Design of a Trusted Auction System Using Relationship-based Internet Community

Kun-Woo Yang, Soon-Young Huh
Korea Advanced Institute of Science and Technology

Abstract

The explosive growth of the internet-based transactions requires not only a secure payment system but also an appropriate trust measuring methodology and secure transaction protocols to guarantee the minimal risk for the transacting entities involved in specific transactions. Especially, in internet auction systems where either buyers or sellers or both can be more than one in one transaction, providing those systems that make sure no one transacting entity takes a major risk becomes critical. In this paper, an improved trust measuring system using a relationship-based internet community for an auction system is proposed. The proposed system incorporates fuzzy set and calculation concepts to help build trust matrices and models, which is used to measure the level of risk involved in a specific auction trade concerned. Also, this paper devises a set of trade protocols for auction systems to recommend a proper trade protocol according to the risk level involved. To test the appropriateness of the proposed trusted auction system, a prototype system has been developed under a Windows-NT environment.

Keywords: trust measure, auction system, fuzzy logic

1. Introduction

The explosive growth of internet users and related technology advances have enabled many corporations to do online businesses in many different forms. Consequently, not only the number of internet-based transactions but also the total trade volume resulted from those online transactions has been increased tremendously. Even if internet commerce is getting popular, it is still far from its potential for growth mainly because of the lack of trust in the online environment (Hoffman et al., 1999). Since anyone on the internet can set up an online store and sell products or services, it is also very important to have an appropriate way to measure the trust level of the involving parties (Manchala, 1998; Manchala, 2000; Su and Manchala, 1997).

Especially, in internet auction systems where many buyers and sellers can trade many different items at the same time, understanding what causes trust and how (Doney and Cannon, 1997; Hoffman et al., 1999; Mayer et al., 1995) and providing a proper procedure to protect users, both buyers and sellers, from any monetary losses is critical to success as an internet auction service provider. Currently, escrow services, insurance services, authentication, and security protocols are used as transaction party protection methods. For instance, Yahoo.com and eBay.com, which are providing auction services, have strategic alliances with iescrow.com to protect their users involved in auction trades by providing escrow services optionally. However, application of those additional protecting mechanisms should be dependent on the trust level of the transaction parties and the value of each trade because using those additional services causes extra costs and also it may slow down the auction trade process. Therefore, to optimize an internet auction process, a systematic approach incorporating a reasonable trust measurement and trade procedure recommendation is needed.

In this paper, we propose a Trusted Auction System, which can measure the trust level of transaction parties and the trades themselves both quantitatively and qualitatively. Additionally, the proposed system can recommend a trade protocol, which both a buyer and a seller can follow to protect themselves, based on the measured trust level of each auction trade. To measure the trust level of each auction trade, we adopt many trust variables including user profiles of relationship-based internet community to overcome the shortcomings of using simple transaction history as a trust measuring criterion. In processing many trust variables and calculating a trust level, this paper adopts fuzzy theory to transform vague trust values based on various trust variables into the overall trust level. Input values for each trust variable take either quantitative or qualitative forms. Fuzzy theory provides a systematic approach to process qualitative variables sometimes having even vague descriptive verbal expressions for input values (Zadeh, 1973).

This paper is organized as follows. Section 2 reviews previous researches regarding trust measuring for electronic commerce using a trust matrix and a relationship-based internet community. In section 3, we explain how we can adopt the relationship-based community system for measuring trust levels among transaction parties. Also, the overall Trusted Auction System architecture is proposed with detailed explanation of each sub-component of the system. Section 4 covers the appropriate trade protocol recommendation based on the measured trust. Finally, section 5 summarizes the paper and future research topics regarding improving the proposed auction system.

2. Related Works

2.1. Trust measures for electronic commerce

Measuring the trust level of buyers and sellers has been researched as one of authentication methods using public key infrastructure. Also, many researches have focused on using matrices for measuring trust such as PGP (Stallings, 1995), PEM (Kent, 1993), Maurer (Maurer, 1996), Beth-Yahalom (Yahalom and Klein, 1997). Reiter and Stubblebine identified the problems with the simple procedural authentication process based on key exchanges and proposed a new authentication process using matrices (Reiter and Stubblebine, 1997).

In Su and Manchala's research (1997), a trust measuring method based on a trust matrix was proposed. In that paper, terms used in trust measuring were defined as follows. A transacting entity is anyone involved in an electronic commerce transaction including buyers, sellers, intermediaries, and etc. A trust authority is an institution that authenticates the integrity of transacting entities. Transacting entities get authenticated through trust protocols from trust authorities. An agreement framework is a document that defines the relationship among all the stakeholders in the transaction and terms and conditions of the transaction, which is recorded in the involved trust authority.

To secure the appropriate trust level for each online transaction, an independent trust certificate authority should be established to certify the trust level of all the transacting entities involved in the transaction concerned (Manchala, 1998). To measure the trust level of any transacting entity, trust variables such as cost of transaction, transaction history, customer loyalty, and indemnity from independent institutions are used and trust actions are defined accordingly.

Choosing proper trust variables is the key to measuring the exact trust level of the transaction involved. Su and Manchala (Manchala, 2000; Su and Manchala, 1997) introduced Electronic Commerce Trust Relationship (ECTR) matrix, which defined relationship between variables showing the status of transacting entities and ones concerning a transaction itself. In ECTR matrix, the resulted relationship is shown as a trust action. Based on the calculated trust level, involving transacting entities can choose an appropriate trust action, which includes the verification of each process in the transaction like payment or delivery. Since this additional verification process requires additional costs, this additional cost-bearing process is adopted only when needed in case of a low trust level. Depending on the trust level of the involving transacting entities, the security level used in the trade information exchanges on the network is differentiated. For example, a transaction with a low monetary value and a high trust level should adopt a simple hash function such as MD5 (Rivest, 1992) to encrypt payment information. On the contrary, for a transaction with a high value and a low trust level, a higher security scheme such as SET is to be used.

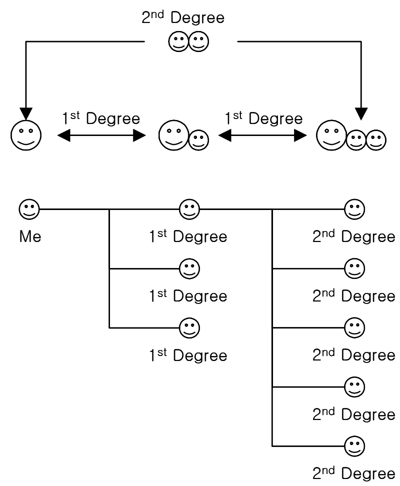
2.2. Relationship-based internet community

An internet community service is providing the space on the internet where internet users can get together, create useful information by themselves and share it. Among all the online services including contents providers, community services, communication services and internet shopping malls, an internet community is considered the most effective one for recruiting new members and keeping them. This is mainly due to the network externality the community service has once it is established among people having common interests.

However, an internet community service has a problem of anonymity, which can cause serious problems especially when it is involved with electronic commerce. People who do not want their personal information to be accessed freely by other people may not enter correct information about themselves when they get membership for the community sites. This possibility of membership with incorrect member information may lead to malicious activities such as indecent content posting on the bulletin boards. When it comes to the electronic commerce transactions, the problem gets complicated because it may cause a monetary loss to one side of the transaction. To stop these fraudulent activities, online community services try hard to make their members to input correct personal information when they get their membership because people are reluctant to get involved in any activities that may damage their dignity when their true identities are open.

Relationship-based community services overcome such an anonymity-related problem to a certain level by making their members provide their correct information voluntarily. For example, in community services such as sixdegrees.com and cyworld.com, a person that one knows directly can be linked with a first-degree relationship. Likewise a person that one is linked through a first-degree relationship will have a second-degree relationship with him or her. Members of relationship-based communities are encouraged to provide correct information about themselves because they can be directly linked to people they know only when they have correct identities on the specific community. Consequently, the community site providing such a service has high potential to be a good intermediary for safe online transactions. Figure 1 shows the relationship concept in a relationship-based community service. The left-most circle represents a person and circles directly connected to the left-most one shows the people that have first-degree relationships with the person.

[Figure 1] Example of Relationship-based Internet Community



3. Design of a Trusted Auction System

We define a Trusted Auction System as one that provides a better mechanism to perform trades with a secure protection method for transacting entities by reducing the possibility of fraudulent activities of conventional auction systems. The characteristics of the proposed system are summarized as i) trust level quantification of transacting entities using a fuzzy expert system, ii) introduction of new trust measuring variables using relationship-based communities, iii) measurement of the trust level of each auction trade itself not only that of transacting entities, and iv) recommendation of proper trade protocols based on the trust measurement.

3.1. Applicability of relationship-based internet community

The relationship-based internet communities provide basic community services such as bulletin boards, real-time chatting, online polls, and so forth. The most unique characteristic that differentiates relationship-based communities from other conventional ones is the fact that members within the community can be connected based on their true relationships in real world. For instance, friends in a real life can be connected as friends in the online community and those direct relationships are defined as the first-degree relationship. Also people with the second-degree relationship can be one person's mutual friends that have a first-degree relationship with that person on their own. In this sense, we may consider that the number of degrees defined in the community represents the closeness of people connected with the relationship.

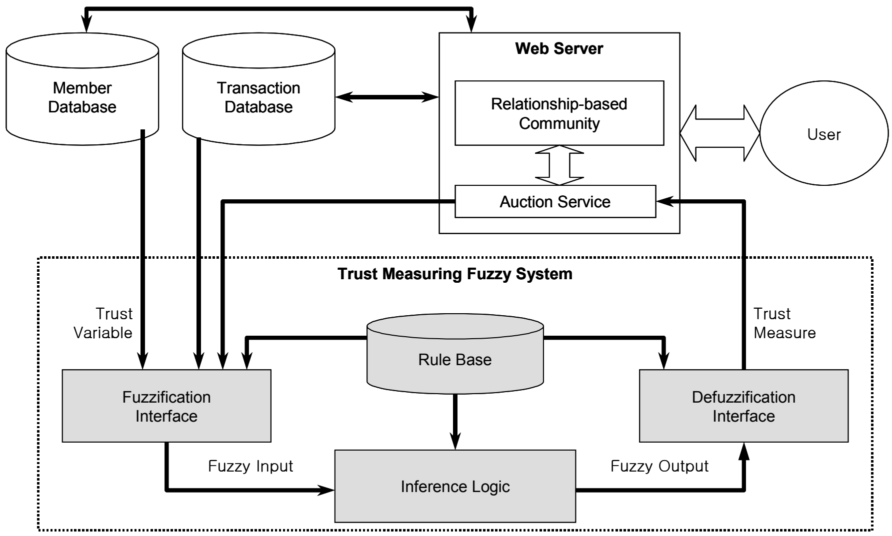
There are generally two major categories of fraudulent activities related to the online auction transactions. The one is not paying for the items one bought after receiving them and it can be viewed as a fraudulent activity of buyer's side. The other is a seller's side fraudulent activity, which is not sending sold items after receiving the proper payment for the items. Since those kinds of intended fraudulent practices may hurt the reputation of the entire site that provides online auction services, providing an effective way to protect all the transacting parties, either buyers or sellers, is critical to succeed in the business. Therefore, most of well-known auction services enable one to view previous transaction history of the other party to make him or her decide whether or not to do the auction trade with that person on his or her own. Some of sites are making people rank the auction trade using a scale such as "satisfactory," "neutral" or "unsatisfactory" and then those recorded scores are displayed later for reference when that person tries to engage in another auction trade.

Most of online trade fraudulent activities are due to the anonymity of internet because people with malicious intents would not commit crimes if their real identities were open to the public. In this sense, the profile information such as the number of first-degree relationships and average number of visits to the site in the relationship-based internet community can be a good candidate for trust measuring variables since it can be considered that those values show the loyalty level of that person. As mentioned previously, members in the relationship-based communities tend to provide their correct personal information to maximize network effects and they must be reluctant to make any malicious actions because their personal information is open.

3.2. Overall architecture of Trusted Auction System

The proposed Trusted Auction System can be divided into two sub components. The one is part that provides the relationship-based community service along with a conventional auction service. So members of the community are able to use auction services exactly the same way they do in other auction sites. The other part, which is integrated with this community service, is a trust measuring fuzzy system that measures trust level of each trade in real time to provide the risk level involved with the specific auction trade and recommend an appropriate trade protocol. Figure 2 shows the overall architecture of the proposed auction system.

[Figure 2] Trusted Auction System



The purpose of the trust measuring fuzzy system is to quantify the trust level of a transacting entity involved and it is composed of the following sub-components.

- Fuzzification interface: It performs a fuzzification process for the input value. That is converting the input value into an appropriate verbal expression, which is one of the predefined fuzzy values for each input value.
- Rule Base: It defines fuzzy rules used for inferences to measure a trust level.
- Inference Logic: It performs actual trust measurement using fuzzy logic and rules defined in the rule base. That is calculating a trust level using fuzzy logic and fuzzy rules emulating human's decision-making process.
- Defuzzification Interface: It transforms fuzzy values calculated by the inference logic into a crisp value through a defuzzification process.

3.2.1. Trust measurement

In conventional auction systems, there is a possibility that one might manipulate the trust level of oneself by selling and buying one's own items many times because most of conventional auction systems use a point-keeping type of feedback system for trust measurement. In this situation, either the buyer or the seller cannot measure the exact trust level of the counterpart. Therefore, to prohibit intentional manipulation of the trust level, there should be a way to encourage auction trade entities to use their real names by providing better services to motivate real-name uses. However, since complete real-name-based systems are hard to be implemented systematically, there is a need to diversify trust variables used to measure trust level of transaction entities.

In addition to conventional trust variables such as previous trade history, there can be a number of possible trust variables we can adopt from a relationship-based internet community system. One of them is the number of degrees between the transacting entities involved in a specific auction trade. For instance, if the buyer and the seller have a second-degree relationship, it means that a person both the buyer and the seller knows has a first-degree relationship with each of them. Therefore, there will be lower possibility for them to experience any fraud in that trade compared to having it with a person that they do not have any relationship at all.

Another possible variable is the number of first-degree relationships that the person has. For example, if a person has first-degree relationships with 50 people in that community, it means that he or she has 50 people to verify his or her identity in that site. Therefore, we can conclude that the more people that person has first-degree relationships with, the higher the trust level he or she has.

The number of login times a day, which tells how loyal that person is to the site is another possible trust variable we can consider to use. For example, if there is a person who accesses the community site ten times a day could be considered to have a higher loyalty level than a person with average access frequency of once a week and, consequently, a higher trust level.

The relationships between those trust variables can be displayed in a matrix called Fuzzy Trust Surface (Manchala, 1998). Figure 3 (a) shows an example of a fuzzy matrix that shows the relationship between a trust variable named transaction history and one named transaction cost. The content of each cell shows the trust level involved in the trade based on the input value for each variable. In figure 3 (b), the relationship between number of degrees between transacting entities and the trade amount is shown. Those fuzzy matrices are defined by a human expert and fuzzy matrices defined in this way will be transformed into fuzzy rules to be used for fuzzy inferences in the fuzzy expert system to calculate the overall trust level of the trade.

[Figure 3] Fuzzy Trust Surface

Transaction History \ Transaction Cost	micro	small	medium	high	expensive
excellent	VH	VH	H	H	M
good	VH	H	H	M	L
normal	VH	H	M	M	L
bad	H	M	L	L	VL
worst	M	M	L	VL	VL

(a)

# of Degrees between Transacting Entities \ Trade Amount	extremely small	small	medium	Large	extremely large
extremely close	VH	VH	VH	H	M
close	VH	H	H	M	L
normal	VH	H	M	M	L
far	H	M	L	L	VL
extremely far	M	M	L	VL	VL

(b)

VH: Very High
H: High
M: Medium
L: Low
VL: Very Low

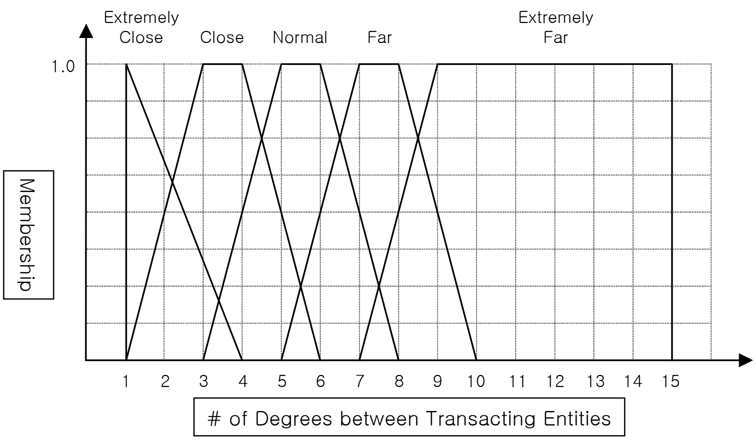
3.2.2. Fuzzification interface

To use variables explained in the previous section for measuring a trust level through fuzzy inferences, the input values for those trust variables should be transformed into fuzzy numbers, first. It is the fuzzification interface in the trust measuring fuzzy system that performs this transformation. In the rule base, a fuzzy membership function is predefined for each trust variable by human experts based on their previous experiences. There are many ways to define fuzzy membership functions including a triangular fuzzy number and a trapezoidal fuzzy number. In this paper, we use a trapezoidal fuzzy number function because more than one input value can have the maximum fuzzy number in this case.

Using a trapezoidal fuzzy number, the membership function for the number of degrees between transacting entities can be defined as follows and also figure 4 shows the graphical representation of the membership function.

- Extremely Close = [1, 1, 1, 4]
- Close = [1, 3, 4, 6]
- Normal = [3, 5, 6, 8]
- Far = [5, 7, 8, 10]
- Extremely Far = [7, 9, 15, 15]

[Figure 4] Fuzzy Membership Function



Using fuzzy membership functions defined for each trust variable, crisp input values are processed to have fuzzy number forms. First, input values go through a scale mapping process in which they match with a predefined input fuzzy value range to make it convenient to perform fuzzy operations such as fuzzy summation or fuzzy multiplication. Those transformed values are fuzzificated by calculating the degree of fulfillment. For example, if the input value for the number of degrees between transacting entities is 4, the membership value for “extremely close” will be ‘0’ and ‘1’ for “close.” In this sense, the degree of fulfillment is $DOF_{\# of \deg rees = 4} = \{0, 1, 0.5, 0, 0\}$.

3.2.3. *Inference logic*

The input values transformed into fuzzy numbers through fuzzification interface are used to calculate a trust level by inference logic. In the rule base, the fuzzy membership functions for all the input variables and the relationships among them are predefined. According to the relationships defined in the rule base, two input values are chosen for degree of fulfillment (DOF) calculation. The minimum value is assigned for the result matrix of DOF using the following formula.

$$w_i = A_{i1}(x_1{}^0) \wedge A_{i2}(x_2{}^0)$$
$$C^0(w) = [w_1 \wedge C_1(w)] \vee [w_2 \wedge C_2(w)] \vee \cdots \vee [w_n \wedge C_n(w)]$$
$$= \max[w_i \wedge C_i(w)] \qquad \textit{for } i = 1 \textit{ to } n$$

In the above formula, $X_1{}^0$ and $X_2{}^0$ represent input values and A_{i1} and A_{i2} represent their fuzzy membership functions respectively. Also, '$\wedge$' is the min operator (Mamdani, 1974), which returns smaller value among operands as a result. Therefore, using Max-Min operation (Zadeh, 1973), $C^0(w)$, the overall trust level, is determined by the maximum value among the calculated fuzzy outputs from various trust variables. For example, let's say that values of two input variables, number of degrees between transacting entities and trade amount, are 4 and 55000 respectively. DOF of two input variables are given as follows.

$$DOF_{\#\ of\ \deg rees = 4} = \{0, 1, 0.5, 0, 0\} \qquad DOF_{trade\ amount = 55000} = \{0, 0.25, 1, 0.25, 0\}$$

With the given DOFs of input values, the final DOF between two variables is like one in figure 5 (a). With this matrix, the fuzzy rule matrix for two variables, which is figure 3 (b), is composed into one result matrix using the formula given above. The composition matrix is shown in figure 5 (b).

[Figure 5] Degree of Fulfillment Matrix and Matrix Composition

# of Degrees between Transacting Entities \ Trade Amount	extremely small	small	medium	Large	extremely large
extremely close	0	0	0	0	0
close	0	0.25	1	0.25	0
normal	0	0.25	0.5	0.25	0
far	0	0	0	0	0
extremely far	0	0	0	0	0

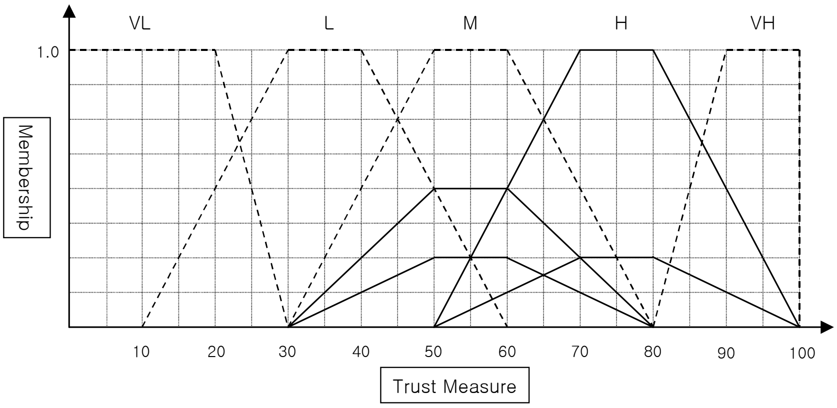
(a)

# of Degrees between Transacting Entities \ Trade Amount	extremely small	small	medium	Large	extremely large
extremely close					
close		0.25H	1H	0.25M	
normal		0.25H	0.5M	0.25M	
far					
extremely far					

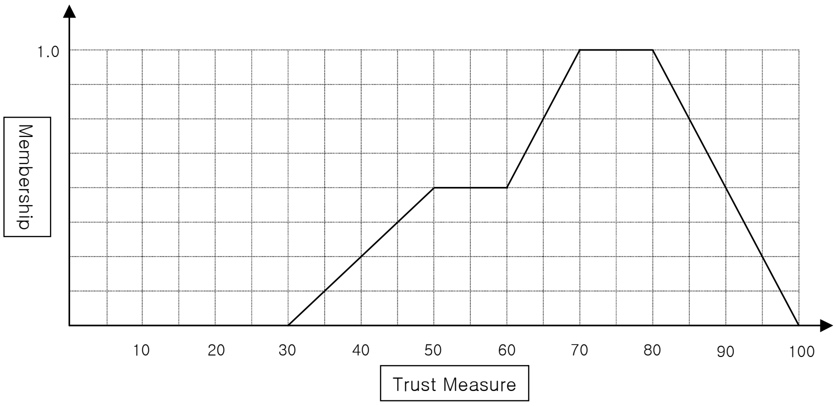
(b)

This composition result is represented graphically in figure 6. In that figure, the dotted line represents the membership function for the trust level of the output variable, while the composition result of 0.25M, 0.5M, 0.25H, 1H is shown with the solid line. Using the max-min formula to get the maximum value, the final result is drawn such as one shown in figure 7.

[Figure 6] Matrix Composition Through Fuzzification Interface



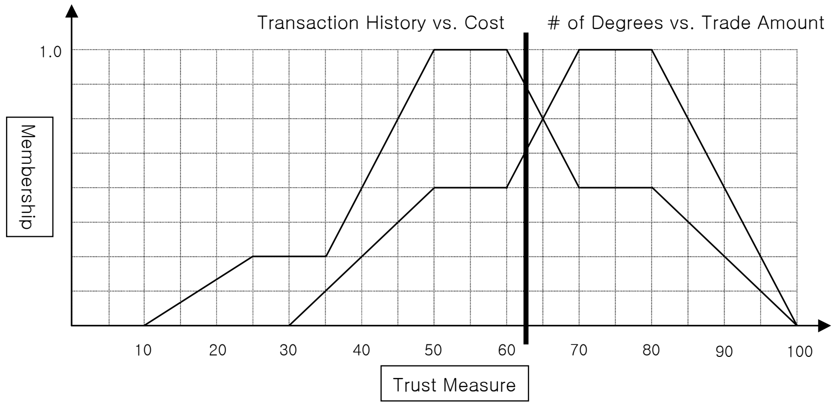
[Figure 7] Maximum Value Line Using Max-Min Formula



3.2.4. Defuzzification interface

Defuzzification interface of the trust measuring system converts the fuzzy output value calculated by inference logic into a crisp value. Since the inference logic produces as many output values as the number of relationships between trust variables defined in the rule base, it is needed to convert various fuzzy output values into one crisp trust value to determine the overall trust level of the trade concerned. The proposed system uses center of area method for this conversion calculation. As an illustration of this composition method, figure 8 shows the composition of output vales from a fuzzy number based on transaction history and cost and one based on the number of degrees between transaction entities and trade amount.

[Figure 8] Fuzzy Value Composition Through Defuzzification Interface



4. Safe Trade Protocols for a Trusted Auction System

4.1. Basic constructs

The sufficient condition for a successful trade can be defined as $\{give_{s \to b}(g), pay_{b \to s}(m)\}$ where 's' stands for seller, 'b' for buyer, 'g' for good, and 'm' for money respectively. The possible fraudulent actions associated with this trade procedure include buyer's refusal for payment and seller's refusal to send the agreed item. Also the repudiation from either the buyer or the seller about the other's action can be a problem.

To stop these fraudulent actions from happening, the credible intermediaries should guide the trade procedure for a secure trade process. For example, to manage monetary transfer between the buyer and the seller, an escrow service can be adopted while a door-to-door delivery service can be used for secure product delivery. Using these intermediary services causes additional costs and also slows down the trade process even though it can reduce the risk involved in the transaction and guarantee a secure trade. Therefore, unconditional use of intermediaries sometimes can mean an unnecessary expenditure. For trades between transacting entities with a high trust level, additional intermediaries services are not necessary and even causes inefficiency. Consequently, there is a need to differentiate trade protocols according to trust level associated with each trade.

4.2. Recommendation of appropriate trade protocols

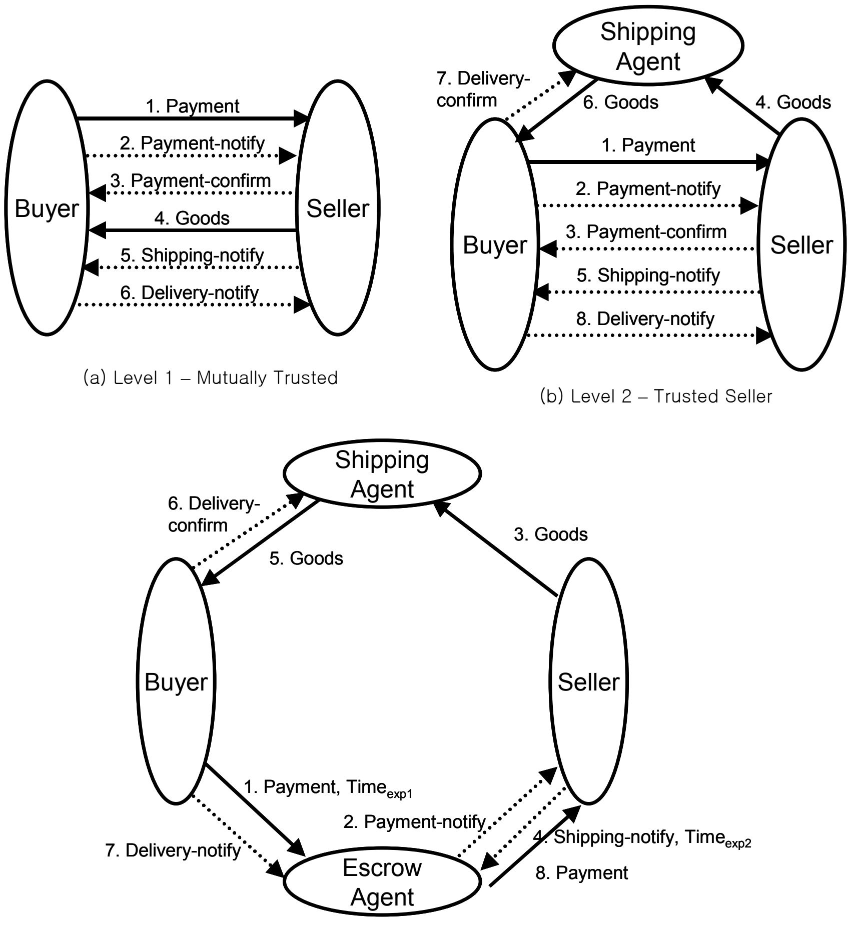
To simplify the discussion, let us consider that only two kinds of intermediary services, escrow and delivery, can be involved in an auction trade. Based on the fact whether or not to use escrow or delivery services, the trade protocols are categorized as three different levels as shown in the figure 9. Level 1 protocol is shown in figure 9 (a). This protocol does not use any of trade intermediaries. In this case, the related trade cost is low and the trade time is short compared to other protocols although the risk level associated with it is comparatively high. Therefore, it is appropriate to adopt this protocol only when the trust levels of both the buyer and the seller are high.

Level 2 protocol, shown in figure 9 (b), uses only a shipping agent for product delivery. Using this protocol, the seller sends the product via a shipping agent after getting the payment for the product. In this case, the buyer trusts in the seller due to his or her high trust level. The trade time involved would be the same as in protocol (a) but the transaction cost is increased for a delivery service.

In level 3, illustrated in (c) of figure 9, the buyer sends the payment to an escrow service agent and the seller checks if the payment is reached to the escrow agent before sending the item. Using a shipping agent, the seller sends the item and then the escrow agent sends the prepaid payment from the buyer after it checks the completion of the product delivery by the shipping agent. This is the protocol that can be used when both of the buyer's and seller's trust levels are comparatively low and consequently, they do not trust each other. Definitely, the transaction cost is the highest among three and it takes the longest time to finish the trade due to the additional process associated with it.

The characteristics of each trade protocol are summarized in table 1 and the Trusted Auction System proposed in this paper recommends a proper trade protocol based on the trust level calculated by the trust measuring fuzzy system.

[Figure 9] Secure Trade Protocols



(a) Level 1 – Mutually Trusted

(b) Level 2 – Trusted Seller

(c) Level 3 – Mutually Distrusted

[Table 1] Comparison of Trade Protocol

Trade Protocol	Seller's Trust	Buyer's Trust	Shipping Agent	Escrow Agent	Transaction Cost	Transaction Time	Security Level
Level 1	Very High High	Very High High	Not Use	Not Use	Low	Short	Low
Level 2	Very High High	Moderate Low Very Low	Use	Not Use	Moderate	Short	Moderate
Level 3	Moderate Low Very Low	Moderate Low Very Low	Use	Use	High	Long	High

5. Summary and Conclusions

In an internet auction trade, there are possibilities that various types of fraudulent actions, which might cause monetary losses to either the buyer or the seller, get involved. This is mainly because it is hard to authenticate the actual transacting entities due to the users' anonymity on the internet. Therefore, as an internet auction service provider, the auction site should have a way to protect transacting entities from any possible damages. For this purpose, a couple of methods such as user feedback, escrow services, etc. are devised and actually adopted by commercial internet auction systems. However, those approaches show limitations in evaluating the trust level of transacting entities and recommending differentiated trade protocols.

In this paper, a Trusted Auction System, which incorporates a fuzzy system to measure the trust level of each trade using fuzzy numbers and their composition, is proposed. The proposed system adopts various trust variables used to measure the trust level of involving transacting entities from a relationship-based internet community where users of the communities are encouraged to provide their correct personal information for network externality. The input values for those various trust variables are converted to fuzzy numbers by a trust measuring fuzzy system using fuzzy trust matrices defined in the rule base. The calculated fuzzy numbers from rules defined among various trust variables are composed into one overall trust level by the defuzzification interface. An appropriate trade protocol that both the buyer and the seller can follow to have a secure trade is recommended based on the calculated trust level of the trade concerned. The proposed system overcomes the shortcomings of a simple trust measuring mechanism using only previous transaction history, which most of conventional auction services adopt. However, the proposed system requires human experts to get involved to define trust matrices, which can be somewhat subjective and therefore show some differences depending on the experts who define them.

A prototype system was developed under Windows NT environment to test the appropriateness of the proposed system. Currently, we are trying to refine the fuzzy inference logic to enhance the fuzzy calculation process and the method to automate defining fuzzy rules for different pairs of trust variables.

References

Doney, P., and Cannon , J. "An Examination of the Nature of Trust in Buyer-Seller Relationships," *Journal of Marketing* (61), April 1997, pp. 35-51

Freier, A. O., Karlton, P., and Kocher, P. "The SSL Protocol, Version 3.0, Netscape Specification," Nov. 1996; available at http://www.netscape.com/eng/ssl3/ssl-toc.html

Hoffman, D., Novak, T., and Peralta, M. "Building Customer Trust Online," *Communications of the ACM* (42:4), April 1999, pp. 80-85

Kailar, R. "Accountability in Electronic Commerce Protocols," *IEEE Transactions of Software Engineering* (22:5), May 1996

Kent, S. "Internet Privacy Enhanced Mail," *Communications of the ACM* (36:8), August 1993, pp. 48-60

Ketchpel, S., and Garcia-Molina, H. "Making Trust Explicit in Distributed Commerce Transactions," *16th International Conference on Distributed Computing Systems (ICDCS '96)*, Hong Kong, May 1996

Lai, C., Medvinskey, G., and Newman, B. C. "Endorsing, Licensing and Insurance for Distributed System Services," *Proceedings of 2nd ACM Conference of Computer and Communication Security*, November 1994

Mamdani, H. "Application of Fuzzy Algorithms for Control of Simple Dynamic Plant," *IEEE Proceedings of Control & Science* (121:12), Dec 1974, pp. 1585-1588

Manchala, D. "Trust Metrics, Models and Protocols for Electronic Commerce Transactions," *18th International Conference on Distributed Computing Systems (ICDCS '98)*, Amsterdam, May 1998

Manchala, D. "E-Commerce Trust Metrics and Models," *IEEE Internet Computing*, March-April 2000, pp. 36-44

Maurer, U. "Modeling a Public-Key Infrastructure," *Proceedings of the 1996 European Symposium on Research in Computer Security (ESORICS '96)*, 1996

Mayer, R., Davis, J., and Schoorman, F. "An Integrative Model of Organizational Trust," *Academy of Management Review* (20:3), 1995, pp. 709-734

Rabin, M. "Transaction Protection by Beacons," *Journal of Computer and System Science* (27), 1983, pp. 256-257

Reiter, M.K., and Stubblebine, S.G. "Toward Acceptable Metrics of Authentication," *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE Computer Soc. Press, Los Alamitos, Calif., May 1997

Rivest, R. L. *The MD5 Message Digest Algorithm*, April 1992

Sandholm , T., and Lesser, V. "Equilibrium Analysis of the Possibilities of Unenforced Exchange in Multiagent Systems," *Proceedings of the 14th International Joint Conference of Artificial Intelligence (IJCAI-95)*, 1995

Stallings, W. *Protect Your Privacy, A Guide for PGP Users*, Prentice Hall, 1995

Su, J., and Manchala, D. "Building Trust for Distributed Commerce Transactions," *17th International Conference on Distributed Computing Systems (ICDCS '97)*, Baltimore, May 1997

Yahalom, R., and Klein, B. "Trust Relationships in Secure Systems – A Distributed Authentication Perspective," *Proceedings of the 4th ACM Conference on Computer and Communications Security*, April 1997

Zadeh, L. "Outline of a New Approach to the Analysis of Complex Systems ans Decision Processes," *IEEE Transactions on Systems Management and Cybernetics* (SMC-3:1), January 1973, pp. 28-44