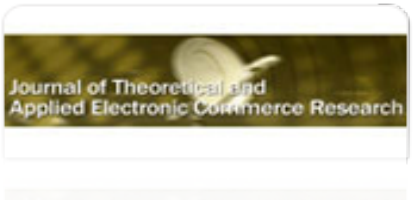

Journal of Theoretical and Applied Electronic Commerce Research
E-ISSN: 0718-1876
ncerpa@utalca.cl
Universidad de Talca
Chile

Kumar Sharma, Neeraj; Gaur, Vibha; Bedi, Punam
Safeguarding Buyers with Attack-Resilient Reputation Parameters
Journal of Theoretical and Applied Electronic Commerce Research, vol. 11, núm. 1, enero, 2016, pp. 46-66
Universidad de Talca
Curicó, Chile

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

Safeguarding Buyers with Attack-Resilient Reputation Parameters

Neeraj Kumar Sharma[1], Vibha Gaur[2] and Punam Bedi[3]

[1] University of Delhi, Department of Computer Science, Delhi, India, neeraj.sharma@rla.du.ac.in
[2] University of Delhi, Department of Computer Science, Delhi, India, vibhagaur@andc.du.ac.in
[3] University of Delhi, Department of Computer Science, Delhi, India, pbedi@cs.du.ac.in

Received 9 March 2014; received in revised form 20 March 2015; accepted 23 March 2015

Abstract

Agent-mediated reputation systems provide the necessary decision making support to facilitate the automation of processes, and to improve the quality of services in an information asymmetric e-market. Reputation systems encourage honest behavior and discourage malicious behavior of buyer and seller agents by safeguarding honest participants and by laying a foundation for security through social control mechanisms. In this paper, we propose a reputation system that aims to safeguard honest buyers from rogue behavior by counterparties and deceptive buying peers. It employs reputation functions with attack-resilient parameters based on the e-market parameters like value of the transaction and varying experience of agents.These parameters help to reduce the incentive for dishonest behavior, and to minimize harm in case of attacks by rogue sellers in order to improve the trustworthiness among participants in the e-market.

Keywords: Reputation, Trustworthiness, E-market, Robustness, Attack-resilience

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

1 Introduction

The widespread use of Internet is associated with related concerns of trust and reputation, especially for e-commerce transactions involving monetary exchange [31]. The use of agent technologies in reputation systems makes e-commerce more user-friendly and relatively secure as it facilitates accurate assessment of buyer and seller behavior.

Reputation has been expressed as "a perception that an agent has of another's intentions and norms" [16] or, “the opinions that nodes in the system have about their peers” [18]. Reputation and trust complement each other as an agent expects a positive outcome when interacting with another agent that has a reputation for being trustworthy [7]. Trust involves looking forward in time by expecting that another agent will do what it says it will, whereas reputation involves looking backward in time by assessing whether an agent behaved as per expectations.

Reputation systems help buyers/sellers to decide whether to participate in a transaction or not. In the e-market, generally sellers enjoy an information bias as compared to buyers, as buyers have no access to physical goods before the final payment; and, to make buying decisions, buyers rely on the product description by the seller. Hence, it is the buyer who mainly needs protection mechanisms that ensure honest behavior from sellers. On the other hand, a seller can benefit from such a situation by providing a good of lower quality, or simply by not providing any good at all; by frequently changing its identity to disown bad reputation; by colluding with others to maliciously manipulate its own or others reputation; or, by providing unfair information to others. In addition, due to the absence of the requirement of geographical proximity of counterparties in e-market transactions; the difficulty of identifying the actual person behind a transaction; and, a very limited shield of law enforcement due to multiple jurisdictions, prohibitive cost of investigation and prosecution makes it extremely difficult to penalize a cheater in the e-market in a traditional way. In such an environment, reputation systems aim to reduce the risk of engaging with potentially untrustworthy participants by providing a mechanism for establishing trustworthiness between mutually unknown online entities. This encourages honest behavior and discourages rogue behavior from participants. In the absence of reputation systems, there would be no explicit mechanism to distinguish between honest and fraudulent sellers. Due to high uncertainty, fraudulent sellers would flourish by offering cheap products at discounted rates. However, as all participants in the e-market are self-interested with no hesitation to con others, the success of a reputation system depends on its capability to protect honest participants. While existing reputation systems aim to promote honest behavior, their passive approaches are not enough to protect buyers from rogue traders [1]. If reputation systems expect fraudulent behavior and employ reputation computing strategies that are resilient to such behavior, then online buying and selling could become much safer.

The proposed reputation system is situated in a single cycle, sealed bid reverse auction, distributed e-market environment with self-interested buyers and sellers. The reverse auction involves rigorous work by the buyer that starts with a Request for Quote (RFQ) describing the buyer's requirements. In turn, multiple sellers join the bidding, and a virtual auction is established where sellers bid against one another over the Internet to sell the product [5]. In sealed bid auctions, bidders cannot see competitors' offers. On receiving product offers, the buyer agent selects the seller who is offering the product with the highest expected value. Each transaction culminates with buyer and seller agents updating the reputation of each other.

An attack on a reputation system can be defined as a sequence of activities with a desired outcome to exploit vulnerabilities in the reputation design [28]. In the e-market, the design of reputation functions must incorporate attack-resilient factors that enable distinction between honest or fraudulent behavior to reward honest and to punish rogue parties. If not identified and penalized, cheaters may not only harm honest members by reducing their trustworthiness but may also lead to failure of the e-market. This paper proposes a reputation computing methodology, which is resilient to common attacks as it is sensitive to parameters like the value of the transaction, the penalty for dishonest behavior, and the mutual experience of a buyer-seller pair. A robust reputation system should also identify the context in which one has earned trustworthiness, for example, as a counterparty, or as an advisor. In the proposed system, in addition to maintaining the reputation of sellers based on its own experience and opinions from other buying peers, a buyer also assigns reputation to opinion providing buying peers based on whether their opinions were fair or unfair.

A number of works from the literature [3], [25], [34] use the concept of penalty and reputation/dis-reputation thresholds, but these are subjective to a specific participant. In contrast, we set the seller's reputation and dis-reputation thresholds dynamically based on parameters like the buyer's risk taking ability, its past experience, and the value of transaction. It is based on the convention that in a high value transaction and untrustworthy environment, a buyer needs greater protection, therefore the reputation and dis-reputation thresholds should be set to a higher value as compared to a scenario with a low value transaction and a trustworthy environment. The penalty for dishonest behavior in our system has two components: a fixed minimum penalty, and a flexible component that changes with the value of the transaction. It underlines that rogue behavior in a large transaction is more harmful, and must invoke a higher penalty to discourage fraudulent sellers. The proposed reputation system promotes honest behavior and discourages dishonest behavior by computing reputation in a way that reduces the benefit of rogue sellers and also minimizes the impact of many attacks.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

This paper is structured as follows. Section 2 discusses the literature work and background of reputation systems is given in section 3. The e-market model is defined in section 4. Section 5 describes the reputation computing methodology. Section 6 provides the design and implementation, and section 7 comprises of an experimental study. Section 8 provides a discussion on the attack-resilience capability of our system, and section 9 concludes the paper.

2 Related Work

To alleviate the trustworthiness crisis in online purchase, several approaches have been proposed. A number of online trading platforms comprise of reputation systems to encourage honest transactions between buyers and sellers through feedback provision [6]. However, existing reputation systems fall short of dealing with individual and collusive behavior of rogue sellers to increase their own ratings or to reduce others reputation [12].

PeerTrust [20] uses a trust metric that takes into account the satisfaction of the source peer and credibility of the feedback source based on the number of transactions of a peer with other peers. It collects runtime feedback from peers that may be honest or dishonest. But it does not make a clear distinction between feedback from different sources. It computes feedback credibility endogenously, and is prone to errors if majority of feedback is collusive. In contrast, our system survives majority unfair ratings as a buyer filters out dishonest opinions based on their deviation from its own experience.

In Yu and Singh [34], an agent computes trustworthiness of others based on its direct interaction and others testimony. To track deceptions in reputation sharing, it uses the deviation among advisors' opinion to filter out unfair advice.

A probabilistic trust model for handling inaccurate reputation sources [19] computes the trust of an agent using past experience of interacting agents, and for lack of experience, it uses third party information. To discard unfair opinions, it finds the accuracy of the current advice based on past experience and tries to adjust the advice based on its accuracy. But, it assumes that sellers act consistently, which may not always be the case. It also needs to go over an advisor's past advice each time to estimate its accuracy.

Beta Reputation System [9] combines the seller ratings received from advisors using number of fair and unfair ratings. To handle unfair opinions, it uses Iterated Filtering approach to filter out ratings that are not in the majority. Hence, it is effective only when majority of ratings are fair.

Some reputation systems [23], [28] use only self experience of members. In Tran [28], sellers adjust the goods' price and quality to maximize profit. Roozmand et al. [23] computes reputation using quality, price and delivery time of goods. These systems suffer from Re-entry and Sybil attacks as their new sellers do not start from least reputation.

Huynh, Jennings and Shabolt [8] compute participants' trust based on direct experience, witness information, role based rules and third party referrals. It uses an inaccuracy tolerance threshold to specify the maximal allowed gap between the actual performance and witness rating and penalizes unfair witnesses accordingly.

Hazard and Singh [6] state that reputation systems must have *Monotonicity* and *Accuracy* properties. Our system follows Monotonicity, as selection of a seller and reputation computing are based on attributes like low price and high quality, and a rogue seller is penalized quickly to keep the reputation estimate accurate.

Selvaraj and Anand [25] provide a comprehensive survey of security issues in reputation systems for peer-to-peer (P2P) networks. They categorize different attacks as network-related and peer-related. In peer-related attacks, it identifies that Whitewashing, Sybil, and collusive attacks occur commonly, and discusses the vulnerability of some reputation systems [32], [36] to these attacks. It also discusses few research issues and challenges that are common to reputation systems in e-commerce like right peer selection and reliable exchange of reputation.

Marmol and Perez [18] analyze the applicability of a number of attacks (like Malicious Spies and Sybil attacks) in trust and reputation systems for distributed environments, and a discussion on the utility to handle these attacks.

Kussul, Kussul and Skakun [24] describe a number of attacks for the security of utility-based reputation systems in grids based on the security scenarios initially defined by Marmol and Perez [10]. To tackle attacks, they incorporate a statistical model of user behavior besides several other components like assigning initial reputation to a new participant, capturing coalition between a buyer and a resource, and determining the time decay and score functions.

Koutrouli and Tsalgatidou [9] provide a thorough view of the various threats in distributed reputation systems. They classify attacks and their cooresponding defense mechanisms. They also identify conflicts between different defense mechanisms and desirable characteristics of reputation systems. They also give a roadmap for reputation system designers to design robust reputation systems for P2P applications by identifying areas that require further research.

The reputation system proposed in this paper incorporates a number of attack-resilient reputation parameters in the design of reputation function to enhance its capability to defend against a number of common attacks. It also

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

comprises of a reputation sharing strategy to ensure that an unfair exchange of reputation information is filtered out before its use in computing the seller's shared reputation.

3 Background

With the popularity of e-commerce, the frequency of online fraud is also on the rise. Such an environment requires a proactive approach to safeguard honest participants from fraudsters who disguise themselves as honest parties [36]. Reputation systems are oriented to reduce the vulnerability of honest participants by playing an important role in mitigating information asymmetry and transaction risks by encouraging honest and discouraging fraudulent behavior of participants. This Section highlights the role of reputation systems as social behavior control mechanisms and also identifies different unacceptable social behaviors by self-interested participants in the form of various attacks.

3.1 Reputation Systems as Soft Security Mechanisms

Hard security and soft security are two different but interdependent approaches to security in information systems. The term hard security is used for techniques like authentication, authorization, integrity and confidentiality that aim to prevent intruders from entering the system, and the term soft security is used for techniques that assure protection against valid but rogue members of an environment based on social behavior control mechanisms like reputation systems [14]. Satisfactory detection and removal of vulnerabilities in the e-market require research in both these approaches to security. As shown in Figure 1, these approaches can be visualized as two layers, where trust due to soft security mechanisms like reputation systems cannot exist without the trust due to hard security mechanisms.

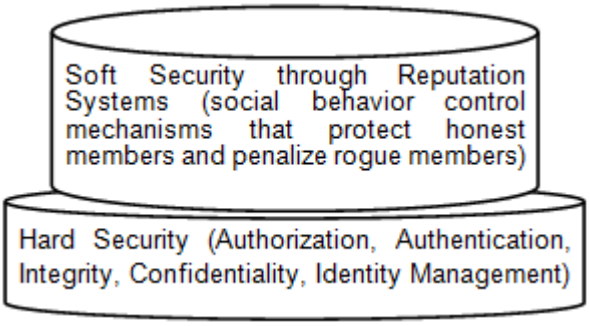

Figure 1: Layered architecture of hard and soft security

In environments with autonomous and self-interested participants, ensuring honest behavior is a challenging task. Reputation systems are based on common ethical norms to define a broad boundary of acceptable social behavior. These systems act as deterrent for rogue behavior by discouraging cheaters, and minimizing the impact of attacks. Presence of vulnerabilities in the reputation design may result in increase of attacks. The growth of attack-resilient reputation systems is therefore crucial for the e-market, otherwise cheaters would flourish thus leading to its failure.

3.2 Common Attacks on Reputation Systems

In this section, we discuss some common attacks on reputation systems. In Ballot Stuffing (BS) attack, a group of agents collude to rate another agent with abnormally high ratings to boost its reputation, and in Badmouthing (BM) a group of agents collude to rate an agent with low ratings.

In Re-Entry (REN) attack, a low rated agent exits the market and re-enters with a new identity to disown bad reputation. It is assisted by the availability of cheap pseudonyms in the online environment.

Reciprocity (REC) is an attack in which two agents mutually rate each other with abnormally high ratings whereas in Retaliation (RET) both the agents rate each other with abnormally low ratings.

In Value-Imbalance (VIM) attack, a rogue seller behaves honestly for small value transactions to gain reputation but cheats in a large value transaction. This attack thrives in systems where the amount of change in reputation for honest or dishonest behavior is not influenced by the price of product/products involved in that transaction.

In Multiple-Identity (MI) or Sybil Attack, a seller opens multiple accounts thereby increasing its chance to sell a good. It continues selling the goods honestly through some and dishonestly through others without facing any major penalty. It exits from a low reputation account and opens another account.

In Oscillations (OC) attack, rogue sellers supply bad products in some scenarios whereas in others they behave honestly. Handling OC is complex, as its resilience depends on behavioral pattern of parties.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

Reputation-Lag (RLG) takes advantage of the time gap, before cheating results in reduced reputation. In this period, an agent gets unlimited opportunities to cheat before others get aware of its lost reputation due to rogue behavior.
Self Promoting (SP) attack [18] involves one or more actors behaving fraudulently to falsely enhance their own reputation. For example, such an attack could occur if colluding parties mutually participate in frequent transactions to enhance reputation of each other.

In Malicious Spies (MS) attack [10], rogue peers behave honestly as traders/customers, but allocate abnormally high ratings to peers who always provide bad products/services.

In Orchestrated (ORC) attack [18], attackers employ a combination of strategies to launch a multifaceted and coordinated attack. Attackers change their behavior over time and divide themselves into sub-groups where each group plays different roles at different times.

The impact of different attacks by fradudulent participants in the e-market is much more than the manipulation of reputation values as these attacks may result in monetary loss and ruined business reputations. Resilience to various potential attacks is therefore extremely important, otherwise these attacks would lead to complete attrition of community trust in the e-market thus leading to its failure.

4 The E-Market Model

In the dynamic and potentially adversarial e-market environment, reputation systems seek to generate an accurate assessment of participants' behavior [18]. If the reputation design is susceptible to deceitful behavior from rogue participants, it can itself become a point of failure for the e-market due to its inability to accurately separate honest and dishonest participants. A reputation system that quickly adapts to changes in the e-market would be highly useful to protect honest parties from cheaters as it could model their behavior with greater accuracy.

The proposed e-market environment is: open, as agents can join or leave the e-market any time; dynamic, as it undergoes constant changes; uncertain, as the true worth of a good can be judged only after its purchase; un-trusted, as the e-market is populated with honest and dishonest agents; and distributed, as collection, computation and propagation of ratings is done by respective participants.

Major constituents of the e-market are buyer agents, seller agents, seller agent's comprehension of buyer's requirements, ability of an agent to track others' behavior, and the buyer–seller interaction cycle. To compute reputation we use Reinforcement Learning (RL) which is a machine learning technique that deals with what an agent should do in each state and how to map situations to action for maximizing long term rewards. RL involves mapping situations to actions, so as to maximize a scalar reward signal. In RL, the learner must discover the actions that yield the most reward by trying them. At times, actions may affect not only the immediate reward, but also the next situation and all subsequent rewards. The trial-and error search and delayed reward are the most important distinctive features of RL. Few well-known techniques for solving the RL problem are Dynamic Programming (DP), Monte Carlo (MC), and Temporal-Difference (TD) learning [33]. The proposed reputation system uses TD learning as it is a combination of MC and DP and is one of the vital and novel approaches of RL. Like MC, TD methods can learn directly from experience without a model of the environment. However, unlike MC, in which one must wait until the end of an episode to update the value function, TD algorithms only need to wait until the next time step.

Different processes belonging to a transaction in the e-market like computing and sharing of sellers' reputation and seller selection [35] for purchasing a product are sensitive to dynamic e-market parameters like the mutual experience of buyer/seller agents and value of the transaction. To utilize buyer's improved knowledge of a seller's behavior with each successive mutual transaction, the relative weight of seller's reputation based on self-experience of a buyer increases as compared to the advice by other buyer agents. Incorporating value of the transaction in the reputation function follows the principle that honest behavior in a big transaction is more significant than in a small transaction. In a robust reputation system, the reputation of a rogue participant should drop quickly, while it should be hard for a participant to boost its reputation in a short period of time [22]. Hence, the penalty for fraudulent behavior in the proposed reputation system is kept more than reward to ensure that in case of dishonest behavior by a seller, its reputation drops swiftly. Figure 2 shows the conceptual architecture of this environment.

In the e-market, agents automate the following e-commerce processes: search, advise, compare and select products and sellers; purchase products on behalf of actual buyers; track the behavior of other participants; filter out unfair information; update reputation of their counterparties based on self experience and others opinions; and update their peers' reputation based on their behavior during a transaction. In this paper, we focus on how the robustness of the reputation system is enhanced by using attack-resilient reputation parameters.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

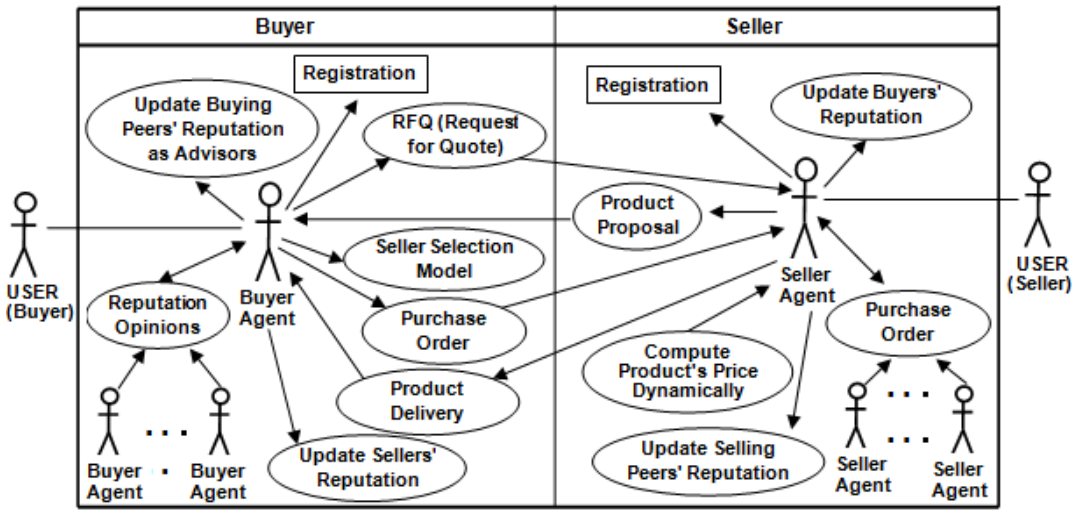

Figure 2: Architecture of distributed e-market

5 Reputation Computing Methodology

The methodology for computing reputation establishes the basic traits of a reputation system and may strengthen or weaken its resilience against various attacks. In this section, we present an attack-resilient reputation computing methodology to promote honest and to discourage dishonest behavior. In the proposed environment, important milestones in a transaction comprise of buyer's fuzzy product requirement specification, soliciting offers from sellers, seller selection, updating individual reputation, soliciting opinions from peers, computing shared reputation, and combining individual and shared reputation to form the overall reputation of a seller. In the proposed reputation system, Individual Reputation (IR) reflects a seller's trustworthiness based on self-experience of the buyer, and Shared Reputation (SR) reflects the opinion of other buyers about the reputation of a seller. The sequence diagram in Figure 3 represents ordering of processes in a transaction.

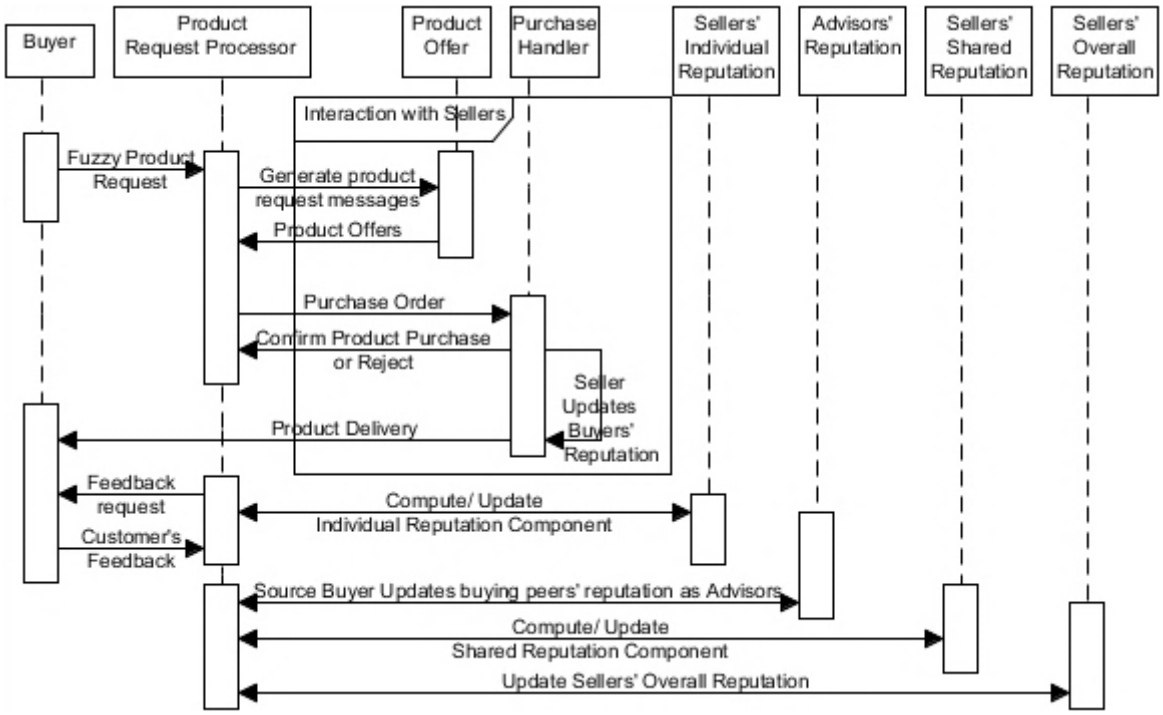

Figure 3: Interaction sequence of agents in an e-market transaction

In our system, B is the set of buyers, S is the set of sellers, and G is the set of goods. Let $r_t^b(s) \in [0,1]$ represent IR of seller *s* for buyer *b* at time *t*, $or_t^{others}(s) \in [0,1]$ represents SR of seller *s* for buyer *b* at time *t*, and $or_t^b(s) \in [0,1]$ represents overall reputation of seller *s* at time *t* for buyer *b*. Each buyer maintains four seller profiles: reputed, non-reputed, dis-reputed and new sellers. A seller is reputed if $or_t^b(s) \geq \Theta^b$, where Θ^b is buyer *b*'s reputation threshold

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

and $0 < \Theta^b < 1$; a seller is non-reputed if $\theta^b < or_t^b(s) < \Theta^b$, where θ^b is *b*'s dis-reputation threshold; and a seller is dis-reputed if $0 < or_t^b(s) \leq \theta^b$, where $0 < \theta^b < \Theta^b$. For sellers that are new to buyer *b*, $or_t^b(s) = 0$, and a seller remains in this list until its reputation moves above dis-reputation threshold θ^b. Before crossing θ^b, if a seller cheats then it is termed as dis-reputed. The seller profiling helps a buyer to decide with whom to interact. Reputed sellers enjoy high trustworthiness from the buyer, dis-reputed sellers are blacklisted, and non-reputed sellers are neither most preferred nor blacklisted. Similar to sellers, buyers acting as advisors are also categorized as reputed, non-reputed, dis-reputed and new.

Handling e-commerce transactions is sometimes difficult as the buyer's assessments of goods' attributes are often subjective, fuzzy, conflicting and non-commensurable in nature. The proposed system allows buyers to purchase a product by specifying their product requirements in terms of importance of different attributes in linguistic terms like *Highly Important* or *Moderately Important*. To select a seller, it uses a seller selection methodology [35] in which the buyer agent first computes fuzzy weights of different attributes of a good as per buyer's requirement and past experience. It solicits product offers from different sellers by forwarding buyer's fuzzy product request to existing sellers. On receiving goods' offers from different sellers, the buyer agent computes the expected value of the good by multiplying the fuzzy matrix containing sellers' product offers with fuzzy weights of different attributes, and purchases the good from a seller that offered the product with the highest expected value. After the product is delivered to the buyer, it solicits buyer's feedback for different product attributes, and computes the actual value of the good by using the seller selection methodology. If the actual value of the good is computed to be greater than its expected value reflecting that the buyer is satisfied with the product, the buyer agent enhances the reputation of the seller, otherwise it reduces the reputation of the seller as discussed below.

5.1 Computing Individual Reputation (IR)

Individual reputation of the seller is based on the buyer's experience during a transaction. If the buyer $b \in B$ is satisfied with the transaction, using reinforcement learning, it enhances the $r_{t+1}^b(s)$ i.e. IR of seller *s* at time *t*+1 as:

$$r_{t+1}^b(s) = or_t^b(s) + \mu\,(1 - or_t^b(s)). \tag{1}$$

$$\text{Further, } \mu = \frac{\eta}{\beta(1+\varepsilon)^n} \tag{2}$$

$$\text{and } \eta = 1 - e^{-\lambda x}. \tag{3}$$

Here, *μ* represents *effective reputation value increase factor*, and *η* represents *relative value factor* to ensure that $r_{t+1}^b(s)$ increases monotonically with value of the transaction, and $or_t^b(s)$ represents the overall reputation of seller s for buyer *b* at time *t*. In addition, x is the value of the transaction, and *η* maps the value of x to the range [0,1]. In case of a single good being purchased, x equals the price *p* of the good *g*. Also, *λ* is a constant in the range [0,1] that is used to moderate the sharp change in the value of the exponential function, and *e* is an exponential constant. In Equation (2), β is the *initial reputation discount factor* with a fixed assumed value of 1, *ε* is *mutual trustworthiness discount rate* with an initial value 0 and increments by a small fraction with each successive transaction between a buyer-seller pair, and n is the number of past transactions between that buyer-seller pair. It ensures that with increase in number of transactions between a buyer-seller pair, IR increases at a relatively smaller rate to reduce the impact of any collusion between the buyer and seller to inflate each other's reputation. If the environment is highly uncertain, β can also be set to a value higher more than 1. It can be observed from Equation (1) that $r_{t+1}^b(s)$ i.e. IR at time *t*+1 is based on $or_t^b(s)$ i.e. overall reputation at time *t* to underline that the overall reputation denoting the trustworthiness of seller *s* for buyer *b* at the end of last transaction forms a part of the self experience of buyer *b* in the next transaction. As for large values of x, η may quickly approach 1, before computing *η*, we first scale down x to a value within a reasonable range as:

$$\mathrm{x} = \mathrm{new\_min_x} + (\mathrm{new\_max_x} - \mathrm{new\_min_x}) * \frac{\mathrm{x} - \mathrm{min_x}}{\mathrm{max_x}}, \tag{4}$$

where, $[min_x, max_x]$ is the original and $[new\_min_x, new\_max_x]$ is the new range for x. In rest of the paper, when we imply value of the transaction using x, it means scaled value of x using Equation (4).

If the buyer *b* is not satisfied with purchased good *g*, using reinforcement learning, buyer *b* updates the IR of the seller *s* at time *t*+1 as:

$$r_{t+1}^b(s) = or_t^b(s) - \xi(1 - or_t^b(s)). \tag{5}$$

$$\xi = \gamma \frac{\eta}{\beta(1+\varepsilon)^n}, \tag{6}$$

$$\text{where, } \gamma = \gamma_{min} + \epsilon * x. \tag{7}$$

where, *ξ* is the *effective reputation value decrease factor* for dishonest behavior of a seller. Like *μ*, *ξ* also depends on value of the transaction and the number of past transactions between a buyer-seller pair. Hence, there is swift drop in reputation for a big transaction than a small transaction, and this drop is discounted with increase in the number of past transactions between a buyer-seller pair. In Equation (7), γ is the *Penalty Factor*, γ_{min} reflects the minimum

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

value of γ, and ϵ is a vey small fraction. The minimum penalty γ_{min} is kept more than 1 to ensure that reputation decreases sharply than its increase. It is based on the principle that reputation is difficult to build but easy to tear down [33]. The overall penalty γ is dynamic as it varies with the value of a transaction x. It underlines that cheating in a big transaction is more harmful, and must invoke higher penalty to put off rogue sellers.

5.2 Computing Shared Reputation (SR)

In a distributed environment, while sharing sellers' reputation, the requesting buyer may receive unfair ratings from its peers. To handle this problem, we propose a reputation sharing methodology with two major constituents: filtering unfair advice, and allocating reputation to advisors based on their behavior. In the e-market, as buyers may not always be willing to share their opinion, so there should be an incentive for those advisors who always provide opinion on request and are also honest. Our strategy gives incentive to honest advisors from two angles. First, it assigns reputation to advisors exclusively for participating in the reputation sharing process. Second, it enhances the weight of each successive fair opinion by an advisor as a reward for showing honesty in a self-interested environment. The proposed methodology filters other buyers' advice by using the concept of "moment about an arbitrary point" [30] compares the set of received opinions about the target seller's reputation with the IR of the target seller for the opinion seeking buyer. The *second moment* is widely used to measure the *width* of a set of points in one dimension, or in higher dimensions measures the shape of a cloud of points [21]. Instead of finding the deviation from the set of received opinions, this methodology computes the deviation of shared opinions from the seller's IR reflecting the buyer's self experience of the seller. Filtering out unfair opinions based on their deviation from the requesting buyer's self experience, if any, helps to filter out unfair opinions even if majority of opinions are collusive in nature.

Let *b* be the buyer soliciting the reputation of seller *s* from its buying peers as advisors at time *t*+1 and accepts their opinions $sr_{t+1}^{b_i}(s) sr_{t+1}^{b_i}(s)$ denoting the reputation of seller *s* from advisors b_i for *i =1,2,...,n*. It discards any opinions from dis-reputed advisors. To compute the maximum permitted deviation m_2 of received opinions from its own past experience of the seller's reputation, buyer *b* computes the deviation of the set of received opinions i.e. $sr_{t+1}^{b_i}(s)$ from the IR i.e. $r_{t+1}^{b}(s)$ of seller *s* as:

$$m_2 = \frac{\sum_{i=1}^{n}(sr_{t+1}^{b_i}(s) - r_{t+1}^{b}(s))^2}{n} \; m_2 = \sqrt{\frac{\sum_{i=1}^{n}(sr_{t+1}^{b_i}(s) - r_{t+1}^{b}(s))^2}{n}} \; . \tag{8}$$

If the buyer and seller are interacting for the first time, it finds the deviation of the advisors' opinions from their mean $m_{adv_{t+1}} \; s$ as:

$$m_2 = \sqrt{\frac{\sum_{i=1}^{n}(sr_{t+1}^{b_i}(s) - m_{adv_{t+1}}(s))^2}{n}}, \tag{9}$$

$$\text{where, } m_{adv_{t+1}}(s) = \frac{\sum_{i=1}^{n} sr_{t+1}^{b_i}(s)}{n} . \tag{10}$$

Denote opinions where $sr_{t+1}^{b_i}(s) - r_{t+1}^{b}(s) \leq m_2 \; sr_{t+1}^{b_i}(s) - r_{t+1}^{b}(s) \leq m_2$ as fair/honest, and others as unfair/dishonest. $sr_{t+1}^{b_i}(s) - r_{t+1}^{b}(s) > m_2$Filter out unfair opinions $\tilde{D}$from the set of received opinions.

From the set of honest opinions, buyer *b* computes the weight w_{b_i} $w_{b_i}$of each honest opinion by utilizing advisors' b_i past behavior based on parameters like the number and the percentage of honest past transactions between the buyer seller pair. Finally, the buyer computes the aggregated shared reputation $or_{t+1}^{others}(s) or_{t+1}^{others}(s)$ of the seller *s* as: $or_{t+1}^{others}(s)$

$$or_{t+1}^{others}(s) = \frac{\sum_{i=1} w_{b_i} * sr_{t+1}^{b_i}(s)}{\sum_{i=1}^{n} w_{b_i}} \; or_{t+1}^{others}(s) = \frac{\sum_{i=1}^{n} w_{b_i} * sr_{t+1}^{b_i}(s)}{\sum_{i=1}^{n} w_{b_i}} . \tag{11}$$

The buyer *b* also updates the reputation $ar_{t+1}^{b}(b_i) ar_{t+1}^{b}(b_i)$ of each honest/fair advisor $b_{i.}$ as:

$$ar_{t+1}^{b}(b_i) = ar_{t}^{b}(b_i) + \Omega \; (1 - ar_{t}^{b}(b_i)), \tag{12}$$

$$\text{where, } \Omega = 1 - e^{-\Lambda * x}. \tag{13}$$

Here, Ω is the *advisors' reputation increase factor* and x is value of the transaction. It makes the increase in advisors' reputation monotonically relative to transaction value. But, if the advisor's opinion is dishonest, buyer *b* reduces its reputation as:

$$ar_{t+1}^{b}(b_i) = ar_{t}^{b}(b_i) - \varphi \; (1 - ar_{t}^{b} \; b_i \;). \quad ar_{t+1}^{b}(b_i) = ar_{t}^{b}(b_i) + \Omega \; (1 - ar_{t}^{b}(b_i))$$
$$ar_{t+1}^{b}(b_i) = ar_{t}^{b}(b_i) - \varphi \; (1 - ar_{t}^{b}(b_i)) \tag{14}$$

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

where, $\varphi = \wp * (1 - e^{-\Lambda * x})$). (15)

Here, φ φ is the *advisors' reputation decrease factor*, Λ Λ is a constant from 0 to 1, and $\wp$ is penalty for dishonest advice, and $\wp > 1$ $\wp \geq 1$to ensure that penalty for dishonesty is greater than reward for honesty. Finally, buyer agent *b* updates the sets of reputed, non-reputed, dis-reputed and new advisors.

This reputation sharing methodology is sensitive to the past behavior of advisors to encourage advisors to repeatedly provide honest opinions. It also penalizes dishonest advisors by reducing their reputation based on the concept that fake advice is worse than no advice, as its goal is to subvert the reputation system itself. Further, to ensure the availability of honest advisors, a buyer always responds to a request from its reputed advisors. It follows the rule that cooperative behavior by non- competitive peers engaged in repeated transactions is mutually beneficial, as it minimizes the need of seeking opinion from relatively unknown and potentially dishonest advisors.

5.3 Computing Overall Reputation (OR)

After computing the individual and shared reputation, buyer *b* combines these to compute the overall reputation $or_{t+1}^{b}(s)$ of the seller *s* as:

$$or_{t+1}^{b}(s) = \alpha * r_{t+1}^{b}\ s\ + (1 - \alpha) * or_{t+1}^{others}(s). \quad (16)$$

Note that $r_{t+1}^{b}(s)$ is the individual reputation of seller *s* as computed by buyer *b*, and $or_{t+1}^{others}(s)$ is the aggregated shared reputation component. Also, *α* is the *experience gain factor* and $0 \leq \alpha \leq 1$. The initial value of *α* before the first transaction between a buyer-seller pair is 0 and with each successive transaction, it is incremented by a small factor, say 0.01, to ensure that with increase in number of mutual transactions between a buyer-seller pair, the relative weight of IR increases and that of SR decreases. After large number of mutual transactions, when *α* approaches 1, $or_{t+1}^{b}(s)$ depends only on $r_{t+1}^{b}(s)$ as the weight of $or_{t+1}^{others}(s)$ approaches 0. Initially, when a buyer has no experience of a seller, it depends largely on others' opinions at the cost of incurring communication overhead, however once a buyer gains enough experience of a seller, it can avoid the overhead of inter-agent communication. Further, if a seller is new to buyer *b*, its overall reputation $or_{t}^{b}(s)$ is computed as:

$$or_{t}^{b}(s) = or_{t}^{others}(s). \quad (17)$$

Also, if a seller is new in the e-market then, $or_{t}^{b}(s) = 0$. Finally, update the sets of reputed, non-reputed, dis-reputed and new sellers. As our strategy is sensitive to varying parameters of e-market, it reduces the incentive of rogue sellers that try to benefit from vulnerabilities in the reputation function.

5.4 Use of Attack-Resilient Reputation Parameters

In the distrusted e-market environment, usually, the strength of a reputation system is based on its potential to endure attacks by rogue members. Hence, reputation functions must include some defense enhancing parameters to ensure that honest parties are rewarded with higher reputation and improved economic gains and cheaters are penalized with economic loss. In addition to protect from rogue counterparties, a reputation system must also be resilient to attacks involving dissemination of unfair information among agents, and it must also encourage advisors to share fair information. Two major rating misbehaviors during opinion gathering process are Individual Unfair Ratings, and Collaborative Unfair Ratings [2]. Compared with collaborative unfair ratings, individual unfair ratings usually cause less damage, hence we focus on filtering out collaborative unfair ratings. Next, we analyze the contribution of parameters in the reputation functions of the proposed reputation system to enhance its attack-resilience.

5.4.1 Dynamically Setting Reputation and Dis-Reputation Thresholds

As defined above in section 5, each buyer maintains four seller profiles with the help of two thresholds: buyer *b*'s reputation threshold Θ^{b} above which all sellers are termed as reputed, and dis-reputation threshold θ^{b} below which all sellers are termed as dis-reputed. To safeguard buyers, we propose a strategy to compute the reputation and the dis-reputation thresholds based on following three factors.

- Risk taking capability of the buyer: One of the factors to set these thresholds is the buyers' risk taking capability. We denote the buyer specific subjective constants $\text{base\_}\Theta^{b}$ and $\text{base\_}\theta^{b}$ as base values of the reputation and the dis-reputation thresholds for sellers that are set based on buyers' risk taking ability. Consequently, a risk averse buyer would choose a higher value, and a risk tolerant buyer interested in exploring the market would choose a lower value for these thresholds.

- Trustworthiness of e-market: The less trustworthy the e-market is, the higher is the value reputation/dis-reputation threshold should be set to. Trustworthiness of e-market for a buyer is computed based on its experience in past transactions.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

- Value of the Transaction: As fraudulent sellers get greater benefit by cheating in a high value transaction, a buyer needs extra protection. The value of a transaction must be a vital factor in setting the reputation and the dis-reputation thresholds, as the buyer would be more risk averse for a big transaction, and would like to set these thresholds to be higher as compared to their value in a low value transaction.

Based on above discussion, the reputation threshold Θ^b of buyer *b* is computed as:

$$\Theta^b = base\_\Theta^b * (1 + \hbar * (1 - e^{-\lambda x})) . \quad (18)$$

Further, $\hbar = \frac{n - NoHT}{n}$. (19)

Similarly, the dis-reputation threshold θ^b of buyer *b* is computed as:

$$\theta^b = base\_\theta^b * (1 + \hbar * (1 - e^{-\lambda x})) . \quad (20)$$

Here, n is the number of transactions of buyer *b* in the recent past, $NoHT$ is the number of honest transactions out of last n transactions, $\hbar$ is the experience of buyer *b* in last n transactions as a ratio of the number of dishonest transactions to the total number of transactions, λ is a constant between 0 to 1, x is the value of a transaction, and *e* is an exponential constant. If a buyer has no experience of a seller, $\hbar$ has a default value of 1 to initially set these thresholds with a relatively strict criteria. As buyer gains experience of a seller, $\hbar$ is computed based on its actual experience. Also, as these thresholds change monotonically with value of the transaction, their values are higher for big transactions as compared to small ones.

As sellers with reputation below dis-reputation threshold θ^b are blacklisted, a buyer should carefully set the value of $base\_\theta^b$. To avoid majority of sellers falling below the dis-reputation threshold without any concrete evidence of sellers being successively dishonest, $base\_\theta^b$ should be set to a suitably low value.

5.4.2 Dealing with New and Non-Reputed Sellers

In addition to reputed sellers, a buyer should also give a chance to new and non-reputed sellers. Initially, when the buyer itself is new, it must deal with new sellers. As the buyer gains experience of various sellers, it uses an already discovered set of reputed sellers and makes less effort to find new sellers. In an e-market with highly unpredictable seller behavior and greater frequency of new sellers joining the e-market, the tendency to give chance to a new seller should be high. But if most of transactions are honest, or if new sellers seldom join the e-market, the rate of discovery of new sellers may be rather low.

In the proposed system, a buyer uses the following strategy to find new sellers. From the total set of offers by sellers, if the number of reputed sellers' offers is above a certain threshold N, and out of the total set of offers, if the fraction of offers by reputed sellers is above a *well known threshold* WT where $0 < WT < 1$, then the buyer chooses only from reputed sellers. In case the fraction of offers by reputed sellers is on or above *sufficiently known threshold* ST but less than WT for $0 < ST < WT < 1$, then the buyer chooses from reputed and new sellers. Otherwise, the buyer chooses from reputed, non-reputed and new sellers for the product purchase. It implies that for seller selection, new sellers are given slightly higher preference than non-reputed sellers. This is based on the following reasons: to ensure fair competition, new sellers must be given a chance, and non-reputed sellers may comprise of sellers who behaved dis-honestly in the past leading to fall of their reputation below reputation threshold.

5.4.3 Choosing the Appropriate Penalty

Here, we analyze the utility of computing a lower bound on penalty to ward off simple Oscillations (OC) attack by a rogue seller. Consider a situation, where seller *s* was dishonest in the last transaction with buyer *b* that resulted in reduction of its reputation. In the next transaction with buyer *b*, seller *s* behaved honestly in order to enhance its reputation to the same value where it was before the last transaction. Let at time t_0, the overall reputation $or_{t_0}^b$ of *s* for *b* is a result of *b*'s self experience and opinions from others. Assuming that after the transaction between *b* and *s* at time t_1, the actual value of the product received from *s* is found to be less than its expected value. Based on Equation (5) and Equation (6), it resulted in buyer *b* decrementing the Individual Reputation (IR) of seller *s* as:

$$r_{t_1}^b = or_{t_0}^b - \frac{\gamma(1 - e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}(1 - or_{t_0}^b) . \quad (21)$$

At time t_1, let n_1 is the number of past transactions between buyer *b* and seller *s*. To regain lost reputation, *s* behaves honestly in the next transaction with *b* at time t_2 such that *b* enhances the IR of *s*. Using Equation (1) and Equation (2), updating of IR of seller *s* by buyer *b* after the transaction at time t_2 is represented as:

$$r_{t_2}^b = or_{t_1}^b + \frac{(1 - e^{-\lambda x_2})}{\beta(1+\varepsilon)^{n_1+1}}(1 - or_{t_1}^b). \quad (22)$$

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

To keep things simple, we assume that, either $or_{t_1}^{others}$ reflecting the Shared Reputation (SR) is same as IR i.e., $r_{t_1}^b = or_{t_1}^{others}$ or, the weight of $or_{t_1}^{others}$ is negligible. Using Equation (16), the overall reputation becomes equal to IR i.e. $or_{t_1}^b = r_{t_1}^b$. Similarly, $or_{t_2}^b = r_{t_2}^b$. At time t_2, seller *s* regains its past reputation by behaving honesty if, $or_{t_2}^b = or_{t_0}^b$.

$$\text{Hence, } or_{t_1}^b + \frac{(1-e^{-\lambda x_2})}{\beta(1+\varepsilon)^{n_1+1}}(1 - or_{t_1}^b) = or_{t_0}^b ,$$

$$\left(or_{t_0}^b - \frac{\gamma(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}(1 - or_{t_0}^b)\right) + \frac{(1-e^{-\lambda x_2})}{\beta(1+\varepsilon)^{n_1+1}}\left(1 - \left(or_{t_0}^b - \frac{\gamma(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}(1 - or_{t_0}^b)\right)\right) = or_{t_0}^b ,$$

$$\frac{1-e^{-\lambda x_2}}{1+\varepsilon} = \frac{\gamma(1-e^{-\lambda x_1})}{1+\frac{\gamma(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}} . \tag{23}$$

Besides penalty γ, $\frac{(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}$ is the main factor responsible for reputation loss and,

$$(1 - e^{-\lambda x_1}) > \frac{(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}} . \tag{24}$$

Let $1 - e^{-\lambda x_1} = c$, where *c* is a constant in the range (0,1]. Now, to earn back lost reputation, the seller must ensure, $\frac{(1-e^{-\lambda x_2})}{(1+\varepsilon)} > c$. Hence, by using Equation (23),

$$\frac{\gamma(1-e^{-\lambda x_1})}{1+\frac{\gamma(1-e^{-\lambda x_1})}{\beta(1+\varepsilon)^{n_1}}} > c ,$$

$$\gamma > \frac{1}{1-\frac{c}{\beta(1+\varepsilon)^{n_1}}} . \tag{25}$$

By keeping penalty γ sufficiently higher than the threshold described in Equation (25), buyer *b* can negate the impact of simple oscillatory behavior, as the reputation loss for a dishonest transaction would always be higher than the gain for an honest transaction. Hence, if a seller with oscillatory behavior wants to sustain as a reputed counterparty for a buyer, it must behave honestly in large value transactions resulting into reduced incentive for the rogue seller. In the proposed system, we can utilize the above analysis for setting the minimum penalty γ_{min} in Equation (7). Further, in Equation (7), the overall penalty is set dynamically as it also depends on value of the transaction to ensure higher penalty for rogue behavior in a large value transaction as compared to a small value transaction.

5.4.4 Handling Re-Entry/Sybil Attacks

In a transaction, reputation is assigned to a buyer or seller against an identity. To enhance and maintain its trustworthiness, a seller has to sacrifice short term gains by incurring two types of costs: Reputation Building Cost (RBC), and Reputation Maintenance Cost (RMC). RBC comprises of the initial loss of profit that an honest seller has to incur to gain reputation, and RMC comprises of sacrificed short term profits by not indulging in rogue behavior. To build reputation, a seller must be ready to work with minimum profit to establish itself.

In the e-market, if sellers change their identity by Re-Entry (REN) or Sybil attacks, they can repeatedly sell bad products and still earn profits. Frequent identity change raises RMC of honest sellers thus making their survival difficult. Inspired from Zhou et al. [23], we define Net Gain to dishonest seller ($NGds$) based on RMC and RBC as:

$$NGds = \sum_{i=1}^{n}(RMC - RBC). \tag{26}$$

In Equation (26), *n* represents the number of buyers with whom the seller interacts. It can be observed that RBC will only be incurred if a seller delivers high quality products in the initial interaction period with each buyer. However, a rogue seller will benefit by frequently changing its identity, if $NGds$ is sufficiently higher than 0. Hence, to discourage a rogue seller, $NGds$ should be minimized. In systems [25], [29], [33] where new sellers are assigned initial reputation more than the minimum possible reputation RBC approaches 0, and $NGds$ gets equal to RMC of an honest seller. It enhances the incentive of sellers to behave dishonestly by frequently changing their identity as shown in Figure 4.

In reputation systems, ensuring high RBC can be a viable method to reduce the incentive for change in identity. The enhanced RBC would reduce the $NGds$ due to REN as well as Sybil attack. However, on the flip side, increased RBC would also apply to all honest new sellers. We handle this problem by giving a fair chance to new sellers as explained in section 5.4.2. In our system, RBC is relatively high as a new seller begins from the lowest possible reputation of 0, and has to strictly behave honestly to cross dis-reputation and reputation thresholds before it can enjoy the benefits of being reputed. If a new seller behaves dishonestly even once before moving above the dis-reputation threshold, it is designated as a dis-reputed seller for that buyer. The minimized $NGds$ in the proposed reputation system results in reduced incentive for a seller that changes its identity frequently.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

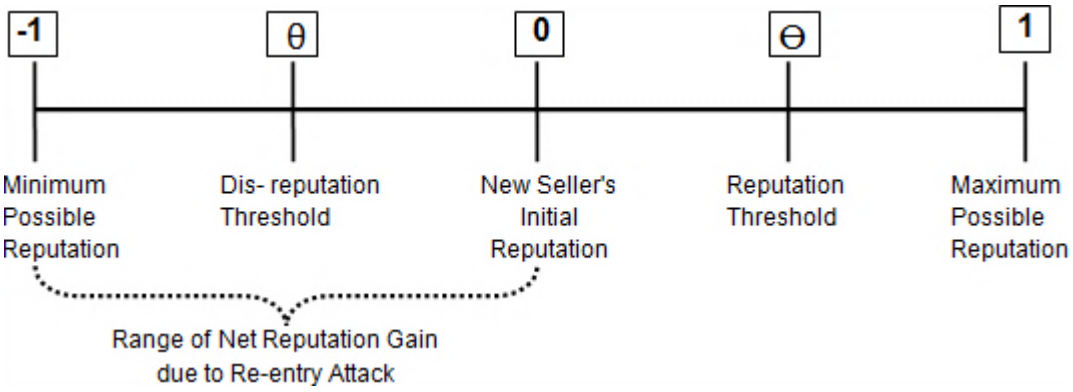

Figure 4: Impact of change in identity if initial reputation is more than minimum reputation

5.4.5 Resolving Value Imbalance (VIM) Attack

The *relative value factor η* defined in Equation (3) ensures that the IR component $r_{t+1}^{b}(s)$ increases monotonically with the value of a transaction. It counters VIM and OC attacks, where a seller acts honestly in small value transactions but turns rouge for a high value transaction. In addition, the *relative value factor η* also plays a key role in deciding the amount of decrease in IR component of a seller for dishonest behavior in a transaction.

5.4.6 Handling Self Promoting (SP) Attack

The term $\beta(1+\varepsilon)^{n}$ in Equation (2) ensures that with increase in number of transactions between a buyer-seller pair, the increase in individual reputation is discounted. Where, β represents the *initial reputation discount factor*, ε is *mutual trustworthiness discount rate* with initial value 0 and a small incremental value with each successive transaction between a buyer seller pair, and n is the number of past transactions between a buyer and seller. It handles SP attack where a buyer and seller collude by indulging in large number of mutual transactions in order to raise the seller's reputation.

6 Design and Implementation

We designed an agent-mediated reputation system built up on top of the agent environment provided by Java Agent Development Framework (JADE). The proposed reputation system is composed of three layers: web interaction layer, object-agent communication layer, and agent environment layer implemented in JADE. Figure 5 shows the overall layered design of proposed multi-agent system.

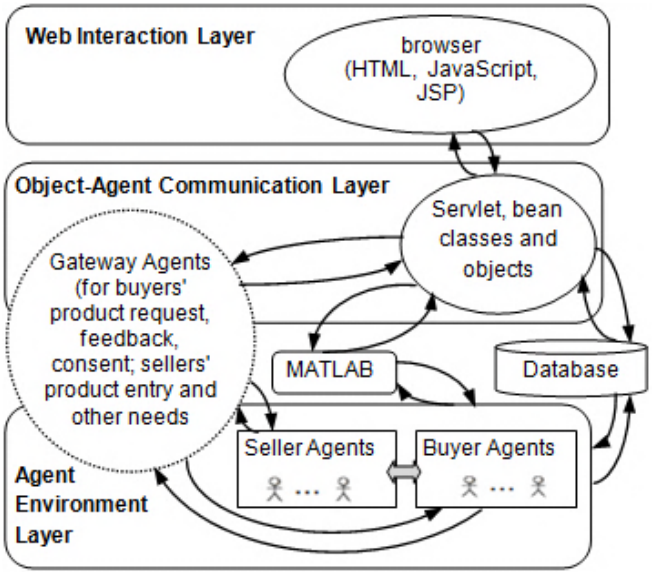

Figure 5: Layered design of distributed e-market

The Web layer deals with actual users and acts as a user interface. The user interaction from the web is captured by the servlet to perform actions like creating a gateway agent for sending a product request to the buyer/seller agent. The programs that create gateway agents, use JadeGateway and GatewayAgent classes of JADE to connect agent

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

environment with any non-agent software. Similarly, any results received from the agent environment are displayed on the web using gateway agents.

The Object-Agent Communication Layer allows interaction between Web Interaction Layer and Agent Environment Layer using specially built classes and programs to connect agent environment with any non-agent software. As shown in Figure 5, the two way object-agent communication is established by creating gateway agents through servlets, and one gateway agent is created for each object-agent interaction.

All buyer and seller agents reside in the Agent Environment Layer. In this layer different buyer and seller agents communicate using asynchronous ACL (Agent Communication Language) messages. Each agent performs its intended tasks by executing various behaviors related to specific events.

To implement the proposed reputation system, we built a working prototype by simulating an e-market with 30 buyers and 10 sellers built upon JADE platform. The object-agent communication was achieved by gateway agents created through servlets. To utilize built in functions and toolboxes, we implemented few algorithms in MATLAB (MATrix LABoratory) R2011b. Two way communication between JAVA/JADE and MATLAB was achieved to utilize MATLABs' computing ability and the power of JADE to implement a multi-agent system along with its agent communication facilities and graphical tools like Remote Agent Management (RMA GUI agent) and Sniffer agent. RMA GUI agent provides the graphical interface of JADE, and sniffer agent shows inter-agent communication. To store data and to enable agents to utilize their past experience, we maintained the database in ORACLE XE. For experiments, we used datasets for the Lenovo Z570 laptop and SanDisk pen drive.

In this section, we illustrate some of the main functions of a buyer agent in a transaction through some screen shots. These screen shots are used for the explanation purpose only, and not for the output of the system. In a transaction, buyer b_1's request for a laptop is handed over to a servlet that creates a gateway agent to provide object-agent communication by receiving b_1's RFQ and taking it to JADE.

The gateway agent hands over buyer's RFQ to the buyer agent, which sends an ACL REQUEST message to DF (Directory Facilitator) agent to find all existing sellers as DF agent performs the job of a yellow paging service in JADE. A snapshot of gateway agent giving RFQ to buyer agent, the buyer agent searching for sellers, and sending the RFQ using an ACL CFP (Call for Proposal) message to sellers is shown in Figure 6.

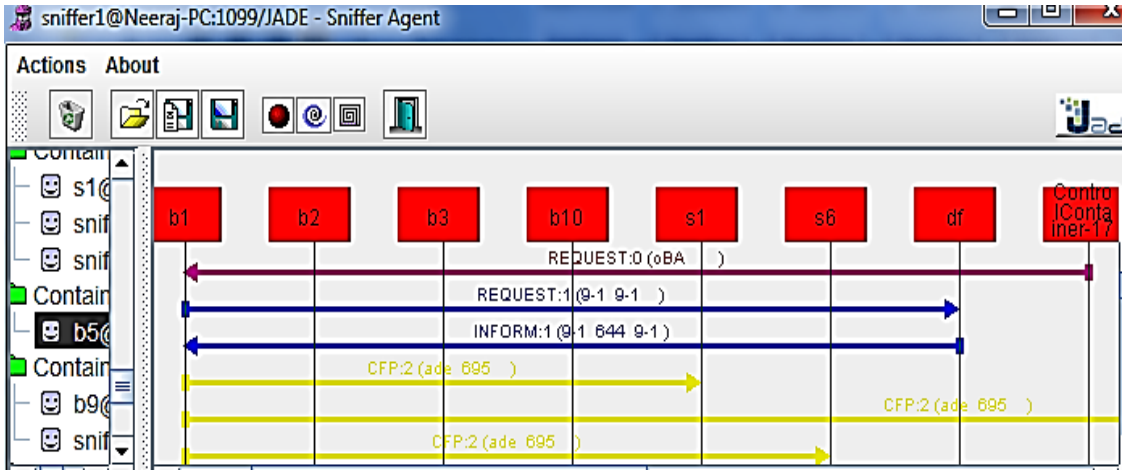

Figure 6: Buyer agent sending RFQ after finding seller agent

After finding the suitable product, interested sellers respond by sending back a PROPOSE ACL message containing their product offers, or REJECT ACL message indicating the un-availability of the product. On receiving the product offers, the buyer agent uses the seller selection methodology [35] to select the seller with the best product offer. After the successful purchase of the product from seller s_6, the gateway agent carried the final response and any other relevant data in the form of an ACL message to the buyer's servlet as shown in Figure 7.

Figure 7: Product selling information received by the web server

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

Once the buyer provided its feedback, the buyer agent computed the individual reputation of the seller. Concurrently, the buyer agent b_1 also solicited the advice from other buying peers regarding the reputation of the target seller agent, by sending the REQUEST ACL message to other buyers as shown in Figure 8.

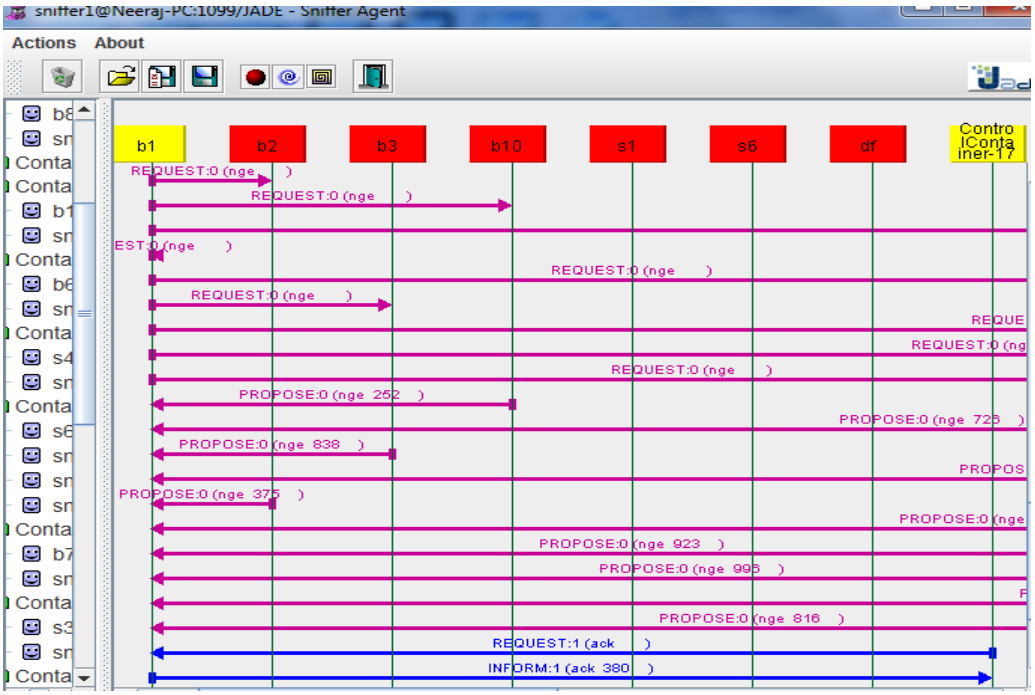

Figure 8: Inter-buyer communication sharing seller's reputation

After receiving buying peers' opinions in the form of PROPOSE ACL messages, the buyer agent b_1 filters out dishonest opinions, computes shared reputation component, and updates the reputation of advising buying peers. Figure 9 illustrates a snapshot of MATLAB showing updated individual reputation of the seller after purchase, filtering of opinions, and updating of advisors' reputation.

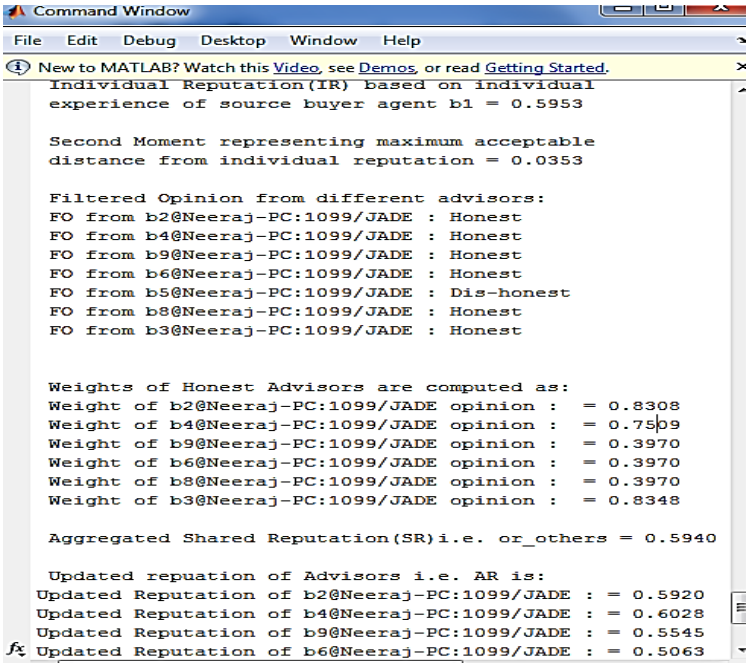

Figure 9: Computing individual and shared reputation

The buyer b_1 combined individual and shared reputation components to compute the overall reputation of seller s_6 as illustrated in Figure 10 below.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

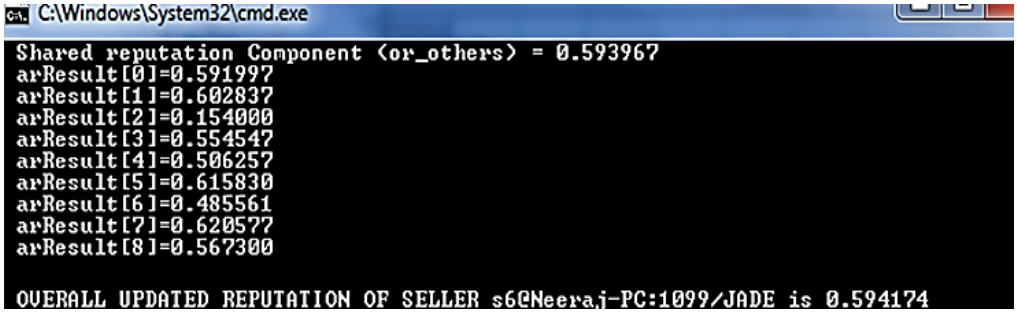

Figure 10: Updated reputation of buying peers as advisors

The reputation of the seller s_6 was updated by b_1 in the database, and an ACL INFORM message was handed over to the gateway agent that passed the message to the buyer servlet and finally to the buyer to reflect the completion of the transaction.

7 Experimental Study

An experimental study was conducted to underline the attack-resilient capability of the proposed reputation system in the e-market. To show the ability of our system, that in this section we refer to as Agent-Mediated Attack-Resilient Reputation (AMARR) system to counter various common attacks on reputation systems, we simulated a number of attack scenarios.

In a particular scenario, after 10 mutual past transactions, seller s_2 launched simple oscillations attack on buyer b_1 in which s_2 behaved honestly and dishonestly in alternative transactions. We compared our AMARR system with Tran and Roozmand systems [25], [33], [34] that use fixed and subjective penalty factors, and are not sensitive to value of the transaction. We have chosen these systems from literature [25], [33], [34] for comparison as these systems are set in the similar e-market environment as that of the AMARR system as these systems are designed for reverse auction scenario in the distributed e-market environment full of self-interested participants, and these systems also utilize concepts like reputation/dis-reputation thresholds for prefiltering and reward/penalty for honest/dishonest behavior. As shown in Figure 11, we first compared by simulating oscillations attack for two different products, namely laptop and pen drive.

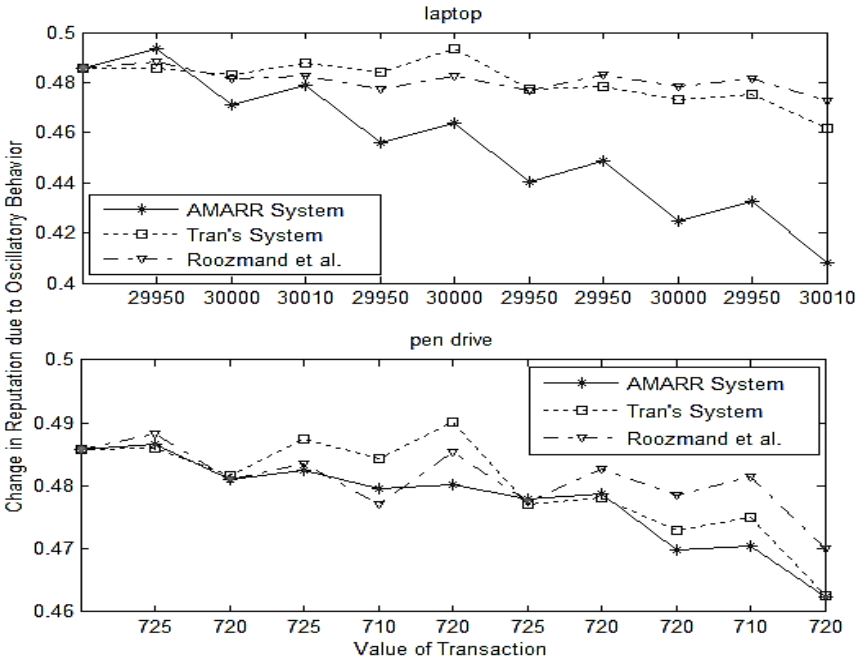

Figure 11: Handling oscillations (OC) attack

We observed that oscillations attack was fully neutralized, as the loss of reputation of seller s_2 due to alternative dishonest transactions was amply higher than the reputation gain due to its honest behavior in alternate transactions. For a small value product like pen drive, our AMARR system was a little better than the other two systems. But for a high value product like laptop, the AMARR system performed substantially better than others, as the penalty as well as reputation in our system are sensitive to value of the transaction.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

In a scenario reflecting Value Imbalance (VIM) attack, buyer b_1 and seller s_4 were involved in repeated mutual transactions for buying laptop and pen drive. For dishonest transactions, penalty in Tran [33] and Roozmand et al. [25] systems and base penalty in our AMARR system was kept at 1.8. During VIM attack, seller s_4 behaved honestly in a number of small value transactions for buying pen drive but dishonestly in case of a large value transaction for buying laptop. Due to intermittent fraudulent behavior, our system reflected an ample drop in Individual Reputation (IR) of s_4 as change in reputation was monotonically proportional to value of the transaction. It helped in neutralizing any incentive of such rogue behavior thus resolving the VIM problem as shown in Figure 12.

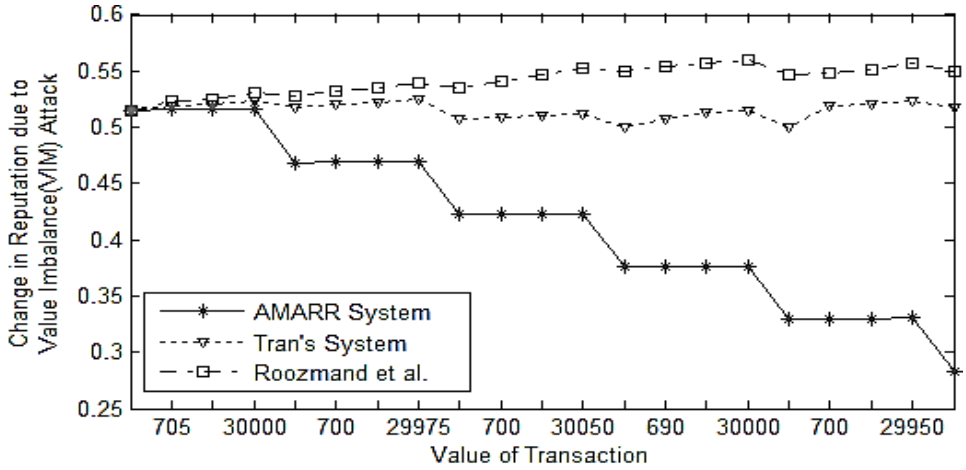

Figure 12: Resolving value imbalance (VIM) attack

Figure 12 also illustrates a sophisticated Oscillations attack where the seller behaved dishonestly only in case of relatively high value transactions to make the detection of its rogue behavior rather difficult. Tran [33] and Roozmand et al. [25] models performed poorly, but our AMARR system was able to defy this attack.

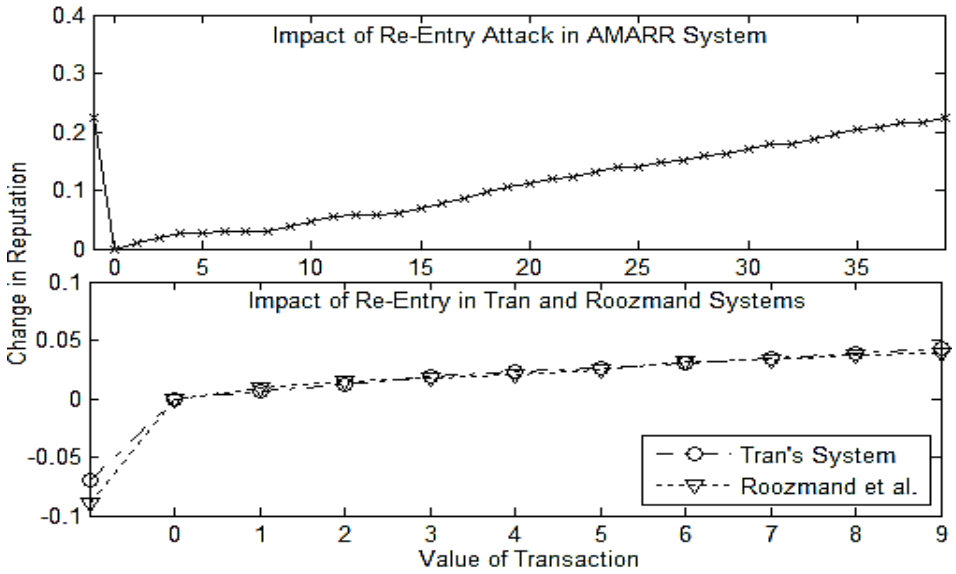

Figure 13: Impact of re-entry (REN) attack

We simulated a scenario for Re-Entry (REN) attack where seller s_5 exits from the e-market to disown bad reputation and re-enters with a fresh identity. The REN attack was launched using our AMARR system with a reputation range of [0,1] as shown in Figure 13, where s_5 worked for 39 transactions to regain its reputation of 0.224 with its previous identity as s_5. Therefore, it was observed that launching REN attack by frequent change in identity was beneficial for s_5 based on the AMARR system. Similarly, s_6 with reputation -0.07 launched REN using Tran [33], and s_7 with reputation -0.09 launched REN using Roozmand et al. [25]. Figure 13 reflects that in Tran's and Roozmand's strategies the seller actually gained reputation by launching REN, as in both these systems - the range of reputation is [-1,1], and a new seller started with a reputation of zero i.e. from the middle of the reputation range.

In a Ballot Stuffing (BS) attack, a number of transactions between buyer b_1 and seller s_6 were observed where BS was launched on b_1 after 1, 20, 30, 50, 75 and 90 transactions with an α incremental rate of 0.01. Figure 14 reflects

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

that the impact of BS reduced with the increase in number of mutual transactions between b_1 and s_6 as the weight of advisors' opinions reduced with each successive mutual transaction.

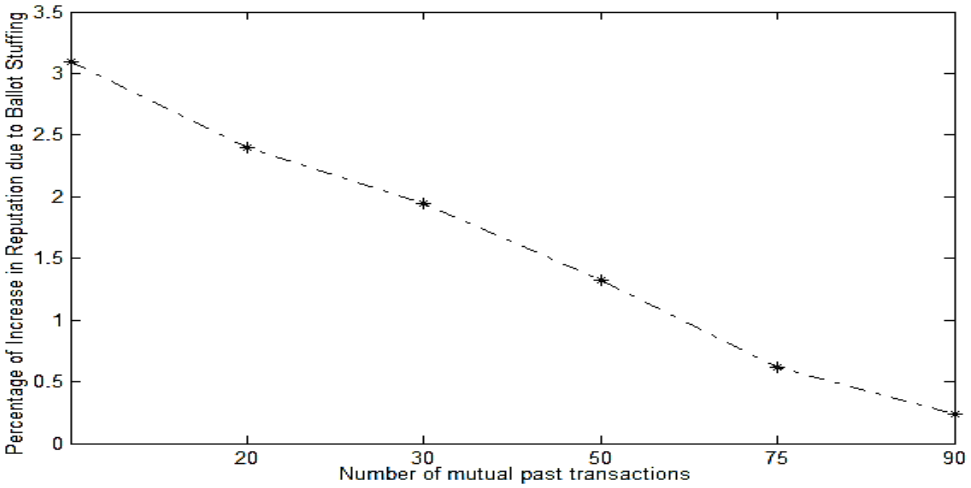

Figure 14: Reducing impact of ballot stuffing (BS) with increase in mutual past experience

In another situation reflecting a special case of Ballot Stuffing/Bad Mouthing attack in which majority of buying peers shared unfair opinions, buyer b_1 solicited opinions about the reputation of seller s_6 from other buying peers. As shown in Figure 15, buying peers were divided into three categories: honest, alternatively honest/dishonest, and dishonest. Among the nine buying peers, two *honest* buying peers always provided fair opinion, two alternatively honest/dishonest peers shared fair/unfair opinion alternatively, and the rest always shared unfair opinion.

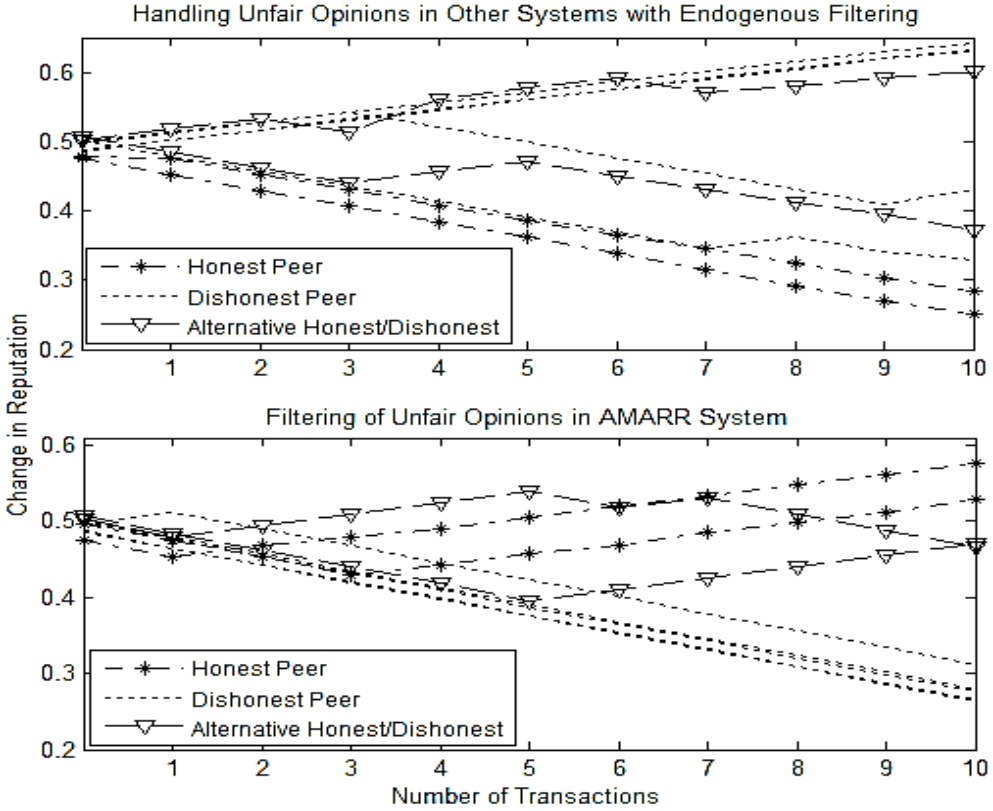

Figure 15: Filtering out unfair opinions in other systems and in the AMARR system

For filtering out unfair opinions we compared two strategies: Majority Rating scheme used in the literature that employs endogenous filtering of unfair information [15], [17], [19] and the Shared Reputation Methodology of our AMARR system that filters out unfair opinions based on their deviation from individual/self experience. We ran the simulation for a number of transactions between b_1 and s_6, though in Figure 15 we have shown the outcome of only first 10 transactions as afterwards the reputation of some buying peers moved below the reputation threshold. It was observed that by following the Majority Rating scheme based on endogenous filtering of information, reputation of

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

two honest buying peers suffered the maximum as due to the presence of a large number of unfair advisors, the mean of advisors ratings from which this method computed deviation was also biased towards unfair advisors. As a result, honest buying peers were filtered out, and peers who shared unfair information gained reputation. On the contrary, it is shown in Figure 15 that by following the Shared Reputation Methodology of our AMARR system (that filtered out unfair opinions based on their deviation from the self experience of the target seller), except for first few transactions, honest opinion providers got the maximum incentive in terms of their reputation as advisors being enhanced consistently with each transaction. Similarly, the dishonest advisors were penalized the most as their reputation decreased consistently, and finally moved below the reputation threshold of advisors.

8 Discussion

As e-commerce involves the exchange of money, the risk involved in distributed e-commerce transactions is much higher than other applications like P2P file sharing [9]. Further, with the increase in e-commerce transactions, the frequency of online fraud is also on the rise. In such an environment, keeping caution is not sufficient and participants of online transactions need a more proactive approach for their protection from fraudsters who often disguise themselves as honest potential partners. The risk involved in e-market transactions can be reduced by integrating attack-resilient features in the reputation design to enhance the trustworthiness of individual users as well as the whole reputation system.

This paper presented a novel approach to develop an attack-resilient reputation system in the distributed e-market environment full of self-interested buyers/sellers. The proposed reputation system proactively expects fraudulent behavior from different participants, especially sellers, and has improved protection for honest buyers as the proposed reputation computing methodology makes it unattractive for rogue sellers to indulge in such attacks.

Handling Re-Entry (REN) and Sybil attacks is actually a problem of identity management. Reputation systems try to handle these attacks by using mechanisms that are not based on their detection but by making it unattractive for the fraudulent participant to indulge in these attacks. The reputation system proposed in this paper is thus based on the approach of reducing the incentive to acquire new identities frequently, and it discourages REN attack for the following reasons. First, to re-enter the e-market with a new identity, an agent must begin from minimum reputation that means an enhanced RBC and thus reduced $NGds$ i.e. net gain to the rogue seller which results into minimized benefit for REN attack. Second, it sets the reputation/dis-reputation thresholds dynamically to ensure that for a big transaction and less trustworthy e-market, these thresholds are set to higher values thus needing an improved effort from a new seller to become reputed. Third, even after re-entering the e-market with a new identity, a seller has to show persistent honest behavior to ensure that its reputation rises above the dis-reputation threshold safely as showing dishonest behavior even once below dis-reputation threshold would result in the new seller being designated as a dis-honest seller and would never be considered again for business by that buyer. In the literature [3], [25], [29], [34], new sellers are assigned reputation that is more than the allowed minimum, which minimizes RBC and thus enhances the incentive of sellers to launch REN attack. To reduce REN, some online auction platforms [26] charge an entry fee from new sellers, and Kerr and Cohen [27] handle REN with partial success.

The proposed system uses the value of transaction as one of the fundamental factors for computing the reputation of a participant. It helps to resolve the Value Imbalance (VIM) attack as the extent of change in reputation is monotonically related to value of the transaction. It makes the reward and penalty for honest/dishonest behavior of sellers relative to the size of a transaction to make VIM attack in-effective. PeerTrust [20] and Trunits [27] recognize this factor for computing trust.

In our system, the impact of Reciprocity (REC) or Retaliation (RET) is limited by the value of a transaction, and the discounted change in reputation with each new successive transaction between a collusive buyer-seller pair. Commercial models like eBay have a strong presence of this attack as approximately 98% of the eBay ratings are positive due to the apprehension of RET attack.

The impact of Self Promoting (SP) attack is reduced in the proposed reputation system as by setting ε i.e. *mutual trustworthiness discount rate*, reputation earned by a seller due to repeated transactions with the same buyer is discounted with each successive mutual transaction. To the best of our knowledge, only Trunits [27] comprehend the significance of dealing with this problem.

Our system minimizes the impact of Sybil attack as reduced incentive for REN due to high RBC also discourages a rogue seller from acquiring multiple identities. With each new identity, a seller must work honestly to become reputed with an apprehension of being designated as a dishonest seller if its behavior is found unsatisfactory. Other systems [3], [25], [34] in which new sellers' initial reputation is more than the minimum reputation, have negligible RBC resulting into high incentive for sellers to launch Sybil attack.

Our reputation sharing strategy reduces the impact of Ballot Stuffing (BS) and Bad Mouthing (BM) with each successive transaction between a buyer-seller pair as weight of shared reputation decreases, and goes negligible when the buyer acquires enough experience of the seller. This strategy is sensitive to dynamic parameters of the e-market, and encourages an honest advisor by enhancing its reputation and the weight of its opinion with each

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 11 / ISSUE 1 / JANUARY 2016 / 46-66

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

successive honest advice. It filters out unfair ratings based on the deviation of advisors' opinions from the individual experience of the source buyer that enables the buyer to handle BS/BM even if majority of advisors are collusive. Existing systems [1], [3], [15] fail to handle these attacks if majority of raters are unfair.

The proposed system can handle Malicious Spies (MS) attack as participants are assigned reputation exclusively as advisors/information providers which is separate from their reputation as customers/traders. Systems in the literature [3], [15], [16] that do not differentiate between a participant's behavior as buyer/seller or as an advisor suffer from MS. By cautiously setting the minimum fixed penalty, and using a dynamic overall penalty that is sensitive to value of the transaction, the proposed reputation system minimizes the impact of Oscillations (OC) attack by a seller. It is based on the fact that to regain lost reputation, a seller has to behave honestly in large value and large number of transactions. This reduces the seller's incentive to launch OC attack. A summary of the built-in attack-resilience capablility of the proposed reputation system when compared to other systems from the literature is presented in Table 1.

Table 1: Comparison of attack-resilience in AMARR system with literature work

Type of Attack	**Attack-Resilience in AMARR System**	**Attack-Resilience in Other Systems**
Value Imbalance (VIM)	VIM is resolved as the amount of change in reputation is monotonically related to the value of a transaction.	Trunits [27] and PeerTrust [20] are sensitive to VIM.
Reciprocity (REC) and Retaliation (RET)	Its impact is minimized as reputation gain of a seller due to repeated transactions with a buyer is discounted with each new transaction. REC/RET is also limited by the value of transaction.	Commercial systems like eBay have a strong impact as 98% of eBay ratings are positive to avoid RET.
Re-entry (REN)	REN attack is partially resolved as high *RBC* results into low incentive for a rogue seller as the $NGds$ is reduced.	e-Bay and Trunits deal with this problem with partial success.
Multiple-Identity (MI) /Sybil	The benefit of minimized incentive of launching REN due to high *RBC* and reduced $NGds$ also spills to scenarios, where a participant tries to manipulate ratings through multiple identities.	Systems with initial reputation more than minimum possible rating [25], [29], [33] suffer from MI.
Reputation Lag (RLG)	The impact of RLG reduces as cheaters' reputation drops sharply due to dynamic penalty and dynamic reputation/dis-reputation thresholds. If a buyer gains enough experience of seller, it need not compute SR leading to quick computing of OR.	Systems based only on individual reputation [25], [27], [33] have lesser impact of RLG.
Ballot Stuffing (BS), or Bad Mouthing (BM)	The effect of BS/BM reduces with each successive transaction amid a buyer-seller pair as the weight of SR reduces and turns negligible when a buyer gains sufficient experience of the seller.	Few systems [4], [15], [16], [20] handle this attack with varying success.
Malicious Spies (MS)	MS impact is minimized as separate reputation is assigned to a user as an opinion provider, or as buyer/seller.	Very few systems (Regan & Cohen, 2005) provide reputation to advisors.
Self Promoting (SP)	It fairly handles SP attack as reputation earned by a seller for repeated transactions with a buyer is discounted with each successive mutual transaction.	No other system except Trunits [27], [28] explicitly recognizes this problem.
Oscillations (OC)	It minimizes the impact of OC by setting the penalty factor cautiously and, due to the sensitivity of the reputation function to value of transaction.	Systems having penalty greater than the reward [25], [33] give some solution.
Orchestrated (ORC)	Partial solution to a subset of attacks is possible as dealing multiple attacks with actors changing roles is very difficult.	No known solution for this type of multifaceted attacks.

The proposed system also minimizes the harm due to Reputation-Lag (RLG) attack as the IR as well as OR of rogue sellers reduce swiftly due to dynamic setting of both the penalty factor, and reputation/dis-reputation thresholds. Hence, a seller's deceitful behavior is rapidly detected due to a sudden drop in its OR. Further, when a buyer acquires sufficient experience of a seller, this system does not require the need to compute SR resulting into a reduced time lag in computing OR. Systems from literature [25], [27], [33], [34] that are based only on IR consisting of only direct evidence are not generally affected by RLG attack as there is no sharing of reputation among participants and therefore time gap between deceitful behavior and reduced reputation is less.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

Suitable setting of seller's reputation and dis-reputation thresholds in our system helps in accurate seller profiling. We set these thresholds using factors like buyer's risk taking ability, trustworthiness of e-market, and value of the transaction. Existing systems [3], [25], [33] use sellers' reputation/dis-reputation thresholds that are purely subjective for each buyer.

The proposed system would also be able to handle a combination of the subset of attacks to which the proposed system is resilient. For example, in an environment with a combination of Sybil and SP attacks, the proposed system would be able to handle as the proposed reputation sharing methdology elaborated in section 5.2 would be able to handle unfair reputaion sharing, and with each successive transaction between a buyer-seller pair, the discounted change in reputation while computing its IR reduces the impact of SP attack. However, at times the combination of attacks launched at a given time could be quite complex with a large and varying number of participants involved in the attack, and is known as Orchasterated (ORC) attacks in literature. In case of an ORC attack that involves launching of a number of attacks in parallel, the proposed system only helps to reduce its impact by handling a subset of these attacks, as handling multiple attacks with actors changing roles at different points of time is very difficult.

In addition to buyers, honest sellers must also be safeguarded in the e-market. A major risk of online sellers is that they may not get paid after delivering the product [11]. In our system, a seller delivers a product only after receiving the payment, hence the seller is protected from the payment concerns. But, full attack-resilience in an online environment cannot be realized just due to a sound reputation function as it requires an integrated approach involving identity management, authentication, and non-repudiation in the system [13]. Therefore, a good reputation system should encourage honest behavior, discourage rouge behavior, and allow protection of participants from various attacks.

The proposed reputation system incorporates built-in defense capability in the reputation computing methodology by increasing its resilience to various attacks, and by discouraging fraudulent behavior by slapping a high and dynamically computed penalty on dishonest sellers as compared to the corresponding reward for an honest behavior. The proposed reputation system can be further extended by applying it to different type of products. The reputation sharing strategy can be made more robust by exploring new strategies to filter out unfair opinions. In addition, investigating more complex interactions in the e-market, for example, exploring the e-market by allowing transactions to complete in more than one cycle with buyer-seller negotiation could be an interesting extension.

9 Conclusions

In this paper, we underlined the importance of attack-resilient parameters in a distributed reputation system for the e-market. In the e-market with self-interested participants, the proposed reputation system models the trustworthiness of participants using reputation functions that encourage honest behavior, where at the same time it ensures that the sellers who cheat the most are penalized the most.

The attack-resilient parameters in the proposed reputation system are sensitive to the changing parameters of e-market like the experience of agents and the value of a transaction. One of the main contributions of the proposed system is to compute the reputation of the sellers in such a way that the benefits of rogue sellers are minimized thus making it unattractive to indulge in fraudulent behavior. This is achieved by dynamically setting the reputation and dis-reputation thresholds for sellers, by introducing effective reputation value increase/decrease factor, by dynamically setting the appropriate penalty factor, and by reducing the incentive for launching Re-Entry, Oscillations, Value-Imbalance and collusion based attacks. In the proposed reputation system, the increase in transactional experience leads to increased weight of individual reputation, and honesty in a large value transaction leads to a higher increase in reputation as compared to a small value transaction. Fraudulent sellers are penalized with relatively large and swift drop of reputation resulting into quick detection of their fraudulent behavior and reduced future business opportunities. Our system also assigns reputation to advisors to safeguard buyers not only from rogue sellers but also from deceptive advisors.

References

[1] W. H. Chang and J. S. Chang, An effective early fraud detection method for online auctions, Electronic Commerce Research and Applications, vol. 11, no. 4, pp. 346-360, 2012.
[2] C. B. Cheng, Reverse auction with buyer-supplier negotiation using bi-level distributed programming, European Journal of Operational Research, vol. 211, no. 3, pp. 601-611, 2011.
[3] C. Dellarocas, Reputation mechanisms, in Economics and Information Systems, vol. 1, Handbooks in Information Systems (T. Hendershott, Ed.). Bingley, UK: Emerald Group Publishing Limited, 2006, pp. 629-660.
[4] V. Gaur and N. K. Sharma, A dynamic seller selection model for agent mediated e-market, in Proceedings of International Conference on Advances in Computing and Communication (ACC 2011), Part II, CCIS 191, Kochi Kerala, India, 2011, pp. 284-295.
[5] S. C. Gupta, Fundamental of Statistics. New Delhi, India: Himalaya Publishing House, 2005.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762016000100004

[6] C. J. Hazard and M. P. Singh. (2009, November) Reputation Dynamics and Convergence: A Basis for Evaluating Reputation Systems, 2009. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.157.5233
[7] K. Hoffman, D. Zage and C. Nita-Rotaru, A Survey of Attack and defense techniques for reputation systems, ACM Computing Surveys, vol. 42, no. 1, pp. 2-19, 2009.
[8] T. D. Huynh, N. R. Jennings and N. R. Shabolt, An integrated trust and reputation model for open multi-agent systems, Journal of Autonomous Agents and Multi-Agent Systems, vol. 13, no. 2, pp. 119-154, 2006.
[9] A. Josang and R. Ismail, The beta reputation system, in Proceedings of 15th Bled Electronic Commerce Conference, Bled, Slovenia, 2002, pp. 1-14.
[10] A. Josang, R. Ismail and C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[11] R. Kerr and R. Cohen, Modeling trust using transactional, numerical units, in Proceedings of The Conference on Privacy, Security and Trust, Article No. 21, Markham, Canada, 2006, pp. 1-11.
[12] R. Kerr and R. Cohen, Smart cheaters do prosper: Defeating trust and reputation systems, in Proceedings of AAMAS 2009, Budapest, Hungary, 2009, pp. 993-1000.
[13] J. I. Khan and S. D. Shaikh, A phenotype reputation estimation function and its study of resilience to social attacks, Journal of Network and Computer Applications, vol. 32, no. 4, pp. 913-924, 2009.
[14] E. Koutrouli and A. Tsalgatidou, Taxonomy of attacks and defense mechanisms in P2P reputation systems - lessons for reputation system designers, Computer Science Review, vol 6, no. 2-3, pp. 47-70, 2012.
[15] O. Kussul, N. Kussul and S. Skakun, Assessing security threat scenarios for utility-based reputation model in grids, Computers & Security, vol. 34, pp. 1-15, 2013.
[16] S. Lee, K. Choi and Y. Suh, A personalized trustworthy seller recommendation in an open market, Expert Systems with Applications, vol. 40, no. 4, pp. 1352-1357, 2013.
[17] R. Maranzato, A. Pereira, A. P. D. Lago, and M. Neubert, Fraud detection in reputation systems in e-markets using logistic regression, in Proceedings of 25th ACM Symposium on Applied Computing, SAC'10, March 22-26, Switzerland, 2010, pp. 1454-1455.
[18] F. G. Marmol and G. M. Perez, Security threats scenarios in trust and reputation models for distributed systems, Computers and Security, vol. 28, no. 7, pp. 545-556, 2009.
[19] J. Patel, W. T. L. Teacy, N. R. Jennings, and M. Luck, A probabilistic trust model for handling inaccurate reputation sources, LNCS 377, in Proceedings of Third International Conference on Trust Management, Paris, France, 2005, pp. 193-209.
[20] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, Numerical Recipes: The Art of Scientific Computing, 3rd Edition. New York: Cambridge University Press, 2007.
[21] K. Regan and R. Cohen, Designing adaptive buying agents in electronic markets using advice from other buyers to model seller reputation, Journal of Business and Technology, vol. 1, no.1, 1-10, 2005.
[22] P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood, The value of reputation on eBay: A controlled experiment, Experimental Economics, vol. 9, no. 2, pp. 79-101, 2006.
[23] O. Roozmand, M. A. Nematbakhsh and A. Baraani, An Electronic marketplace based on reputational and learning, Journal of Theoretical and Applied E-Commerce Research, vol. 2, no. 1, pp. 1-17, 2007.
[24] J. Sabater and C. Sierra, REGRET: Reputation in gregarious societies, in Proceedings of the Fifth International Conference on Autonomous Agents, Canada, 2001, pp. 194-195.
[25] C. Selvaraj and S. Anand, A survey on security issues of reputation management systems for peer-to-peer networks, Computer Science Review, vol. 6, no. 4, pp. 145-160, 2012.
[26] M. Srivatsa and L. Liu, Securing decentralized reputation management using trustguard, Journal of Parallel Distributed Computing, no. 66, vol. 9, pp. 1217-1232, 2006.
[27] J. M. Such, A. Espinosa, A. Garcia-Fornes, and V. Botti, Partial identities as a foundation for trust and reputation, Engineering Applications of Artificial Intelligence, vol. 24, no. 7, pp. 1128-1136, 2011.
[28] T. Tran, Protecting buying agents in e-marketplaces by direct experience trust modelling, Knowledge and Information Systems, vol. 22, no. 1, pp. 65-100, 2010.
[29] T. Tran and R. Cohen, Improving user satisfaction in agent-based electronic marketplaces by reputation modeling and adjustable product quality, in Proceedings of AAMAS'04, New York, 2004, pp. 828-835.
[30] J. C. Wang and C. C. Chiu, Recommending trusted online auction sellers using social network analysis, Expert Systems with Applications, vol. 34, no. 3, pp. 1666-1679, 2008.
[31] F. Wu, H. H. Li and Y. H. Kuo, Reputation evaluation for choosing a trustworthy counterparty in C2C e-commerce, Electronic Commerce Research and Applications, vol. 10, no. 4, pp. 428-436, 2011.
[32] L. Xiong and L. Liu, PeerTrust: Supporting reputation-based trust for P2P electronic communities, IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, 2004.
[33] B. Yu and M. P. Singh, An evidential model of distributed reputation management, in Proceedings of AAMAS'02, Bologna, Italy, 2002, pp. 294-301.
[34] B. Yu and M. P. Singh, Detecting deception in reputation management, in Proceedings of AAMAS'03, Melbourne, Australia, 2003, pp. 73-80.
[35] J. Zhang and R. Cohen, Evaluating the trustworthiness of advice about seller agents in e-marketplaces: A personalized approach, E-Commerce Research and Applications, vol. 7, no. 3, pp. 330-340, 2008.
[36] M. Zhou, M. Dresner and R. J. Windle, Online reputation systems: Design and strategic practices, Decision Support Systems, no. 44, vol. 4, pp. 785-797, 2008.