane Balfe and Anish Mohammed. Final fantasy-securing on-line gaming with trusted computing. In *Proceedings of the International Conference on Autonomic and Trusted Computing*, pages 123-134, Banff, Canada, 2007. Springer.
- [BM14] Gregory Bedny and David Meister. *The Russian theory of activity: Current applications to design and learning*. Psychology Press, 2014.
- [BP98] Sergey Brin and Lawrence Page. The anatomy of a large-scale hypertextual web search engine. *Comput Networks Isdn*, 30(1):107-117, 1998.
- [BRDM11] Patricia Beatty, Ian Reay, Scott Dick, and James Miller. Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys*, 43(3):141-1446, April 2011.
- [BS16] Teofilo Branco, Jr. and Henrique Santos. What is missing for trust in the cloud computing? In *Proceedings of the 2016 ACM SIGMIS Conference*

- on Computers and People Research*, SIGMIS-CPR '16, pages 27-28, New York, NY, USA, 2016. ACM.
- [Bul13] SL Bulloch. Seeking construct validity in interpersonal trust research: A proposal on linking theory and survey measures. *Social indicators research*, 113(3):1289-1310, 2013. Query date: 2012-10-17. Available from: <http://www.springerlink.com/index/518M5H4614300881.pdf>.
- [CC12] K. Chang and J. Chen. A survey of trust management in WSNs, internet of things and future internet. *Transactions on Internet and Information Systems*, 6(1):5-23, 2012. Available from: http://www.dbpia.co.kr/view/ar_view.asp?arid=1784767.
- [CC13] Justin Clark-Casey. Transferring a virtual environment client session between independent OpenSimulator installations. In *Proceedings of The 5th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES'13)*, pages 1-3, Bournemouth, United Kingdom, September 11-13, 2013. IEEE Press.
- [CCA15] Jin-Hee Cho, Kevin Chan, and Sibel Adali. A survey on trust modeling. *ACM Computing Surveys (CSUR)*, 48(2):281-2840, October 2015.
- [CE15] Partheeban Chandrasekaran and Babak Esfandiari. Toward a testbed for evaluating computational trust models: experiments and analysis. *Journal of Trust Management*, 2(1):1-27, 2015.
- [CF98] Cristiano Castelfranchi and Rino Falcone. Principles of trust for mas: Cognitive anatomy, social importance, and quantification. In *Proceedings of the International Conference on Multi Agent Systems*, pages 72-79, Paris, France, 1998. IEEE, IEEE.
- [CG12] Rui Costa Cardoso and Abel Gomes. Security issues in massively multiplayer online games. In *Handbook of Research on Serious Games as Educational, Business and Research Tools*, chapter Security Issues in Massively Multiplayer Online Games, pages 290-314. IGI Global, Hershey, PA 17033, USA, igi global, 2012 edition, 2012.
- [CG14] Rui Costa Cardoso and Abel Gomes. Towards a trust framework for multi-user virtual environments. In Beniamino Murgante, Sanjay Misra, Ana Maria A.C. Rocha, Carmelo Torre, Jorge Gustavo Rocha, Maria Irene Falcão, David Taniar, Bernady O. Apduhan, and Osvaldo Gervasi, editors, *Proceedings of International Conference on Computational Science and Its Applications (ICCSA'14)*, volume 8579 of *Lecture Notes in Computer Science*, pages 754-768, Guimarães, Portugal, June 30 - July 3, 2014. Springer-Verlag.
- [CGF16a] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire. A user trust system for online games — part i: An activity theory approach for trust representa-

- tion. *IEEE Transactions on Computational Intelligence and AI in Games*, PP(99):1-1, 2016.
- [CGF16b] R. C. Cardoso, A. J. P. Gomes, and M. M. Freire. A user trust system for online games – part ii: A subjective logic approach for trust inference. *IEEE Transactions on Computational Intelligence and AI in Games*, PP(99):1-1, 2016.
- [CHL06] Kuan-Ta Chen, Polly Huang, and Chin-Laung Lei. Game traffic analysis: An mmorpg perspective. *Computer Networks*, 50(16):3002-3023, 2006.
- [CI06] SC Currall and AC Inkpen. On the complexity of organizational trust: a multi-level co-evolutionary perspective and guidelines for future research. In Akbar Zaheer Reinhard Bachmann, editor, *Handbook of Trust Research*, pages 235-246, UK, 2006. Edward Elgar Publishing Limited. Available from: <http://discovery.ucl.ac.uk/52416/>.
- [CKN⁺15] Federico Cerutti, Lance M Kaplan, Timothy J Norman, Nir Oren, and Alice Toniolo. Subjective logic operators in trust assessment: an empirical study. *Information Systems Frontiers*, 17(4):743-762, August 2015.
- [CKW03] Cynthia L. Corritore, Beverly Kracher, and Susan Wiedenbeck. On-line trust: concepts, evolving themes, a model. *Int J Hum-comput St*, 58(6):737-758, 2003. Trust and Technology. Available from: <http://www.sciencedirect.com/science/article/pii/S1071581903000417>.
- [CL16] Ryan E. Carlin and Gregory J. Love. Political competition, partisanship and interpersonal trust in electoral democracies. *British Journal of Political Science*, FirstView:1-25, January 2016. Available from: http://journals.cambridge.org/article_S0007123415000526.
- [CLPC08] Kuan-Ta Chen, Andrew Liao, Hsing-Kuo Kenneth Pao, and Hao-Hua Chu. Game bot detection based on avatar trajectory. In *Proceedings of the 7th International Conference on Entertainment Computing (ICEC'08)*, Lecture Notes in Computer Science, vol. 5309, pages 94-105, Pittsburgh, USA, September 25-27, 2008. Springer-Verlag.
- [CM02] Anirban Chakrabarti and G Manimaran. Internet infrastructure security: A taxonomy. *Network, IEEE*, 16(6):13-21, 2002.
- [CNP04] Augusto Celentano, Michele Nodari, and Fabio Pittarello. Adaptive interaction in web3d virtual worlds. In *Proceedings of the Ninth International Conference on 3D Web Technology*, Web3D '04, pages 41-50, New York, NY, USA, 2004. ACM.
- [CPK08] Hangbae Chang, Jong Hyuk Park, and Hongsuk Kang. The security system design in online game for u entertainment. In *Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on*, pages 1529-1533. IEEE, 2008.

- [CSC11] Jin-Hee Cho, Ananthram Swami, and Ing-Ray Chen. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 13(4):562-583, November 2011.
- [CSM⁺11] Filipe Caldeira, Thomas Schaberreiter, Edmundo Monteiro, Jocelyn Aubert, Paulo Simões, and Djamel Khadraoui. Trust based interdependency weighting for on-line risk monitoring in interdependent critical infrastructures. In *Proceedings of The 6th International Conference on Risk and Security of Internet and Systems (CRiSIS'11)*, pages 1-7, Timisoara, Romania, September 26-28, 2011. IEEE, IEEE Press.
- [CSMT02] George Cvetkovich, Michael Siegrist, Rachel Murray, and Sarah Tragesser. New information and social trust: Asymmetry and perseverance of attributions about hazard managers. *Risk analysis*, 22(2):359-367, 2002.
- [CYL13] Yung Kyun Choi, Sukki Yoon, and Heather P Lacey. Online game characters' influence on brand trust: Self-disclosure, group membership, and product type. *Journal of Business Research*, 66(8):996-1003, 2013.
- [CZDB11] Pawat Chomphosang, Ping Zhang, Arjan Durresi, and Leonard Barolli. Survey of trust based communications in social networks. In *Proceedings of 14th International Conference on Network-Based Information Systems (NBIS'11)*, pages 663-666, Tirana, Albania, September 7-9, 2011. IEEE Press. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6041991.
- [Dam08] Bruce Damer. Meeting in the ether: A brief history of virtual worlds as a medium for user-created events. *Journal of Virtual Worlds Research*, 1(1):1-17, 2008.
- [DC07] Edward Dieterle and Jody Clarke. Multi-user virtual environments for teaching and learning. In M. Pagani, editor, *Encyclopedia Multimedia Technology Networking*, volume 2, pages 1033-1044. Idea Group Inc., Pennsylvania, United States, 2007.
- [DCK16] Jens Dibbern, Wynne W. Chin, and Thomas Kude. The sourcing of software services: Knowledge specificity and the role of trust. *SIGMIS Database*, 47(2):36-57, June 2016.
- [Del03] Chrysanthos Dellarocas. The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Management science*, 49(10):1407-1424, 2003.
- [Deu58] Morton Deutsch. Trust and suspicion. *J Conflict Resolut*, 2(4):265-279, 1958.
- [DF11] Sara De Freitas. Serious virtual worlds: A scoping study. The Serious Games Institute, Coventry University, United Kingdom, 2011.

- [D'H00] Sim D'Hertefelt. Trust and the perception of security, 2000. Available from: <http://www.interactionarchitect.com/research/report20000103shd.htm>.
- [DH08] Farhad Daneshgar and Sharon Ho. Sociological factors affecting trust development in virtual communities. *International Journal of Networking and Virtual Organisations*, 5(1):51-63, December 2008.
- [DH12] Jean-Guillaume Dumas and Hicham Hossayni. Matrix powers algorithms for trust evaluation in public-key infrastructures. In *Proceedings of the 8th International Workshop on Security and Trust Management (STM)*, pages 129-144, Pisa, Italy, 2012. Springer, Springer.
- [DHJS04] T Dong-Huynh, N Jennings, and N Shadbolt. FIRE: An integrated trust and reputation model for open multi-agent systems. In *Proceedings of the 16th European Conference on Artificial Intelligence (ECAI)*, pages 18-22, Valencia, Spain, 2004. IOS Press.
- [DHMV14] Lynn Dombrowski, Gillian R Hayes, Melissa Mazmanian, and Amy Volda. E-government intermediaries and the challenges of access and trust. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 21(2):13, 2014.
- [DIG13] John David N. Dionisio, William G. Burns III, and Richard Gilbert. 3D virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*, 45(3):341-3438, July 2013.
- [Dix09] Alan Dix. *Human-Computer Interaction*, pages 1327-1331. Springer US, Boston, MA, liu, ling and özsü, m. tamer edition, 2009.
- [DL10] Barney Dalgarno and Mark JW Lee. What are the learning affordances of 3-D virtual environments? *British Journal of Educational Technology*, 41(1):10-32, 2010.
- [DP08] Steven B Davis and W Joseph Price. Security issues for third party games: Technical, business and legal perspectives. *Computer Law & Security Review*, 24(2):163-168, 2008.
- [DPJX12] Weiqi Dai, T. Paul Parker, Hai Jin, and Shouhuai Xu. Enhancing data trustworthiness via assured digital signing. *IEEE Transactions on Dependable and Secure Computing*, 9(6):838-851, 2012.
- [DYLL15] Xiaolin Du, Yunming Ye, Raymond YK Lau, and Yueping Li. Opinion-rings: Inferring and visualizing the opinion tendency of socially connected users. *Decision Support Systems*, 75:11-24, 2015.
- [dZ09] Melissa de Zwart. Piracy vs. control: Models of virtual world governance, and their impact on player and user experience. *Journal of Virtual Worlds Research*, 2(3):3-16, 2009.
- [EFK10] A Etang, D Fielding, and S Knowles. *Are Survey measures of Trust Cor-*

- related with Experimental Trust? Empirical Evidence from Cameroon.* (Department of Economics, University of Otago, Dunedin, South Island, New Zealand, 2010. Query date: 2012-10-17. Available from: <http://otago.ourarchive.ac.nz/handle/10523/1118>.
- [EHW13] Elisabetta Erriquez, Wiebe van der Hoek, and Michael Wooldridge. Building and using social structures: A case study using the agent ART testbed. *ACM Transactions on Intelligent Systems and Technology*, 4(2):251-2520, March 2013.
- [FG00] Giovanni RF Ferrari and Tom Griffith. *Plato: 'The Republic'*. Cambridge University Press, Cambridge, UK, 2000.
- [FGH11] M Firdhous, O Ghazali, and S Hassan. Trust and trust management in cloud computing: A survey. Technical report, Universiti Utara Malaysia, Kuala Lumpur, Malaysia, 2011.
- [FGM11] Javier G. Marín-Blázquez Félix Gómez Mármol, Gregorio Martínez Pérez. Meta-tacs: A trust model demonstration of robustness through a genetic algorithm. *Intelligent Automation and Soft Computing*, 17(1):41-59, 2011.
- [Fit91] Melvin Fitting. Kleene's logic, generalized. *Journal of Logic and Computation*, 1(6):797-810, December 1991.
- [FKM⁺05] Karen K. Fullam, Tomas B. Klos, Guillaume Muller, Jordi Sabater, Andreas Schlosser, Zvi Topol, K. Suzanne Barber, Jeffrey S. Rosenschein, Laurent Vercoeur, and Marco Voss. A specification of the agent reputation and trust (art) testbed: Experimentation and competition for trust in agent societies. In *Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems*, AAMAS '05, pages 512-518, New York, NY, USA, 2005. ACM.
- [Fre95] Maximina M. Freire. A socio-cultural/semiotic interpretation of inter-communication mediated by computers. In *Proceedings of International Conference on L.S. Vygotsky and the Contemporary Human Sciences*, Moscow, Russia, September 5-8, 1995.
- [FSG⁺14] Diogo AB Fernandes, Liliana FB Soares, João V Gomes, Mário M Freire, and Pedro RM Inácio. Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2):113-170, 2014.
- [Fuk95] Francis Fukuyama. *Trust: The social virtues and the creation of prosperity*. Free Press, New York, USA, 1995.
- [GA07] Yolanda Gil and Donovan Artz. Towards content trust of web resources. *Web Semant.*, 5(4):227-239, December 2007.
- [Gam88] Diego Gambetta. *Trust: Making and breaking cooperative relations*. Basil

Blackwell Ltd., Oxford, UK, 1988.

- [GBL⁺15] Jones Granatyr, Vanderson Botelho, Otto Robert Lessing, Edson Emílio Scalabrin, Jean-Paul Barthès, and Fabrício Enembreck. Trust and reputation models for multiagent systems. *ACM Comput. Surv.*, 48(2):271-2742, October 2015.
- [GH11] Manish Gupta and Jiawei Han. Heterogeneous network-based trust analysis: A survey. *ACM SIGKDD Explorations Newsletter*, 13(1):54-71, August 2011. Available from: <http://dl.acm.org/citation.cfm?id=2031341>.
- [GM12] Kannan Govindan and Prasant Mohapatra. Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*, 14(2):279-298, May 2012. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5770276.
- [GMMPGS09a] F G Mármol, Gregorio Martínez Pérez, and Antonio F. Gómez Skarmeta. TACS, a trust model for P2P networks. *Wireless Personal Communications*, 51(1):153-164, October 2009.
- [GMMPGS09b] Félix Gómez Mármol, Gregorio Martínez Pérez, and Antonio F. Gómez Skarmeta. TACS, a trust model for P2P networks. *Wireless Personal Communications*, 51(1):153-164, October 2009.
- [GOG13] Nurit Gal-Oz and Ehud Gudes. Trust and reputation in and across virtual communities. In *Proceedings of the 16th International Conference on Extending Database Technology, EDBT '13*, pages 769-772, New York, NY, USA, 2013. ACM.
- [Gol05] Jennifer Ann Golbeck. *Computing and applying trust in web-based social networks*. PhD thesis, University of Maryland, College Park, Maryland, USA, 2005. AAI3178583.
- [Gol09] Jennifer Golbeck. Trust and nuanced profile similarity in online social networks. *Transactions on Web*, 3(4):121-1233, September 2009.
- [GS00] Tyrone Grandison and Morris Sloman. A survey of trust in internet applications. *IEEE Communications Surveys & Tutorials*, 3(4):2-16, 2000.
- [Gul95] Ranjay Gulati. Does familiarity breed trust? the implications of repeated ties for contractual choice in alliances. *Academy of management journal*, 38(1):85-112, 1995.
- [Har14] Phil Harrison. Selective interactive mapping of real-world objects to create interactive virtual-world objects, December 2014. US Patent 8,902,227.
- [HCH07] F. K. Hussain, E. Chang, and O. K. Hussain. State of the art review of the existing pageranktm based algorithms for trust computation. In *Proceedings of the Second International Conference on Systems and Networks*

- Communications (ICSNC'2007)*, pages 1-7, Cap Esterel, French Riviera, France, August 2007. IARIA.
- [Heg13] Florian Heger. *Scalable Propagation of Continuous Actions in Peer-to-Peer-based Massively Multiuser Virtual Environments: The Continuous Events Approach*. PhD thesis, University of Mannheim, Germany, April 2013.
- [Het98] Marc J Hetherington. The political relevance of political trust. *American political science review*, 92(04):791-808, 1998.
- [HHJ08] Guan Yu Huang, Shun Yun Hu, and Jehn Ruey Jiang. Scalable reputation management with trustworthy user selection for P2P MMOGs. *International Journal of Advanced Media and Communication*, 2(4):380-401, December 2008.
- [HHRM12] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries, and Max Mühlhäuser. Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications*, 1(1):1, 2012. Query date: 2012-10-17.
- [HJS04] T Dong Huynh, Nicholas R Jennings, and N Shadbolt. Developing an integrated trust and reputation model for open multi-agent systems. In *Proceedings of the 7th International Workshop on Trust in Agent Societies*, pages 65-74, New York, USA, 2004. Springer.
- [HJS06] Trung Dong Huynh, Nicholas R. Jennings, and Nigel R. Shadbolt. Certified reputation: How an agent can trust a stranger. In *Proceedings of the Fifth International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS '06*, pages 1217-1224, New York, NY, USA, 2006. ACM.
- [HL98] John D Howard and Thomas A Longstaff. A common language for computer security incidents. *Sandia National Laboratories*, 1998.
- [HLL10] Chien-Lung Hsu, Chia-Chang Liu, and Yuan-Duen Lee. Effect of commitment and trust towards micro-blogs on consumer behavioral intention: A relationship marketing perspective. *International Journal of Electronic Business Management*, 8(4):292, 2010.
- [HM07] Greg Hoglund and Gary McGraw. *Exploiting online games: cheating massively distributed systems*. Addison-Wesley Professional, 2007.
- [HMB03] Zayd Hendricks, Gary Marsden, and Edwin Blake. A meta-authoring tool for specifying interactions in virtual reality environments. In *Proceedings of The 2nd International Conference on Computer Graphics, Virtual Reality, Visualization and Interaction in Africa (AFRIGRAPH'03)*, pages 171-180, Cape Town, South Africa, February 3-5, 2003. ACM, ACM Press.
- [HN13] Jingwei Huang and David M Nicol. Trust mechanisms for cloud comput-

- ing. *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1):1, 2013.
- [Hof02] Aaron M Hoffman. A conceptualization of trust in international relations. *European Journal of International Relations*, 8(3):375-401, 2002.
- [Hos95] Larue Tone Hosmer. Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review*, 20(2):379-403, 1995. april.
- [HR13] Shuk Ying Ho and Alex Richardson. Trust and distrust in open source software development. *Journal of Computer Information Systems*, 54(1):84-93, 2013.
- [HS13] A Hammam and S. Senbel. A trust management system for ad-hoc mobile clouds. In *Proceedings of 8th International Conference on Computer Engineering Systems (ICCES)*, pages 31-38, Ain Shams University, November 2013. IEEE.
- [HSRF95] Will Hill, Larry Stead, Mark Rosenstein, and George Furnas. Recommending and evaluating choices in a virtual community of use. In *Proceedings of The ACM Conference on Human Factors in Computing Systems (CHI'95)*, pages 194-201, Denver, Colorado, USA, May 7-11, 1995. ACM Press/Addison-Wesley Publishing Co.
- [HSS⁺12] Florian Heger, Gregor Schiele, R Suselbeck, Laura Itzel, and Christian Becker. Scalability in peer-to-peer-based mmves: The continuous events approach. In *Proceedings of The 2012 IEEE Consumer Communications and Networking Conference (CCNC'12)*, pages 629-633, Planet Hollywood, Las Vegas, USA, January 14-17, 2012. IEEE, IEEE Press.
- [Hum08] Sal M. Humphreys. Ruling the virtual world. governance in massively multiplayer online games. *European Journal of Cultural Studies*, 11(2):149-171, April 2008. Available from: <http://eprints.qut.edu.au/13328/>.
- [Hwa14] Yujong Hwang. Understanding the different influences of online trust on loyalty by risk takers and avoiders. *International Journal of Human-Computer Interaction*, 30(12):977-984, 2014.
- [HZ08] Jiankun Hu and Fabio Zambetta. Security issues in massive online games. *Security and Communication Networks*, 1(1):83-92, 2008.
- [HZNR07] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attacks on reputation systems. Technical Report 07-0123, Purdue University, 2007.
- [HZNR09] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation systems. *ACM Comput. Surv.*, 42(1):11-131, December 2009.

- [IL07] Cynthia E Irvine and Karl Levitt. Trusted hardware: Can it be trustworthy? In *Proceedings of the 44th annual Design Automation Conference, DAC '07*, pages 1-4, New York, NY, USA, 2007. ACM, ACM.
- [(IN11] Tech Report (INFSO). Trustworthy ICT research in FP7. Technical report, European Commission, Information Society and Media Directorate-General (DG INFSO), Information Society and Media Directorate-General (DG INFSO) Unit F5 Trust and Security unit B-1049 Brussels, 2011. Available from: http://cordis.europa.eu/fp7/ict/security/home_en.html.
- [Jal06] Janne Jalava. Trust as a decision. Technical report, University of Helsinki, 2006. Available from: <http://ethesis.helsinki.fi/julkaisut/val/sospo/vk/jalava/trustasa.pdf>.
- [JB08a] Francis L. Jeffries and Thomas E. Becker. Trust, norms, and cooperation: Development and test of a simplified model. *Journal of Behavioral and Applied Management*, 19(3):316-336, 2008.
- [JB08b] Audun Jøsang and Touhid Bhuiyan. Optimal trust network analysis with subjective logic. In *Proceedings of The 2nd International Conference on Emerging Security Information, Systems and Technologies, (SECURWARE'08)*, pages 179-184, Cap Esterel, France, August 25-31, 2008. Second International Conference SECURWARE '08, IEEE Press.
- [JED⁺03] Alex Jarett, Jon Estanislao, Elinka Dunin, Jannifer MacLean, Brian Robbins, David Rohrl, John Welch, and Jeferson Valadares. Igda online games white paper. *International Game Developers Association*, 2, 2003.
- [JGK06] Audun Jøsang, Elizabeth Gray, and Michael Kinatader. Simplification and analysis of transitive trust networks. *Web Intelligence and Agent Systems: An International Journal*, 4(2):139-161, April 2006. Available from: <http://dl.acm.org/citation.cfm?id=1239776.1239778>.
- [JHJ10] Wang Jin and Sun Huai-Jiang. A novel subjective logic for trust management. *Journal of Computer Research and Development*, 47(1):140-146, 2010.
- [JHP06] A. Jøsang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. In Vladimir Estivill-Castro and Gillian Dobbie, editors, *Proceedings of the 29th Australasian Computer Science Conference (ACSC'06)*, volume 48 of ACSC '06, pages 85-94, Hobart, Tasmania, Australia, January 16-19, 2006. Australian Computer Society, Inc. Available from: <http://dl.acm.org/citation.cfm?id=1151699.1151710>.
- [JHSMT13] David Jelenc, Ramón Hermoso, Jordi Sabater-Mir, and Denis Trček. Decision making matters: A better way to evaluate trust models. *Knowledge-Based Systems*, 52:147-164, November 2013.

- [JI02] Audun Jøsang and Roslan Ismail. The beta reputation system. In *Proceedings of the 15th Bled Electronic Commerce Conference*, volume 5, pages 2502-2511, Bled, Slovenia, 2002. University of Maribor.
- [JIB07] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618-644, March 2007.
- [Jø97] Audun Jøsang. Artificial reasoning with subjective logic. In A. Nayak and M. Pagnucco (eds.), editors, *Proceedings of The 2nd Australian Workshop on Commonsense Reasoning*, pages 1-17, Perth, Australia, December 1-1, 1997. Australian Artificial Intelligence Institute.
- [Joh74] David W Johnson. Communication and the inducement of cooperative behavior in conflicts: A critical review. *Communications Monographs*, 41(1):64-78, 1974.
- [Jøs13] Audun Jøsang. *Subjective Logic*. Book Draft 18 Feb, Norway, 2013. Available from: http://folk.uio.no/josang/papers/subjective_logic.pdf.
- [JP05] Audun Jøsang and Simon Pope. Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43*, APCCM '05, pages 59-68, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc., Australian Computer Society, Inc. Available from: <http://dl.acm.org/citation.cfm?id=1082276.1082284>.
- [Kaa99] Max Kaase. Interpersonal trust, political trust and non-institutionalised political participation in western Europe. *West European Politics*, 22(3):1-21, 1999.
- [KC10] Reid Kerr and Robin Cohen. Treet: The trust and reputation experimentation and evaluation testbed. *Electronic Commerce Research*, 10(3-4):271-290, 2010.
- [KD16] Mukesh Kumar and Kamlesh Dutta. LDAt: Lftm based data aggregation and transmission protocol for wireless sensor networks. *Journal of Trust Management*, 3(1):1-20, 2016.
- [KGS12] K Kilteni, R Groten, and M Slater. The sense of embodiment in virtual reality. *Presence*, 21(4):373-387, November 2012.
- [KHZF05] M Kosfeld, M Heinrichs, P Zak, and U Fischbacher. Oxytocin increases trust in humans. *Nature*, 435:673-676, 2005.
- [Koi07] E Koivisto. Mobile games 2010, url: <http://research.nokia.com/tr/nrc-tr-2007-011.pdf>. Accessed July, 15:2007, 2007.
- [Køi11] Geir M Køien. Reflections on trust in devices: An informal survey

- of human trust in an internet-of-things context. *Wireless Personal Communications*, 61(3):495-510, 2011. Available from: <http://www.springerlink.com/index/Q7J0651532352H68.pdf>.
- [Kou12] Farinaz Koushanfar. *Hardware Metering: A Survey*, pages 103-122. Springer New York, New York, NY, tehranipoor, mohammad and wang, cliff edition, 2012.
- [Kru06] Karl Krukow. *Towards a theory of trust for the global ubiquitous computer*. Doctoral disseration, University of Aarhus, Denmark, 2006.
- [KSGM03] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The EigenTrust algorithm for reputation management in P2P networks. In *Proceedings of The 12th International World Wide Web Conference (WWW'03)*, pages 640-651, Budapest, Hungary, May 20-24, 2003. ACM Press.
- [LA98] Raph Levien and Alexander Aiken. Attack resistant trust metrics for public key certification. In *Proceedings of the 7th Conference on USENIX Security Symposium - Volume 7, SSYM'98*, pages 18-18, Berkeley, CA, USA, January 1998. USENIX Association. Available from: <http://dl.acm.org/citation.cfm?id=1267549.1267567>.
- [LCCL11] Yeng-Ting Lee, Kuan-Ta Chen, Yun-Maw Cheng, and Chin-Laung Lei. World of warcraft avatar history dataset. In *Proceedings of the Second Annual ACM Conference on Multimedia Systems*, pages 1-6, San Jose, CA, USA, Feb 2011. ACM.
- [LDRL09] Xin Liu, Anwitaman Datta, Krzysztof Rzadca, and Ee-Peng Lim. StereoTrust: a group based personalized trust model. In *Proceedings of The 18th ACM Conference on Information and Knowledge Management (CIKM'09)*, CIKM '09, pages 7-16, Hong Kong, China, November 2-6, 2009. ACM Press.
- [Lev04] Raph Levien. *Attack resistant trust metrics for public key certification*. PhD thesis, University of Berkeley, 2004.
- [LJL⁺15] Shixi Liu, Cuiqing Jiang, Zhangxi Lin, Yong Ding, Rui Duan, and Zhicai Xu. Identifying effective influencers based on trust for electronic word-of-mouth marketing: A domain-aware approach. *Information Sciences*, 306:34-52, 2015.
- [Lju08] Alexander Ljung. People profiles and trust: on interpersonal trust in web-mediataed social spaces. Master's thesis, School of Media Technology School of Technology, CSC SE-100 44 Stockholm, Sweden, 2008.
- [LLF09] Junhai Luo, Xue Liu, and Mingyu Fan. A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Comput. Netw.*, 53(14):2396-2407, September 2009.

- [LLJ⁺11] Yining Liu, Keqiu Li, Yingwei Jin, Yong Zhang, and Wenyu Qu. A novel reputation computation model based on subjective logic for mobile ad hoc networks. *Future Generation Computer Systems*, 27(5):547-554, May 2011.
- [LLYY09] Gehao Lu, Joan Lu, Shaowen Yao, and Yau Jim Yip. A review on computational trust models for multi-agent systems. *The open information science journal*, 2:18-25, 2009.
- [LM54] P. F. Lazarsfeld and R. K. Merton. Friendship as a social process: A substantive and methodological analysis. *Freedom and Control in Modern Society*, 18:18-66, 1954.
- [Lop07] Cristina Lopes. OpenSimulator, 2007. Available from: <http://opensimulator.org>.
- [LT01] Matthew KO Lee and Efraim Turban. A trust model for consumer internet shopping. *International Journal of electronic commerce*, 6(1):75-91, 2001.
- [LTW10] Wei Liu, Yang-Bin Tang, and Huai-Min Wang. Personalized reputation model in cooperative distributed systems. In *Proceedings of The 16th International Conference on Parallel and Distributed Systems (ICPADS'10)*, pages 740-745, Shanghai, China, December 8-10, 2010. IEEE, IEEE Press.
- [Luh79] Niklas Luhmann. *Trust and Power*. Chichester Wiley, New York, US, 1979.
- [Luh00] Niklas Luhmann. *Familiarity, Confidence, Trust: Problems and Alternatives*, volume Trust: Making and Breaking Cooperative Relations, pages 94-107. Electronic edition, Department of Sociology, University of Oxford,, Department of Sociology, University of Oxford, gambetta, diego (ed.) edition, 2000. Available from: <http://www.sociology.ox.ac.uk/papers/luhmann94-107.pdf>.
- [Lur81] A R Luria. *The working brain*. Basic Books, 1981.
- [LWH13] Paul Benjamin Lowry, David W. Wilson, and William L. Haig. A picture is worth a thousand words: Source credibility theory applied to logo and website design for heightened credibility and consumer trust. *International Journal of Human-Computer Interaction*, 30(1):63-93, November 2013.
- [Mac07] M. Macedonia. Generation 3D: Living in virtual worlds. *Computer*, 40(10):99-101, October 2007.
- [Mar94] Stephen Paul Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, Department of Computing Science and Mathematics, University of Stirling, United Kingdom, June 1994. Available from: <http://citeseer.ist.psu.edu/198394.html>; <http://www.iit>.

nrc.ca/~steve/pubs/Trust/PhD/Trust.ps.gz.

- [Mas07] Paolo Massa. *A survey of trust use and modeling in real online systems*, pages 51-83. IGI Global, Hershey, PA , USA, 2007.
- [McL11] Carolyn McLeod. Trust. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, Stanford, CA, United States, fall 2015 edition, 2011. Available from: <http://plato.stanford.edu/archives/spr2011/entries/trust/>.
- [MCR12] Rodger Morrison, Casey G. Cegielski, and R. Kelly Rainer. Trust, avatars, and electronic communications: implications for e-learning. *Journal of Computer Information Systems*, 53(1):80-89, Fall 2012.
- [MDH02] N. L. McKnight D. H., Chervany. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *Int J Electron Comm*, 6(2):35-59, 2002. Trust ONLINE E-commerce.
- [Med12] A Medic. Survey of computer trust and reputation models the literature overview. *International Journal of Information*, 2:254-275, 2012.
- [MGM06] Christian Monch, Gisle Grimen, and Roger Midtstraum. Protecting online games against cheating. *Netgames'06*, pages 1-11, October 2006.
- [MH94] Robert M Morgan and Shelby D Hunt. The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3):20-38, 1994. Available from: <http://www.jstor.org/stable/1252308>.
- [MH07] Gary McGraw and Greg Hoglund. Online games and security. *Security & Privacy, IEEE*, 5(5):76-79, 2007.
- [MMBP12] G. Mármol, G. Marín-Blázquez, and M. Pérez. Lftm linguistic fuzzy trust mechanism for distributed networks. *Concurrency and Computation: Practice and Experience*, 24(17):2007-2027, 2012.
- [MMG⁺08] Brian E Mennecke, David McNeill, Matthew Ganis, Edward M Roche, David A Bray, Benn Konsynski, Anthony M Townsend, and John Lester. Second life and other virtual worlds: A roadmap for research. *Communications of the Association for Information Systems*, 22(20):371-388, 2008.
- [MMH02] Lik Mui, Mojdeh Mohtashemi, and Ari Halberstadt. A computational model of trust and reputation. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, pages 2431-2439, Big Island, Hawaii, January 7-10, 2002. IEEE, IEEE Press.
- [Mom10] Mohammad Momani. Trust models in wireless sensor networks: A survey. In Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki, and Dhinaharan Nagamalai, editors, *Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Chennai*,

India, July 23-25, 2010. Proceedings, pages 37-46, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

- [MP09] Félix Gómez Mármol and Gregorio Martínez Pérez. Security threats scenarios in trust and reputation models for distributed systems. *Computers & Security*, 28(7):545-556, 2009.
- [MP10] Félix Gómez Mármol and Gregorio Martínez Pérez. *State of the Art in Trust and Reputation Models in P2P networks*, pages 761-784. Springer US, Boston, MA, 2010.
- [MP11a] Félix Gómez Mármol and Gregorio Martínez Pérez. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication systems*, 46(2):163-180, February 2011.
- [MP11b] Félix Gómez Mármol and Gregorio Martínez Pérez. Trust and reputation models comparison. *Internet Research*, 21(2):138-153, 2011.
- [MP12] Félix Gómez Mármol and Gregorio Martínez Pérez. Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, 35(3):934-941, 2012.
- [MS04] Michael E Maximilien and Munindar P Singh. Toward autonomic web services trust and selection. In *Proceedings of the 2nd International Conference on Service Oriented Computing, ICSOC'04*, pages 212-221, New York, NY, USA, 2004. ACM Press.
- [MSS14] René Mayrhofer, Hedda R. Schmidtke, and Stephan Sigg. Security and trust in context-aware applications. *Personal Ubiquitous Computing*, 18(1):115-116, January 2014.
- [MT11] Bill McEvily and Marco Tortoriello. Measuring trust in organisational research: Review and recommendations. *Journal of Trust Research*, 1(1):23-63, 2011.
- [NCD⁺10] Seetharam Narasimhan, Rajat Subhra Chakraborty, Dongdong Du, Somnath Paul, Francis G Wolff, Christos A Papachristou, Kaushik Roy, and Swarup Bhunia. Multiple-parameter side-channel analysis: A non-invasive hardware trojan detection approach. In *Proceedings of the 3rd International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 13-18, Anaheim Convention Center, Anaheim, CA, 2010. IEEE.
- [ND05] Sylvie Noel and Sarah Dumoulin. Cheaters, resource farmers, ninja looters, and gankers: If we make collaborative virtual environments more like games, should our users be worried? In *Proceedings of the 9th European Conference on Computer-Supported Cooperative Work, Workshop on Computer Games and CSCW (ECSCW2005)*, pages XX-XX, Paris, France, September 2005. Springer.

- [Net06] Arnoštka Netrvalová. *Modelling and Simulation of Trust Evolution*. PhD thesis, University of West Bohemia in Pilsen, Department of Computer Science and Engineering, 2006. Available from: <http://www.kiv.zcu.cz/~netrvalo/phd/rigo.pdf>.
- [Nib79] G. H. Nibaldi. Technical evaluation criteria for trusted computer systems. Technical report, MITRE, 1979.
- [Noo10] AK Noor. Emerging cae technologies and their role in future ambient intelligence environments. *Central European Journal of Engineering*, 1(1):2-8, 2010. Query date: 10-01-2011. Available from: <http://www.springerlink.com/index/B03N746W81521654.pdf>.
- [NSB06] Cong Duc Nguyen, Farzad Safaei, and Paul Boustead. Optimal assignment of distributed servers to virtual partitions for the provision of immersive voice communication in massively multiplayer games. *Computer Communications*, 29(9):1260-1270, 2006. Query date: 31-01-2011. Available from: <http://linkinghub.elsevier.com/retrieve/pii/S0140366405003762>.
- [NU10] Zeinab Noorian and Mihaela Ulieru. The state of the art in trust and reputation systems: A framework for comparison. *Journal of Theoretical and Applied Electronic Commerce Research*, 5(2):97-117, 2010.
- [NV12] PhilipJ. Nickel and Krist Vaesen. Risk and trust. In Sabine Roeser, Rafaela Hillerbrand, Per Sandin, and Martin Peterson, editors, *Handbook of Risk Theory*, pages 857-876. Springer Netherlands, Delft, Netherlands, 2012.
- [OCB12] Mawloud Omar, Yacine Challal, and Abdelmadjid Bouabdallah. Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. *J. Network and Computer Applications*, 35(1):268-286, 2012. Available from: <http://www.sciencedirect.com/science/article/pii/S1084804511001767>.
- [ORMCB12] Gema Bello Orgaz, María D. R-Moreno, David Camacho, and David F. Barro. Clustering avatars behaviours from virtual worlds interactions. In *Proceedings of The 4th International Workshop on Web Intelligence & Communities (WI&C'12)*, pages 41-47, Lyon, France, April 16-16, 2012. ACM, ACM Press.
- [PAS13] Ilung Pranata, Rukshan Athauda, and Geoff Skinner. Modeling decentralized reputation-based trust for initial transactions in digital environments. *ACM Transactions on Internet Technology*, 12(3):81-835, May 2013.
- [Pat02] Andrew S. Patrick. Building trustworthy software agents. *Ieee Internet Comput*, 6(6):46-53, 2002. Available from: <http://www.computer.org/internet/ic2002/w6046abs.htm>.

- [Pat07] Jigar Patel. *A trust and reputation model for agent-based virtual organisations*. PhD thesis, University of Southampton, 2007.
- [Pea13] Siani Pearson. Privacy, security and trust in cloud computing. In Siani Pearson and George Yee, editors, *Privacy and Security for Cloud Computing*, pages 3-42. Springer, London, 2013.
- [Per99] R Perlman. An overview of pki trust models. *Ieee Network*, 13(6):38-43, November 1999.
- [Per09] A. Perry. Online games. In (Ed.) McQuade, S. C. III, editor, *Encyclopedia of cybercrime*, pages 79-81. Greenwood Press, 2009.
- [PK08] Stefano De Paoli and Aphra Kerr. Conceptualizing trust: a literature review. *NIRSA Working Paper Series*, June-August:1-29, 2008.
- [PLC08] Seong-Soo Park, Jong-Hyouk Lee, and Tai-Myoung Chung. Cluster-based trust model against attacks in ad-hoc networks. *Third 2008 International Conference on Convergence and Hybrid Information Technology, Vol 1, Proceedings*, pages 526-532, 2008.
- [PMD97] Joseph P. Cannon Patricia M. Doney. An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, 61(2):35-51, 1997. Available from: <http://www.jstor.org/stable/1251829>.
- [PMW13] Sachar Paulus, Nazila Gol Mohammadi, and Thorsten Weyer. Trustworthy software development. In *Proceedings of The IFIP International Conference on Communications and Multimedia Security*, pages 233-247, Magdeburg, Germany, 2013. Springer.
- [PNJd15] Thao P Nguyen and Brian J d'Auriol. Estarmom: Extendable simulator for trust and reputation management in online marketplaces. In *Proceedings of the ASE Conference on BigData/SocialInformatics/PAS-SAT/BioMedCom*, pages 1-10, Harvard University, Cambridge Pennsylvania, 2015. Academy of Science and Engineering.
- [PRMSL⁺09] Paul Paul R. Messinger, Eleni Stroulia, Kelly Lyons, Run Niu, Kristen Smirnov, and Stephen Perelgut. Virtual worlds – past, present, and future: New directions in social computing. *Decision Support Systems*, 47(3):204-228, 2009.
- [PSA12] Ilung Pranata, Geoff Skinner, and Rukshan Athauda. A holistic review on trust and reputation management systems for digital environments. *International Journal of Computer and Information Technology*, 1(1):44-53, September 2012.
- [PSM13] Isaac Pinyol and Jordi Sabater-Mir. Computational trust and reputation models for open multi-agent systems: a review. *Artif Intell Rev*, 40(1):1-25, 2013.

- [Qui68] R. Quillian. Semantic memory. In *Semantic Information Processing*, pages 227-270, Boston, MA, USA, 1968. MIT Press.
- [Rai00] Maria Antonietta Raimondo. The measurement of trust in marketing studies: a review of models and methodologies. In *Proceedings of the 16th IMP conference*, pages XX-XX, Bath, UK, 2000. Citeseer, XXX.
- [RCS⁺10] Rabindra A. Ratan, Jae Eun Chung, Cuihua Shen, Dmitri Williams, and Marshall Scott Poole. Schmoozing and smiting: Trust, social institutions, and communication patterns in an MMOG. *Journal of Computer-Mediated Communication*, 16(1):93-114, 2010.
- [RHJ04] Sarvapali D Ramchurn, Dong Huynh, and Nicholas R Jennings. Trust in multi-agent systems. *The Knowledge Engineering Review*, 19(01):1-25, 2004.
- [RK05] Sini Ruohomaa and Lea Kutvonen. Trust management survey. In Peter Herrmann, Valérie Issarny, and Simon Shiu, editors, *Proceedings of the Third International Conference, iTrust Trust Management*, volume 3477 of *Lecture Notes in Computer Science*, pages 77-92, Paris, France, 2005. Springer.
- [Rob05] Morgan Roberts. A study of the massively multiplayer online business model within the interactive entertainment industry. Master's thesis, Master of Business Administration San Francisco State University, 2005.
- [S⁺76] Glenn Shafer et al. *A mathematical theory of evidence*, volume 1. Princeton university press Princeton, Princeton, NJ USA, 1976.
- [SAW12] Amirali Salehi-Abari and Tony White. Dart: A distributed analysis of reputation and trust framework. *Computational Intelligence*, 28(4):642-682, 2012.
- [SB14] S. Udhaya Shree and M. S. Saleem Basha. An exhaustive survey of trust models in P2P network. *International Journal on Web Service Computing (IJWSC)*, 5(3):1-12, 2014.
- [SC09] Shervin Shirmohammadi and Mark Claypool. Guest editorial for special issue on massively multiplayer online gaming systems and applications. *Multimedia Tools and Applications*, 45(1-3):1-5, 2009.
- [SCM10] Kieran Sullivan, Jim Clarke, and Barry P. Mulcahy. Trust-terms ontology for defining security requirements and metrics. In Ian Gorton, Carlos E. Cuesta, and Muhammad Ali Babar, editors, *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume*, ACM International Conference Proceeding Series, pages 175-180, New York, NY, USA, 2010. ACM.
- [Sei05] Jean-Marc Seigneur. *Trust, Security and Privacy in Global Computing*.

PhD thesis, University of Dublin, Trinity College,, 2005.

- [SGJ07] Travis Schluessler, Stephen Goglin, and Erik Johnson. Is a bot at the controls?: Detecting input data attacks. In *Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games*, pages 1-6. ACM, 2007.
- [SHM04] S Song, K Hwang, and M Macwan. Fuzzy trust integration for security enforcement in grid computing. In H Jin, GR Gao, ZW Xu, and H Chen, editors, *Network and Parallel Computing, Proceedings*, volume 3222 of *Lecture Notes in Computer Science*, pages 9-21, Heidelberger platz 3, d-14197 Berlin, Germany, 2004. IFIP, Springer-Verlag. IFIP International Conference on Network and Parallel Computing, Wuhan, China, Oct 18-20, 2004.
- [SKK⁺12] Seokshin Son, Ah Reum Kang, Hyun-chul Kim, Taekyoung Kwon, Juyong Park, and Huy Kang Kim. Analysis of context dependence in social interaction networks of a massively multiplayer online role-playing game. *PloS one*, 7(4):e33918, 2012.
- [SLPK09] Yan Sun, Thomas F La Porta, and Parviz Kermani. A flexible privacy-enhanced location-based services system framework and practice. *IEEE Transactions on mobile computing*, 8(3):304-321, 2009. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4586377.
- [SLT10] Michael Szell, Renaud Lambiotte, and Stefan Thurner. Multirelational organization of large-scale social networks in an online world. *Proceedings of the National Academy of Sciences*, 107(31):13636-13641, 2010.
- [SM12a] M. Sužnjević and M. Matijašević. Player behavior and traffic characterization for mmorpgs: A survey. *Multimedia Systems*, 942:4962, June 2012.
- [SM12b] M. Suznjevic and M. Matijasevic. Towards reinterpretation of interaction complexity for load prediction in cloud-based MMORPGs. In *Proceedings of International Workshop on Massively Multiuser Virtual Environments, Haptic Audio Visual Environments and Games (HAVE'12)*, pages 148-149, Munich, Germany, October 8-9, 2012. IEEE Press.
- [SNP13] Wanita Sherchan, Surya Nepal, and Cecile Paris. A survey of trust in social networks. *ACM Computing Surveys*, 45(4):471-4733, August 2013.
- [SS01] Jordi Sabater and Carles Sierra. REGRET: Reputation in gregarious societies. In *Proceedings of the 5th International Conference on Autonomous Agents*, AGENTS '01, pages 194-195, New York, NY, USA, 2001. ACM, ACM.
- [SS05] Jordi Sabater and Carles Sierra. Review on computational trust and reputation models. *Artificial Intelligence Review*, 24(1):33-60, September 2005.

- [SSM11] M. Suznjevic, I. Stupar, and M. Matijasevic. Traffic modeling of player action categories in a MMORPG. In *Proceedings of The 4th International Conference on Simulation Tools and Techniques (SIMUTools'11)*, pages 280-287, Barcelona, Spain, March 21-25, 2011. ICST.
- [ST11] Stefan Spitz and York Tüchelmann. A survey of security issues in trust and reputation systems for e-commerce. In *Autonomic and Trusted Computing*, Lecture Notes Computer Science, pages 203-214. Springer, Hong Kong Polytechnic University, China, 2011. Query date: 2012-10-17.
- [SVB05] Andreas Schlosser, Marco Voss, and Lars Brückner. On the simulation of global reputation systems. *Journal of Artificial Societies and Social Simulation*, 9(1):4, 2005. Available from: <http://jasss.soc.surrey.ac.uk/9/1/4.html>.
- [Tav12] Mozhgan Tavakolifard. *On Some Challenges for Online Trust and Reputation Systems*. PhD thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2012.
- [TB06] George Theodorakopoulos and John S. Baras. On trust models and trust evaluation metrics for ad hoc networks. *Ieee J Sel Area Comm*, 24(2):318-328, 2006.
- [TCG11] TCG. TPM Main Part 1 Design Principles. Technical Report Version 1.2 Revision 116, Trusted Computing Group, Inc., March 2011.
- [TJG⁺10] Konstantinos Tserpes, Michal Jacovi, Michael Gardner, Anna Triantafillou, and Benjamin Cohen. + spaces: Intelligent virtual spaces for e-governance. In *Proceeding of the 6th International Conference on Intelligent Environments*, pages 318-323, Kuala Lumpur, Malaysia, 2010. IEEE, IEEE.
- [TLHT09] Junfeng Tian, Chao Li, Xuemin He, and Rui Tian. A trust model based on the multinomial subjective logic for P2P network. *International Journal of Communications, Network and System Sciences*, 2(6):546-554, September 2009.
- [TPJL06] W. T. Teacy, Jigar Patel, Nicholas R. Jennings, and Michael Luck. TRAVOS: Trust and reputation in the context of inaccurate information sources. *Autonomous Agents and Multi-Agent Systems*, 12(2):183-198, March 2006.
- [UAL09] Glen L. Urban, Cinda Amyx, and Antonio Lorenzon. Online trust: State of the art, new frontiers, and research potential. *J Interact Mark*, 23(2):179-190, 2009. Anniversary Issue. Available from: <http://www.sciencedirect.com/science/article/pii/S1094996809000413>.
- [Urb13] J Urbano. *A Situation-aware and Social Computational Trust Model*. PhD thesis, FEUP, Universidade do Porto, 2013.

- [Usl02] Eric M Uslaner. *The moral foundations of trust*. Cambridge University Press, Cambridge, UK, 2002.
- [Var09] Vijay Varadharajan. Evolution and challenges in trust and security in information system infrastructures. In *Proceedings of the 2Nd International Conference on Security of Information and Networks, SIN '09*, pages 1-2, New York, NY, USA, 2009. ACM.
- [VCS07] Bart Van Caenegem and Thomas Skordas. Community research activities in secure and trustworthy ICT infrastructures. *Telecommunication Systems*, 35(3):89-97, 2007.
- [VGCK11] Nicholas Violi, Jennifer Golbeck, Kan-Leung Cheng, and Ugur Kuter. Caretaker: A social game for studying trust dynamics. In *Proceedings of the Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and Third International Conference on Social Computing (SocialCom)*, pages 451-456, Boston, Massachusetts, USA, 2011. CPS Conference Publisher Services.
- [vLAV05] Gregor von Laszewski, Beulah Alunkal, and I. Veljkovic. Toward reputable grids. *Scalable Computing: Practice and Experience*, 6(3):95-106, 2005.
- [VM12] Wattana Viriyasitavat and Andrew Martin. A survey of trust in workflows and relevant contexts. *IEEE Communications Surveys & Tutorials*, 14(3):911-940, July 2012. Available from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5989901.
- [VSMH10] Laurian C. Vega, Yeong-Tay Sun, D. Scott McCrickard, and Steve Harrison. Time: A method of detecting the dynamic variances of trust. In *Proceedings of the 4th Workshop on Information Credibility, WICOW '10*, pages 43-50, New York, NY, USA, 2010. ACM.
- [VSP16] Vinod Kumar Verma, Surinder Singh, and N.P. Pathak. Impact of malicious servers over trust and reputation models in wireless sensor networks. *International Journal of Electronics*, 103(3):530-540, 2016.
- [WAC⁺09] Andrew G. West, Adam J. Aviv, Jian Chang, Vinayak S. Prabhu, Matt Blaze, Sampath Kannan, Insup Lee, Jonathan M. Smith, and Oleg Sokol-sky. QuanTM: A quantitative trust management system. In *Proceedings of The 2nd European Workshop on System Security (EUROSEC'09)*, EUROSEC '09, pages 28-35, Nuremberg, Germany, March 31-31, 2009. ACM Press.
- [WBOM15] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. A survey on trust and reputation models for web services: Single, composite, and communities. *Decision Support Systems*, 74:121-134, 2015.
- [WCC⁺09] Chen-Chi Wu, Kuan-Ta Chen, Chih-Ming Chen, Polly Huang, and Chin-Laung Lei. On the challenge and design of transport protocols for

- mmorp.gs. *Multimedia Tools and Applications*, 45(1-3):7-32, 2009.
- [WCY⁺15] Yingjie Wang, Zhipeng Cai, Guisheng Yin, Yang Gao, and Qingxian Pan. A trust measurement in social networks based on game theory. In *Proceedings of the International Conference on Computational Social Networks*, pages 236-247, Helsinki, Finland, 2015. Springer, Springer.
- [WE05] Ye Diana Wang and Henry H. Emurian. An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1):105-125, January 2005.
- [Wes09] Andrew West. Quantitative trust manager simulator, 2009. Available from: <http://rtg.cisupenn.edu/qtm>.
- [WHS11] Yonghong Wang, Chung-Wei Hang, and Munindar P. Singh. A probabilistic approach for maintaining trust based on evidence. *Journal of Artificial Intelligence Research*, 40(1):221-267, January 2011.
- [WJDW10] Wang Wen-Jia and WANG Ding-Wei. Survey on online auction trust models. *Computer Engineering and Applications*, 46(29):1-5, 2010. Query date: 2012-10-17. Available from: <http://www.csa.com/partners/viewrecord.php?requester=gs&collection=TRD&recid=14275783CI>.
- [WKLS09] Andrew G West, Sampath Kannan, Insup Lee, and Oleg Sokolsky. An evaluation framework for reputation management systems. In Z. Yan, editor, *Trust Modeling and Management in Digital Environments: From Social Concept to System Development*, pages 282-308. IGI Global, 2009.
- [WR05] Dorothy E Warner and Mike Raiter. Social context in massively-multiplayer online games (mmogs): ethical questions in shared space. *International Review of Information Ethics*, 4(7), 2005.
- [WS07] Steven Daniel Webb and Sieteng Soh. Cheating in networked computer games: a review. In *Proceedings of the 2nd international conference on Digital interactive media in entertainment and arts*, pages 105-112. ACM, 2007.
- [Xin11] Liu Xin. *Trust beyond reputation: Novel trust mechanisms for distributed environments*. PhD thesis, Nanyang Technological University, 2011.
- [XL04] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *Ieee T Knowl Data En*, 16:843-857, 2004.
- [Yan03] Jeff Yan. Security design in online games. In *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, pages 286-295. IEEE, 2003.
- [Yan08a] Zheng Yan. A comprehensive trust model for component software. In *Proceedings of the 4th International Workshop on Security, Privacy and*

- Trust in Pervasive and Ubiquitous Computing*, SecPerU '08, pages 1-6, Sorrento, Italy, 2008. ACM.
- [Yan08b] Zheng Yan. *Trust Modeling and Management: From Social Trust to Digital Trust*, chapter Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, pages 290-323. IGI Global, Hershey, Pennsylvania (USA), 2008. Available from: <http://www.igi-global.com/bookstore/chapter.aspx?titleid=6870>.
- [YK13] Amir Yahyavi and Bettina Kemme. Peer-to-peer architectures for massively multiplayer online games: A survey. *ACM Comput. Surv.*, 46(1):91-951, July 2013.
- [YKSC06] George Yee, Larry Korba, Ronggong Song, and Y-C Chen. Towards designing secure online games. In *Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*, 2006.
- [YMSF08] Seunglim Yong, Hyun-Yi Moon, Yuseung Sohn, and Miguel Fernandes. A survey of security issues in collaborative virtual environment. *IJCSNS*, 8(1):14-19, 2008.
- [You07] Liangjun You. *An adaptive reputation-based trust model for intelligent agents in e-marketplace*. PhD thesis, The University of Texas at Arlington, USA, December 2007.
- [YP11] Zheng Yan and Christian Prehofer. Autonomic trust management for a component-based software system. *IEEE Transactions on Dependable and Secure Computing*, 8(6):810-823, 2011.
- [YR05] Jeff Yan and Brian Randell. A systematic classification of cheating in online games. In *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games*, pages 1-9. ACM, October 2005.
- [YS00] Bin Yu and Munindar P Singh. A social mechanism of reputation management in electronic communities. In Matthias Klusch and Larry Kerschberg, editors, *Cooperative Information Agents IV - The Future of Information Agents in Cyberspace: 4th International Workshop, CIA 2000, Boston, MA, USA, July 7-9, 2000. Proceedings*, pages 154-165. Springer, Berlin, Heidelberg, 2000.
- [YS02] Bin Yu and Munindar P. Singh. An evidential model of distributed reputation management. In *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, AAMAS '02*, pages 294-301, New York, NY, USA, 2002. ACM.
- [YS03] Bin Yu and Munindar P Singh. Detecting deception in reputation management. In *Proceedings of The 2nd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'03)*, pages 73-80,

- Melbourne, Australia, July 14-18, 2003. ACM Press.
- [YSL⁺13] Han Yu, Zhiqi Shen, Clement Leung, Chunyan Miao, and Victor R Lesser. A survey of multi-agent trust management systems. *IEEE Access*, 1:35-50, May 2013.
- [YSS04] Bin Yu, Munindar P Singh, and Katia Sycara. Developing trust in large-scale peer-to-peer systems. In *First Symposium on Multi-Agent Security and Survivability*, pages 1-10, Philadelphia, USA, 2004. IEEE, IEEE.
- [YWS03] T Yu, M Winslett, and K E Seamons. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Transactions on Information and System Security (TISSEC)*, 6(1):1-42, February 2003.
- [YZCZ11] Su-Rong Yan, Xiao-Lin Zheng, De-Ren Chen, and Wen-Yu Zhang. User-centric trust and reputation model for personal and trusted service selection. *International Journal of Intelligent Systems*, 26(8):687-717, August 2011.
- [YZV14] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120-134, 2014.
- [ZDB11] Ping Zhang, Arjan Durrresi, and Leonard Barolli. Survey of trust management on various networks. In *Proceedings of The 5th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS'11)*, pages 219-226, Korean Bible University, Seoul, Ko, June 30 - July 2, 2011. IEEE, IEEE Press.
- [Zet05] Joel Zetterstrom. A legal analysis of cheating in online multiplayer games. Master's thesis, School Of Economics And Commercial Law, Goteborg University, March 2005.
- [ZH07] Runfang Zhou and Kai Hwang. Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing. *Parallel and Distributed Systems, IEEE Transactions on*, 18(4):460-473, 2007.
- [Zip49] George Kingsley Zipf. *Human behavior and the principle of least effort*. Addison-Wesley Press, 1949.
- [ZKB11] Kun Zhao, Márton Karsai, and Ginestra Bianconi. Entropy of dynamical social networks. *PLoS one*, 6(12):e28116, 2011. Available from: <http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0028116>.
- [ZL05] Cai-Nicolas Ziegler and Georg Lausen. Propagation models for trust and distrust in social networks. *Information Systems Frontiers*, 7(4-5):337-358, 2005.

- [ZM00] Giorgos Zacharia and Pattie Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9):881-907, 2000.
- [ZPMY09] Zhiyong Zhang, Qingqi Pei, Jianfeng Ma, and Lin Yang. Security and trust in digital rights management: A survey. *International Journal of Network Security*, 9(3):247-263, November 2009.
- [ZWZL15] Haibin Zhang, Yan Wang, Xiuzhen Zhang, and Ee-Peng Lim. Reputation-pro: The efficient approaches to contextual transaction trust computation in e-commerce environments. *ACM Trans. Web*, 9(1):21-249, January 2015.
- [ZXJL09] Bo Zong, Feng Xu, Jun Jiao, and Jian Lv. A broker-assisting trust and reputation system based on artificial neural network. In *Proceedings of the International Conference on Systems, Man and Cybernetics (SMC)*, pages 4710-4715, San Antonio, Texas, USA, 2009. IEEE, IEEE.
- [ZXL⁺12] Xujuan Zhou, Yue Xu, Yuefeng Li, Audun Jøsang, and Clive Cox. The state-of-the-art in personalized recommender systems for social networking. *Artificial Intelligence Review*, 37(2):119-132, February 2012.
- [ZYW⁺15] Jie Zhang, Feng Yuan, Linxiao Wei, Yannan Liu, and Qiang Xu. Veritrust: verification for hardware trust. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(7):1148-1161, 2015.