

A Trust Scheme of Intelligence Networks - for Service Delivery

Yang Li, *Member, IEEE* and Anthony H. Chan, *Sr Member, IEEE*

Abstract—A communication session always happens between people and people are social members involved in different social groups. We thus bring in social networking to our intelligence networks to improve the network efficiency and to make better use of human resource. This paper especially addresses the trust relations of social people regarding to service delivery in communication networks. We define the trust system as four facets of service user's experience, neighbor's evaluation, service domain's certificate, and service user's self-recommendation. We further develop a way to individually calculate the trust fidelity on these four types of trust. We then testify the practicability of the trust system by applying it to the service delivery part of the intelligence networks.

Index Terms—Trust, service delivery, intelligence networks, social networks.

I. INTRODUCTION

THIS paper focuses on setting up a set of trust system in intelligence networks and calculating the trustworthiness of service involvers in the networks.

In the recent few years, trust has been attracting more and more researchers in computer and communication networks besides those in social networks. Most people majoring in Internet or e-commerce look at trust in order to avoid attacks due to the popularity of anonymity trust in computer world, whereas this research uses trust scheme to deliver the service with a better quality.

Research on Quality of Service (QoS) includes not only the researches on bandwidth, jitter, or error bit rate, but also those on the completeness of processing a service, such as how successful a service can be or how a service can meet the satisfaction of a user to the most.

We take up social networks and social networking in terms of relationships among individuals in a single service session, rather than relations among many communities, or relations with many communication events. We focus on the

trustworthiness of two service involvers – the service initiator and the service receiver, e.g., how the depth the service initiator trusts the service receiver will affect the quality of service delivery in intelligence networks.

This paper is organized as the followings. Section II prepares the social networks and the intelligence networks as the background of the trust system. Then we set up the concept of the trust system in section III and develop the calculation methods of the system in section IV. In section V, we apply the trust system to the intelligence networks.

II. TRUST IN SOCIAL NETWORKS

Because a communication session always happens between two or more socially related people, the study on social networks is extremely necessary for communication research.

A. Social Networks

“Social networking is built on the idea that there is a determinable structure to how people know each other, whether directly or indirectly.” [1]

Early in the 1930's, people begun to study social members' relations and describe these relations by using the members as dots and their relations as lines [2]. Meanwhile, some researchers began focusing on social groups, such as family, work, associations, and clubs, within social systems, for easier analysis [3]. In 1960s and 1970s, people further explored the mathematical basis of social structure. They drew algebraic models of social cliques and establish concepts such as the strength and distance of connections using theory and multidimensional scaling [3].

Social networks involve many angles, and trust between two users is one of the key aspects. The study on trust helps to disclose how people reply on each other and determine how they are able to treat each other in communication sessions.

Most current researches of the trust in social networks involve trust in a domain, such as trust in e-commerce [4] or trust on Internet [5]. Some other researches specially focus on the trust degree of service involvers in a single communication session.

B. Related Research

In general, we evaluate the trust of service involvers in a communication session by trust degree. This evaluation theory shows significance especially in the researches that emphasize on the service delivery and service management.

We have done research on applying human intelligence to future generation network [6]. In this type of intelligence networks, the trust system counts a lot regarding the successful delivery of a service as much as possible.

Manuscript received May 9, 2006. This work is supported in part by Telkom, Siemens, and National Research Foundation, South Africa under the Broadband Center of Excellence program in University of Cape Town.

Y. Li is currently a PhD student with the Department of Electrical Engineering, University of Cape Town, Rondebosch, 7701, Cape Town, SA (phone: 27-21-6502813; fax: 27-21- 6503465; e-mail: yli@crg.ee.uct.ac.za).

H. A. Chan is a professor of University of the Cape Town, Cape Town, SA (e-mail: achan@ebe.ee.uct.ac.za).

The intelligence networks are the next generation networks embedded with human intelligence. The intelligence networks should be able to carry on a service like what a real user normally does. Namely, the factor of human (e.g., the availability and capability of the expected receiver) will determine in what ways the service is delivered when the network is physically suitable for delivering a service (e.g., the user is with a proper terminal and the networks work well).

The networks may carry out six possible policies of service delivery according to the intelligence mechanism:

- 1) Successfully deliver the service to the receiver if all requirements are met - "Success";
- 2) Immediately deliver the service but with less satisfied performance after getting the permission of the service initiator - "Force";
- 3) Postpone the service and wait till the communication status of the receiver changes to be available - "Wait";
- 4) Find an assistant receiver to assist the originally expected receiver with the service - "Help";
- 5) The receiver learn on how to deal with this type of service from other experienced users - "Learn";
- 6) Fail the service - "Fail".

III. TRUST SYSTEM

Different from that in technical world where people concentrate on the uncertainty of a process or a member in pervasive areas, the trust in social network is prone to trust the related buddy, instead of doubt the buddy.

In a trust relation, we call the person who trusts others as *trustor* and the person whom is trusted by others as *trustee*. We then authorize the trustee to show how trustful he/she can be from his/her own side. The trustee may express his/her trustworthiness by showing the capability of processing the service, the availability for the service, and how much he/she recommend himself/herself to be involved in the service.

An individual's personal capability to handle a service is up to two factors. One is his/her experience of dealing the same type of service in the past (trust on time), and the other is the trust degree of how much his/her social neighbors trust him/her with this type of service (trust on neighbor). The domain the user is currently in determines the availability of the user to this specific type of service because a certain service only happens and is valid in a specific domain (trust on domain). The self-recommendation gives the trustee the chance to declare how much enthusiasm he/she has to perform the service (trust on self-recommendation). This factor is determined by the social relations of the trustee and trustor.

We further group the above four trust abilities into two categories: the service-loosely-coupled trust, including trust on time and trust on neighbor, and the service-tightly-coupled trust, including trust on domain and trust on self-recommendation. The first category of trust is stable because it represents the long-term trustworthiness of the trustee. The second category of trust changes with every service, and thus is instant and temporary.

We define the four angles of trust system in the following subsections and illustrate these four angles as a 4-D space model in Fig. 1:

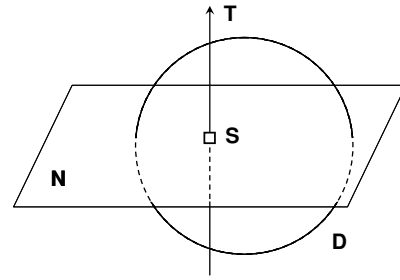


Fig. 1. Skeleton of Trust System in Communication Networks.

The Fig. 1 shows the four effective factors of trust at a service point. A service point is the expression of one person dealing with a specific type of service at a fixed time and with a fixed neighborhood.

In this visual structure of the trust system, the trust on time ("T") is expressed as a vertical arrowed line of time axis, the trust on neighbor ("N") is shown as a plane perpendicular to the time axis, the trust on domain ("D") illustrated in circle is parallel and intersects with the time axis, and the trust on self-recommendation ("S") sits on the time axis as a weighted square dot.

A. Trust on Time

Trust on time is defined as the weighted trust fidelity of the trustee in the most recent time periods.

We count trust on time by period instead of a single moment. The length of the period is up to how frequently this type of service is used in statistics, e.g., one day or one week.

The total number of time periods is set to be definite. In each time period, the trustee has a fixed value of trust fidelity.

Moreover, the closer a time period is to the user, the more this trust fidelity weighs, because the latest time periods more truly reflect the trustee's most recent capability of handling the service due to inertia.

The time on trust can be expressed as in Fig. 2:

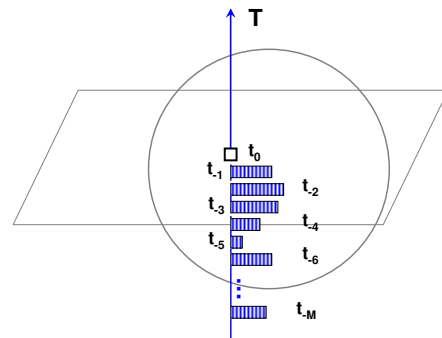


Fig. 2. Illustration of Trust on Time.

In the Fig. 2, the width of the vertical-line-marked bars on the time axis is the time length of the period and all the lengths are equal. The length of the rectangles is the trust fidelity of the trustee in that time period.

Referring to these bars on the time axis, Trust on time starts counting from time periods t_{-1} to t_{-M} . The system excludes the time periods that are earlier than t_{-M} in order to keep the system up to date.

B. Trust on Neighbor

Time on neighbor is defined as the weighted trust fidelity of the trustee with his/her socially related people - neighbors.

We count time on neighbor by the trust fidelity a cluster of neighbors around the trustee. A cluster contains the neighbors whose contact chances with the trustee are in a certain range.

Moreover, the closer the neighbors are to the trustee, the more they deserve to appraise the trust fidelity of the trustee.

Trust on neighbor can be illustrated as in Fig. 3:

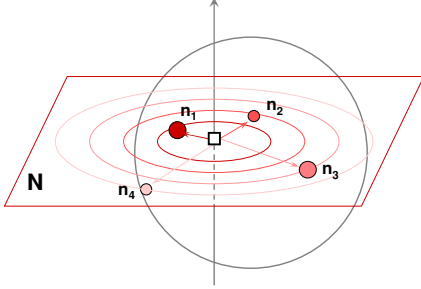


Fig. 3. Illustration of Trust on Neighbor.

In the plane “N” of the Fig. 3, the square dot at the center represents the trustee, the small circle dots represent the weighed evaluation of the neighbors on the trustee, and the chances that a cluster of neighbor contacts with the trustee are depicted as the circles with different radius using the trustee as the center.

The bigger the circle dots are, the more trust fidelity the neighbors think of the trustee. The closer the circle dots are to the center, the more contact times the neighbors have with the trustee, and the evaluation from this cluster of neighbors counts more.

C. Trust on Domain

Time on domain is defined as the availability of the trustee for the service in a specific domain. In other words, trust on domain is to test whether the service matches the domain where the trustee is currently in at the time being.

The availability of the trustee not only means that the trustee is physically available, such as with proper terminal, but also implies how much reputation the trustee has in the domain. The reputation in a domain is determined by the trustee’s social position (or social relations with other people in the domain) and affects the trust on self-recommendation.

Trust on domain can be expressed as in Fig. 4:

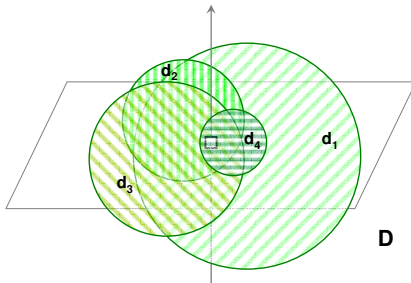


Fig. 4. Illustration of Trust on Domain.

We are able to see how trust fidelity functions in domains by contrasting the domain circles with the time axis in the Fig. 4, such as d_1 (upward-diagonal-marked circle) and d_4 (horizontal-line-marked circle). The domain circles intersect with the time axis and get a time length between the two intersecting points. The length of the time segment represents how much time the trustee is in the domain. The changed

domain projections on the time axis also reflect the trustee’s mobility in different domains.

The different types of marks for these domain circles represent the different trust fidelities of a service in different social domains within the time segment. The domains have different reputation effectiveness on a certain type of service at a certain time.

A type of service may involve with more than one domain. For example, a call to trustee’s cell can interact with trustee’s home, office, club, or public domains.

D. Trust on Self-recommendation

Trust on self-recommendation is defined as whether a user recommends him/her to conditionally accept the specific service. It is determined by the trustee’s willingness to receive the service and one’s social reputation in the domain.

Trust on self-recommendation is expressed as some discrete values, and can be illustrated as in Fig. 5:

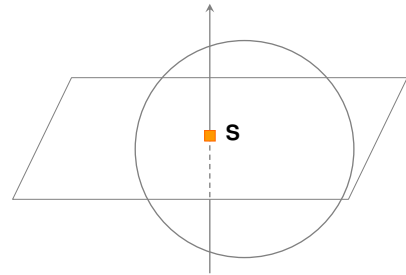


Fig. 5. Illustration of Trust on Self-recommendation.

In the Fig. 5, the trust fidelity of self-recommendation only concerns a NP problem, either “recommending” or “not recommending” himself/herself.

IV. CALCULATION OF TRUSTWORTHINESS

The same as previous work that bases trust degree on numbers [7][8], this paper uses real number intervals as well. The difference is that we add in the method of weighing the selected parameters of trust.

We express a person’s trust fidelity on a specific service as TR , $TR \in (0, 1)$. We exclude the values of “0” and “1” because they are untrue in the real world. It is impossible for a person does not have any trust fidelity at all for the specific service ($TR = 0$) and there is also no perfect service in the real world ($TR = 1$). When $0 < TR < 1$, the service can be delivered in some specific manner with the assistance of the network intelligence.

A. Trust Fidelity on Time

Trust on time is expressed as $TR_t(t-i)$, where i represents the i_{th} time period in the past counting from the current time point

Assume we count M time periods in the past and weigh each time period as $wt_i = \frac{2 \times (M + 1 - i)}{M \cdot (M + 1)}$, $i \in [1, M]$. From this expression we can see that the weighing value wt_i decreases when the time period is more passed, and also we

have $\sum_{i=1}^M wt_i = 1$ to limit the trust on time between 0 and 1.

Thus the trust fidelity on time or we say the trust on the trustee's experience can be written as:

$$TR_t = [wt_1 \quad \dots \quad wt_M] \times \begin{bmatrix} TR_t(t-1) \\ \dots \\ TR_t(t-M) \end{bmatrix} \quad (1)$$

where the t means time period. The TR can be expressed as the following formula:

$$TR_t(t) = \sum_{i=1}^M \left[\frac{2 \times (M+1-i)}{M \cdot (M+1)} \times TR(t-i) \right] \quad (2)$$

B. Trust Fidelity on Neighbor

Unlike the anonymity trust on Internet [9], the trust in social network is based on the assumption that all the service involvers know each other and have a certain amount of trust fidelity on each other.

Each neighbor node in the Fig. 3 does not stand for a single person, but a class of neighbors. The neighbors whose number of chances to contact the trustee is in a certain range are categorized into one cluster. For example, the neighbors who have more than 1000 times touches with the trustee, are categorized into the first cluster n_1 ; those with chances $\in [100,1000)$ are in the second cluster n_2 ; those with chances $\in [10,100)$ are in the third cluster n_3 ; those with chances $\in [1,10)$ are in the fourth cluster n_4 ; and those with no chance are omitted.

Trust on time is expressed as $TR_j(n_j)$, where j is the j_{th} neighbor cluster far from the trustee in social relation.

We assume the trustee has N clusters of neighbors, i.e., $j \in [1, N]$, and each class has trust fidelity on the trustee. Moreover, each class's trust fidelity on the trustee is weighed according to the familiarity of the cluster of neighbors and the trustee. The closer their relation is the higher weighing value the neighbors are able to give to the trustee, because a close relationship means that this cluster of neighbors knows the long-term behaviour of the trustee and thus the neighbors' appraisal of the trustee is worthy of more trust.

We choose the normal function with the independent value $n \in (0, \pi/2)$ as the weighing function. The reason of choosing a normal function instead of a decreased liner function is that the values of normal function can truly reflect the trustworthiness of the neighbors on the trustee. See Fig. 6:

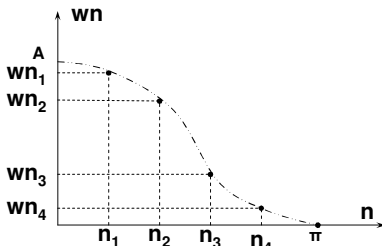


Fig. 6. Weighing function of trust on neighbor.

In the Fig. 6, we let the n_1 , n_2 , n_3 , and n_4 individually represent the 1000-time touch, the 100-time touch, the 10-time touch, and the 1-time touch with the trustee, and the wn_1 , wn_2 , wn_3 , and wn_4 are the weighing values that we

assign to the four neighbor clusters in sequence.

We first compare the weighing values of clusters n_1 and n_2 . Even though the chances of the cluster n_1 to interact with the trustee are ten times as that of the cluster n_2 , but, actually, after a 100-time touch, the neighbor has always known the long-term personality of the trustee very well. Thus there is no big difference between the wn_1 and wn_2 . However, there is a huge fall of the weighing values between the cluster n_2 and n_4 because neighbors in n_4 only contacts the trustee once, his/her trust on the trustee is partial and temporary. Therefore, it is essential to find out the quick-fall part of the weighing function (e.g. the part between the wn_2 and wn_3).

We formulate the weighing values of trust on neighbor as $wn_j = \frac{A}{j} \cdot \sin\left(\frac{\pi}{N+1} \cdot j\right)$. We assume the $(N+1)_{th}$ neighbor cluster does not have any trust fidelity on the person. We have

$$A = \left\{ \sum_{j=1}^N \left[\frac{1}{j} \cdot \sin\left(\frac{\pi}{N+1} \cdot j\right) \right] \right\}^{-1} \quad \text{so that} \quad \sum_{j=1}^N wn_j = 1,$$

Thus we write the trust fidelity on neighbor as:

$$TR_n = [wn_1 \quad \dots \quad wn_N] \times \begin{bmatrix} TR_n(n_1) \\ \dots \\ TR_n(n_N) \end{bmatrix} \quad (3)$$

$$TR_n(n) = \frac{2}{\pi} \cdot \sum_{j=1}^N \left[\frac{A}{j} \cdot \sin\left(\frac{\pi}{N+1} \cdot j\right) \times TR_n(n_j) \right] \quad (4)$$

C. Trust Fidelity on Domain

Trust on domain is up to both the availability and the public reputation of the trustee in the domain. It cannot determine the trust fidelity of the person, but will affect the level of it. Only the person's experience and appraisal from neighbors will affect the person's long-term trust fidelity.

Here we will explain at length the reputation of a person in a domain. Normally, the higher the person's long-term trust fidelity is, the less the domain fidelity is able to affect the person in a service deal. For example, if two presses write that William (Bill) Gates is going to bankrupt, his check may still be accepted by banks because people know that he will not fail easily due to his extremely high social reputation. However, if the two presses write that a normal person is going to bankrupt, the banks will mostly refuse to accept his/her check because of his/her low public reputation.

We express the trustee's availability to receive the service as $avai$ and his/her reputation in the domain as r . Thus the person's trust on domain, or how much the person's availability and reputation is going to affect the service process, can be expressed as:

$$TR_d = avai \cdot r^{(\alpha' \cdot TR_t + \beta' \cdot TR_n)} \quad (5)$$

where $\alpha' + \beta' = 1$ and $r \in (0, 1)$;

When the trustee is available in the domain for the service, $avai = 1$; otherwise $avai = 0$.

Here, the trustee's long-term trust fidelity $(\alpha' \cdot TR_t + \beta' \cdot TR_n) \in [0, 1]$ as well because $\alpha' + \beta' = 1$.

We assume r is a variable and $(\alpha' \cdot TR_t + \beta' \cdot TR_n)$ is a fixed

value. We can get two results from the formula (5):

(1) When the service is available for the trustee ($Avai = 1$), with the same reputation r , the higher the person's long-term trust fidelity is (the greater the $\alpha \cdot TR_t + \beta \cdot TR_n$ is), the less the reputation can affect the person's trust fidelity on domain (the lower the TR_d is), e.g., $0.2349 \cong 0.2^{0.9} < 0.2^{0.1} \cong 0.8513$.

(2) For the trustee with a fixed long-term trust fidelity ($\alpha \cdot TR_t + \beta \cdot TR_n \in [0, 1]$), the higher reputation he/she gets from the public (the greater the r is), the better temporary trust fidelity on domain he/she gets (the greater the TR_d is) because $r \in (0, 1)$, e.g., $0.3162 \cong 0.1^{0.5} < 0.9^{0.5} \cong 0.9487$.

The following problem is to solve the intersecting problem of several domains. Two factors need considering. The first is the choice of the proper domains and the second is to calculate the fidelity with the chosen domains. We name the virtual service domain as D , and the reputation of D is TR_d :

Subject: The operating service only relates to Domain 1 D_1 , expressed as $D = D_1$, and the reputation of the person in Domain 1 is TR_{d1} , then $TR_d = TR_{d1}$;

Subject: The operating service relate to Domain 1, 2, ..., P , expressed as $D = D_1 \cap D_2 \cap \dots \cap D_P$, and these domains are intersecting but exclusive, then $TR_d = \frac{TR_{d1} + TR_{d2} + \dots + TR_{dP}}{P}$;

Subject: The operating service relate to Domain 1, 2, ..., P , and all these domain include a subdomain Q , expressed as $D_Q \subset (D_1 \cap D_2 \cap \dots \cap D_P)$, then $TR_d = TR_{dQ}$.

D. Trust Fidelity on Self-recommendation

We assume that, at a service point, the trustee is able to recommend himself/herself to accept the service using a constant S and the trustee is able to change it whenever he/she would like to.

Trust fidelity on self-recommendation has two determinants. The first is surely the availability of the trustee because only when the trustee is available he/she is able to recommend him/her for the service. The second is the reputation of the trustee in domain. Only when the trustee has a very good reputation then he/she is able to recommend by himself/herself to get the service.

Thus we write the trust fidelity on self-recommendation as:

$$TR_s = \begin{cases} 0, & 0 \leq r < Cons \\ avai \cdot S, & Cons \leq r \text{ and } avai = 0 \text{ or } 1 \end{cases} \quad (6)$$

From the formula (6) we can see that only when the trustee's reputation is above a certain value and he/she is technically available, he/she is able to recommend him/her to continue process the service.

E. Trust Fidelity on All

From the above analysis, we describe the total trust fidelity in the following formula:

$$TR_{t,s,n,d} = \alpha \cdot TR_t + \beta \cdot TR_n + \gamma \cdot TR_d + \mu \cdot TR_s \quad (7)$$

where, $\alpha + \beta + \gamma + \mu = 1$;

Each of the four aspects affects the trustee's

trustworthiness from a specific angle.

V. EFFECT OF TRUSTWORTHINESS ON INTELLIGENCE

We apply human intelligence to the current networks so that the intelligence networks are able to mimic human's abilities to deal with communication services and thus relieve human from heavy communication life.

The intelligence networks have six ways of delivering a service to the receiver. All the six ways are concerned with social networking technologies in order to manage human's communications more effectively.

To choose the most suitable way of delivering a service is up to the trustworthiness value of the receiver for the initiator. We explain how this trustworthiness affects the choice of service delivery in TABLE I:

TABLE I
EFFECT OF INITIATOR'S TRUST ON RECEIVER

Long-term trust				
Trust on Time	Trust on Neighbor	Trust on Domain	Trust on Self-recommendation	Results
	YES	YES	NULL	<i>Success</i>
	NO	YES	YES	<i>Force</i>
	YES	NO	NO	<i>Wait</i>
	NO	YES	NO	<i>Help</i>
	NO	YES	YES	<i>Learn</i>
	NO	NO	NO	<i>Drop</i>

The long-term trust includes trust on time and trust on neighbor. It stands for the trustee's true personal trust fidelity. The trust on domain relates to the service real time, thus it more presents the trustee's availability and reputation for the service in the related domain. Trust on self-recommendation works only when the trustee's trust fidelity on domain reaches a certain value. The results show what the best decision the intelligent network may make.

Here are the explanations for each row of data in the table:

1) *Row 1:* If the service initiator trusts that the receiver is fully capable of and available for the service (long-term trust "YES" and trust on domain "YES"), the initiator will deliver the service immediately (result "Success") no matter whether the receiver recommends himself/herself or not (trust on self-recommendation "NULL").

2) *Row 2:* If the service initiator does not trust the receiver's capability to implement the service (long-term trust "NO"), but the receiver is available both physically and socially (trust on domain "YES"), and he/she recommends himself/herself to handle the service (trust on self-recommendation "YES"), the intelligence mechanism will force the network to deliver the service with less satisfied service quality (result "Force").

3) *Row 3:* If the service initiator trusts the receiver is capable of the service (long-term trust "YES"), whereas the receiver is not available at the time being (trust on domain "NO") and does not recommend himself/herself for the service (trust on self-recommendation "NO"), the initiator will indicate to postpone the service for a period of time till the trustee changes to be available (result "Wait").

4) *Row 4:* If the service initiator finds that the service receiver is not able to handle the service (long-term trust "NO") but is available (trust on domain "YES"), and the receiver also does not recommend himself/herself for the service (trust on self-recommendation "YES"), the intelligent network will indicate the receiver to ask for help from

somebody else in the network (result “Help”).

5) *Row 5*: If the service initiator finds that the service receiver is not able to handle the service (long-term trust “NO”) but is available (trust on domain “YES”) and recommends to process the service, the initiator will suggest the receiver to learn from somebody in the network on how to deal with the service (result “Learn”).

6) *Row 6*: If the service initiator knows that the service receiver is incapable of, not available for, and not interested in handling the service (long-term trust “NO”, trust on domain “NO”, and trust on self-recommendation “NO”), it will drop the service immediately (result “Drop”).

It is seen from the Row 3 and Row 6 of the TABLE I that if a user is low in trust fidelity on domain (trust on domain “NO”), he/she has not right to recommend himself/herself to get the service (trust on self-recommendation “NO”).

VI. CONCLUSIONS AND FUTURE WORK

“The Webster dictionary defines trust as 1) an assumed reliance on some person or thing; a confident dependence on the character, ability, strength, or truth of someone or something; 2) a charge or duty imposed in faith or confidence or as a condition of a relationship; or 3) to place confidence (in an entity).” [10] Correspondingly, we define our trust system in communication networks as trust on time (character of someone), trust on neighbor (charge of duty of a relationship), trust on domain (confidence in an entity), and trust on self-recommendation. Altogether, the trust system is able to reflect the full meaning of the general trust.

The previous work on trust most focus on the uncertainty on Internet, peer-to-peer, or some pervasive networks. Yet this paper emphasizes the structure and calculation of trust system in social networks. What’s more, we apply this trust scheme on the service delivery of intelligence networks to see how it affects the design of communication networks.

We may have two methods to testify trust among people: interviewing real people after they use the trust system or collecting statistic data from simulation tools.

In the future, we need to do the following things in order to build up a full trust system:

- 1) Fix and optimize the following constant parameters by doing interviews with people or collecting simulation data: M , N , A , α' , β' , S , $Cons$, α , β , λ , and μ .
- 2) Implement the trust system in the intelligence networks. By testing and comparing the network utility and human resource efficiency of the intelligence networks, we will be able to indirectly test how a trust mechanism affects the true communication life.

REFERENCES

- [1] Elizabeth F. Churchill and Christine A. Halverson, “Social Networks and Social Networking,” *IEEE Internet Computing*, vol. 9, no. 5, 2005, pp. 14-19.
- [2] J. Scott, *Social Network Analysis: A Handbook*, 2nd ed., Sage Publications, 1991.
- [3] M. Granovetter, “The Strength of Weak Ties,” *Am. J. Sociology*, vol. 78, no. 6, May 1973, pp. 1360–1380.
- [4] Y. H. Tan and W. Thoen, “Formal aspects of a generic model of trust for electronic commerce,” in *Proceedings of the 33rd Hawaii International Conference on System Sciences*, 2000.
- [5] B. Wellman and M. Gulia, “Virtual Communities as Communities: Net Surfers Don't Ride Alone,” *Networks in the Global Village: Life in Contemporary Communities*, B. Wellman, ed., Westview, 1999, pp. 331–366.
- [6] Yang Li and H. Anthony Chan, “A Mechanism of Applying Intelligence to the Network by Considering Users’ Social Relations,” in *Proceedings of the 13th International Conference on Telecommunications (ICT2006)*, Funchal, Madeira, Portugal, May 9-12, 2006.
- [7] T. Beth, M. Borcharding, and B. Klein. *Valuation of trust in open networks (ESORICS 94)*, Brighton, UK, Nov. 1994.
- [8] J. Carter and A. A. Ghorbani, “Towards a formalization of trust,” *Technical Report TR03-158*, Faculty of Computer Science, Univ. of New Brunswick, Fredericton, NB, E3B 5A3, Canada.
- [9] A. Singh and L. Liu, “TurstMe: Anonymous management of trust relationships in decentralized P2P systems,” in *Proc. Of the Third International Conference on Peer-to-Peer Computing (P2P'03)*, Sep. 2003 pp. 142-149.
- [10] M. H. Zhou, W. P. Jiao, and H. Mei, “Customizable framework for managing trusted components deployed on middleware,” in *Proc. 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS)*, Jun. 2005, pp. 283-291.

Yang Li (M'06) received her B.En. from Beijing Univ. of Posts and Telecommunications, R.R.China in 2001, and her M.Sc. from the University of the Western Cape, R.SA in 2005, and is currently studying for a Ph.D. in the Dept. of Electrical Engineering, University of Cape Town, R.SA.

From 2001 to 2002, she was an assistant Engineer in the Technical Division of former SCNB, where her work focused on upgrading the intelligence part of the EWSD switch.

H. Anthony Chan (M'94–SM'95) received his PhD in physics at University of Maryland, College Park in 1982 and then continued post-doctorate research there in basic science.

After joining the former AT&T Bell Labs in 1986, his work moved to industry-oriented research in areas of interconnection, electronic packaging, reliability, and assembly in manufacturing, and then moved again to network management, network architecture and standards for both wireless and wireline networks. He designed the Wireless section of the year 2000 state-of-the-art Network Operation Center in AT&T. He was the AT&T delegate in several standards work groups under 3rd generation partnership program (3GPP). During 2001-2003, he was visiting Endowed Pinson Chair Professor in Networking at San Jose State University. In 2004, he joined University of Cape Town as professor in the Department of Electrical Engineering.

Prof. Chan is Administrative Vice President of the IEEE CPMT Society and has chaired or served numerous technical committees and conferences. He is a distinguished speaker of the IEEE CPMT Society and has been in the speaker list of the IEEE Reliability Society since 1997.