3 ANALYSIS, DESIGN & EXPERIMENTAL STUDY

3.1 Prologue

There are a limited prevailing reputation aware online systems such as the evaluations of e-bay, yahoo auction, and auction existence. The Majority of these systems utilize the single trust factor of feedbacks as reputation strategy, which frequently fails to control the credibility of users efficiently.

One of the initial works in this expanse is the protocol by Aberer as well as Despotovic[41], which aims to recognize dishonest providers by a complaint-based strategy. A drawback of this protocol is that it keeps only the unwanted feedbacks, offering no signifies for a trusted agent to be recognized from a arrival. The trust assessment is also quite simplistic, categorizing most agent perhaps as excellent or untrust worthy. Further more, upkeep of a P-Grid, architecture needs on top of the prevailing P2P structure. Eigen Trust version puts ahead the dispensed computing technique based on DHT[31], making use of the trust algorithm that determines global trust benefits by straight trust value with trust exchange characteristics, but this version exists overlap problem, and possess the higher communicating cost and proportional value of global status, it produces are unable to directly judge either the agent is credible starting the global reputation benefits. Zhou etc. [55] enhance the Eigen Trust version for the elements of motivation of credible providers and the speed of trust version convergence, and leaves forward the Power Trust version. In opposition of the malicious agents component, this model effective than Eigen Trust algorithm, however in the computation of trust benefits, it doesn’t choose the impact of the trust value on dealing volume, and has not to attain discipline formalicious attitude.

Agent Trust model purpose the assurance factor to synthesize local reputation as well as global reputation, enable for numerous factors which might influence dimension of trust, and can manage with false assessment very perfectly, but Agent Trust
system does not give evaluate method of trust factor and technique for ensuring confidence factor. Confidence has been resolved at assorted levels by numerous researchers. In conduct-based trust model is recommended in which trust is calculated by receiving into account the straight trust, reputation and decay function. The assorted parameters similar to number of operations for the assorted types of information are not deemed.

Jøsang etc. offer the approach of multiple-valued logic depending on the subjective logic, using Dirichlet multidimensional possibility distribution as the basis, enabling to have a variety of grades assessment, which can be utilized for the estimation of reputation value, offer more flexible program for design of reputation strategy. But the product only uses direct assessment result to determine trust degree, lacking because endorsement trust, and how to recognize malicious assessment and give it abuse.

Nowadays, the maximum trusted models assess level of trust regarding service provider agents. In the human environment, when people select and buy a asset, the first focus is regardless the purpose of the goods to satisfy their needs, and then choose other attributes of the goods, like as price, the brand value, appeal, functionality, after-sale service and so on, subsequently purchase the items corresponding to needs oneself and complete evaluation of each and every property.

Obtained items, if the attributes of the goods are disciplined with vendors reported, the vendor is deemed as trustworthy. In perspective of the preceding questions, we offer a reputation based energetic trust evaluation version that assesses multiple service characteristics offered by service provider dependent on personal attention, and merges with the trust value, consider regardless to trade subsequently; after the transaction, service requester determines amount of fulfillment according to specific QoS and service provider’s own QoS claimed to judge the trust worthiness of service provider, then provides equivalent rewards and discipline, and trust update.
3.2  A reputation based agent selection strategy for multi agent communication system

Here we devised a model to encapsulate the reputation of both the agent that respond and the agent that request. The proposed protocol avoids spiteful elevation of the agent’s reputation. It also manages the issue of highly inconsistent accessibility pattern of the agents in multi agent communication based systems.

3.2.1  Selecting response agent by its reputation:

The supplicant Agent \( spt \) that requires information selects the respondent agent \( rpt \) with the utmost reputation, then agents \( spt \) and \( rpt \) estimates mutual trust by exchanging their reputation.

A message \( msg \) sent by ‘\( spt \)’ to ‘\( rpt \)’ can be denoted as \( spt \rightarrow rpt : msg \)

\( puk_{rpt} \) Represents the public key of the agent \( rpt \)

\( prk_{rpt} \) Represents the private key of the agent \( rpt \)

The agent \( spt \) sends the request \( rq \) along with its identity \( spt_{idt} \) to all other agents possible to respond, which is by encrypting with public key of each \( rpt \)

\( spt \rightarrow \bigcup_{i=1}^{n} \text{rpt}_i : E_{\text{pk}_{\text{rpt}_i}} (spt_{idt}, rq, H(spt_{idt}), H(rq)) \)

Here in the above equation \( H(spt_{idt}), H(rq) \) represents the one way hash of the agent \( spt \) identity and the request \( rq \) respectively
Upon receiving the message sent by \( spt \), the agent \( rpt \) decrypts it by \( prk_{\text{rpt}} \) and checks the request \( rq \), if willing to respond, then the agent \( rpt \) verifies the self-assessed identity of the \( spt \),

If ‘\( spt_{\text{uth}} \)’ is valid then it verifies its reputation as supplicant. Upon finding the satisfactory reputation of the supplicant \( spt \), the agent \( rpt \) sends an encrypted message \( rmsg \) to supplicant \( spt \). The message \( rmsg \) contains encrypted form of identity of agent \( rpt \), reputation score \( rs \), recent reputation updates frequency \( ruf \), and reputation update divergence threshold \( rudt \) along with the one way hash values of all these.

\[
\bigcup_{i=1}^{n} \text{rpt} \rightarrow \text{spt} : E_{\text{pub}_{\text{rpt}}} (\text{rpt}_{\text{pth}}, \text{rpt}_{\text{rsh}}, \text{rpt}_{\text{ref}}, \text{rpt}_{\text{ruft}}, \text{H}(\text{rpt}_{\text{uth}}), \text{H}(\text{rpt}_{\text{rs}}), \text{H}(\text{rpt}_{\text{ref}}), \text{H}(\text{rpt}_{\text{ruft}}))
\]

Upon receiving response messages from all possible agents, the supplicant agent \( spt \), verifies their identity and picks response agents with valid identity, and then measures the credibility of those valid response agents by estimating their reputation \( rep \). The digital certificate of the response agent \( rep \) will be verified as follows:

\[
\text{rpt}_{\text{sig}} \simeq \text{H}(\text{rpt}_{\text{rs}} + \text{rpt}_{\text{salt}})
\]

Here in above equation \( \text{rpt}_{\text{sig}} \) represents the signature of the agent \( \text{rpt} \) available with agent \( spt \) and \( \text{H}(\text{rpt}_{\text{rs}} + \text{rpt}_{\text{salt}}) \) is one way hashing of the most recent updated reputation score of the \( \text{rpt} \) and salt used to generate the digital certificate signature of the agent \( \text{rpt} \), which is by recent supplicant agent that accepted response from agent \( \text{rpt} \).

The reputation \( rep \) of the response agent \( \text{rpt}_{i} \) can be measured as follows:
Here in above equation \( \text{ruds}_{\text{rpt}} \) represents the response update divergence score, which indicates the divergent number of supplicants involved to get the reputation score \( r_s \) of the agent \( \text{rpt}^i \).

\[
\text{ruds}_{\text{rpt}} = 1 - \frac{\text{rpt}^i_{r_s}}{\text{rpt}^i_{\text{rudt}}}
\]

Here in the above equation \( \text{ruf}_{\text{rpt}} \) indicates the reputation update frequency score of the agent \( \text{rpt}^i \), reputation update frequency refers the ratio of response to requests received.

\[
\text{ruf}_{\text{rpt}} = 1 - \frac{\text{rpt}^i_{r_s}}{\text{rpt}^i_{\text{orf}}}
\]

Finally supplicant agent \( spt \) opts to an agent \( \text{rpt} \) for response, if and only if \( \text{rep(\text{rpt})} \) is maximal than of any other agent with valid identity.

**3.2.2 Updating Reputation:**

Once the agent \( spt \) receives required information from agent \( \text{rpt} \), then supplicant agent \( spt \) initiates to update the reputation score of the responding agent \( \text{rpt} \). According to the scope of the response received from the agent \( \text{rpt} \), the supplicant agent \( spt \) fixes the reputation score of the response as -1, 0 or 1. (i) If response given by agent \( \text{rpt} \) is assessed as valid and helps to the further functional needs of the supplicant agent \( spt \), then reputation score of the response as \( \eta_{r_s} + 1 \), (ii) If the response is not helpful, but the intension of agent \( \text{rpt} \) is not suspicious, then reputation score of the response is
\( r_{rs} + 0 \), (iii) The response sent by agent \( rpt \) is suspected as malicious with an intention of falsifying the further functionality of the supplicant agent \( spt \), then the reputation score of the response is \( r_{rs} - 1 \).

Further the supplicant sends the message to \( rpt \), which is regarding reputation score update. The agent \( rpt \) accepts the given reputation score by a blindfold approach. The supplicant agent \( spt \) sends a message to \( rpt \) as follows:

\[
\text{umsg} = \{ E_{ekey}(\text{repscore}, s_{idt}), H(\text{repscore} + \text{salt}), H(s_{idt}) \}
\]

\( spt \rightarrow rpt : \text{umsg} \)

Here in the above equation, \( E_{ekey} \) represents the encryption process that encrypts by using the key \( ekey \), which is of the key pair \( \{ ekey, dkey \} \). The message contains the encrypted form of the reputation score given by supplicant agent \( spt \) against to the response given by agent \( rpt \), the identity of the supplicant agent and the one-way hash values of the both reputation score and identity. To avoid the conditional acceptance of the reputation score by response agent \( rpt \), here supplicant agent sends it in encrypted format. Upon receiving the message, the agent \( rpt \) accepts \( H(\text{repscore} + \text{salt}) \) as signature of the digital certificate and acknowledges the same by sending that certificate back to supplicant agent \( spt \). Then supplicant agent \( spt \) shares a message \( \text{msg} \) with all other agents. The message \( \text{msg} \) contains the identity of the agent \( rpt \) and the new signature of the digital certificate of the agent \( rpt \) is shared with all other agents. Then supplicant agent \( spt \) sends the decryption key of the key pair \( \{ ekey, dkey \} \) along with \( \text{salt} \) to the response agent \( rpt \).
Upon receiving $dkey$, the agent $rpt$ decrypts the encrypted message part of the ‘$umsg$’ and updates its reputation score ‘$rs$’, ‘$ruf$’ and ‘$rudp$’. Further includes the ‘$salt$’ to digital certificate that used to generate the signature of that digital certificate.

3.3 Performance analysis

We performed experiments to evaluate proposed reputation system and show its feasibility, effectiveness, and benefits. The experiments evaluate proposed reputation based agent selection in terms of its accuracy and the benefit of Reputation based agent selection model when it is used in a distributed community. Each agent in the simulation stores the values obtained for factors those used in reputation assessment. The javafx used to simulate the distributed system with multi agents. An agent collects the data related to parameters used in reputation assessment and conducts the reputation evaluation on the fly when needed. The approximate computation is used for the reputation evaluation.

The objective of this set of experiments is to evaluate the effectiveness of the Reputation model with basic parameters and understand how the malicious behavior and transaction skew in the community affect its performance. We compare proposed approach to the conventional approach called Agent-UNO [53] in which only the first parameter, i.e. the amount of satisfaction, is used to measure the trustworthiness of an agent. The Design diagrams and simulation screen cast explored in Appendix-A

The Figure 1 shows the ratio of services successfully completed with positive or neutral reputation in proposed reputation based agent model and its performance advantage against Agent UNO strategy [53]. The service completion advantage of proposal over Agent UNO is 1.5% more.
Figure 1: The service completion under positive or neutral reputation proportionality observed in proposed reputation based agent selection

Figure 2: The Malicious agents’ avoidance during respondent selection

The Figure 2 maps proposed agent selection strategy against Agent UNO in agent selection optimality. The proposed model has an edge as Agent UNO used the ratio of
0.31 more respondent selection requests compared to proposed reputation based agent selection strategy.

![Payload against respondent selection](chart.png)

Figure 3: Process cost of Service completion by selecting reliable respondent.

The Figure 3 shows that proposed strategy has considerably lesser payload expenses over Agent UNO, which is due to its reliable respondent selection strategy where the excessive payload garnered in proposed reputation based agent selection strategy compared to Agent UNO is lesser by 6.1%.

Figure 4 represents the trust evaluation accuracy of the two models with respect to the malicious behavior factor in the community. We can make a number of interesting observations. First, Reputation based Agent Selection and the Agent-UNO approach perform almost equally well when the malicious behavior factor is low. This is because the Agent-UNO approach relies on there being a large number of trustworthy peers who offer honest statements to override the effect of the false statement provided by the untrustworthy peers and thus achieves a high accuracy. Second, as the malicious behavior factor increases, Reputation based Agent Selection stays effective while the performance of the Agent-UNO approach deteriorates. This can be explained as follows. When the malicious behavior factor in the community increases, the chances for trustworthy peers to interact with untrustworthy peers and receive fake complaints increase. Since the
Agent-UNO approach only uses the number of complaints for computing the trustworthiness of peers and does not take into account the credibility of the complaints, the trustworthy peers with fake complaints will likely be evaluated as untrustworthy incorrectly. On the contrary, Reputation based Agent Selection uses the credibility factor to offset the risk of fake complaints and thus is less sensitive to the misbehaviors of untrustworthy peers.

Figure 4: The comparison of trust evaluation accuracy against malicious agent behavior ratio between Reputation Based Agent Selection and Agent-UNO

Figure 5 represents the trust evaluation accuracy of the two models with respect to the transaction skew factor in the community that indicates the variation in count of requests raised in parallel. When the transaction skew factor increases, Reputation based Agent Selection stays effective while the performance of the Agent-UNO approach deteriorates. This demonstrates the importance of the number of transactions when computing the trustworthiness of peers. The Agent-UNO approach is very sensitive to the transaction skew because it does not take into account the number of transactions in their trust metric.
Figure 5: The comparison of trust evaluation accuracy against divergent skew factor of parallel requests (skew factor 0 indicates all requests are parallel) between Reputation Based Agent Selection and Agent-UNO.

Figure 6 shows the transaction success rate with the average number of transactions each agent has at current time. The graph presents a number of interesting observations. First, we see an obvious gain of the transaction success rate in both communities equipped with a trust mechanism. This confirms that supporting trust is an important feature in an eCommerce community. Second, the Agent-UNO trust metric is not as effective as Reputation based Agent Selection. This also matches the results from the previous experiment. Third, it is also interesting to observe that the transaction success rate increases over the time in the community with Reputation based Agent Selection and then stays stable. This is because as agents interact with each other over the time, agents successfully select trustworthy agents to interact. The untrustworthy agents deterred from participating in transactions. On the other hand, the transaction success rate increases first and then drops before going stable in the community with Agent-UNO method. This is because agents make wrong evaluations due to the limitations of the method and in turn choose untrustworthy agents to interact with before the system gets stable.
Figure 6: The comparison of transaction success ratio against average of agent level transactions between Reputation Based Agent Selection and Agent-UNO.