http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (23): 7435-7441, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.7435.7441

A Rank-based Application-driven Resilient Reputation Framework Model for Social Networks

Haiguang Chen, Yi Li and Xinfeng Huang
Department of Computer Science, Shanghai Normal University, Shanghai, 200234, China

Abstract: The security of Social Networks is an important field of research about SNs and has attracted a lot of attentions nowadays. Up to now, many security protocols have been proposed but most of them focus on the authentication. Although, these methods have addressed many conventional problems in the Social Networks but many novel malicious actors encountered in SNs could not be solved by authentication. Reputation based trust systems represent soft security mechanisms that complement traditional information security. Nowadays, the research of security mechanism based on reputation and trust has become a hot research issue in social networks. In this study, we propose a new security protocol RARRM to construct trustworthy social networks. This protocol not only can distinguish different applications but also can rank trust values. The objective of this protocol is not only to encourage actors to provide good services consecutively to establish a security environment of network but also to punish strictly those malicious actors that are trying to take advantage of reputation system to launch malicious attacks. Through intensive simulation, we will verify the correctness and efficiency of the proposed defense techniques.

Key words: Security, reputation, social network, application-driven, trust rank, confidence degree, dynamic punishing factor

INTRODUCTION

Trust is an important aspect of the relationship between two entities or actors. The trust landscape of a social network (who trusts whom and who can be trust) plays an important role in the intelligence and security domain. Trust forms a basis for formation of collaborative work; it can serve to identify influential actors in a network; and it determines how information will flow in a social network.

A typical social network consists of some actors (individuals) or organizations and some form of interactions between them which could be borrow and return, phone calls, emails, blog posts, etc. As a result, the interactions between individuals in the social network is a good indicator of their social relationships with these individuals. An aspect of trust is based on the notion of embeddedness (Zukin and DiMaggio, 1990) which shows that the interactions between individuals form a basis from which a trust relationship may grow. Sometimes these interactions may not require trust. However, they establish a relationship that can be used to build trust. The various characteristics of these relationships, such as persistence of communications and the balance in participation, may signal the existence or formation of a trusting relationship.

Social sensor networks (SNs) hold the most important applications, for example, collaborative work and mutual trust (Wasserman and Faust, 1994; Easley and Kleinberg, 2010). SNs consist of a set of social actors and a set of the dyadic ties between these actors. The relationship of SNs is very vulnerable to various malicious actors and an adversary can control some actors undetectably and then launch malicious actors toward other actors in SNs. But in some critical applications scenarios network security is integral to wide-scale acceptance of the network applications (or organizations), especially if the organizations protects the important infrastructures or do some important task.

There has been considerable interest in the topic of trust establishment for social networks and is attracting more and more attention. Trust establishment is an important and challenging issue in the security of social networks. As a viable solution for evaluating the trustworthiness of actors in SNs, The basic principle of trust system is to provide a mechanism for rating the actors behaviors and then to collect any reputation information about target actors for computing the trust values of the target actors. The reputation-based trust system can achieve two benefits: First, to stimulate the actors to provide good quality of services, second, to restrain malicious behaviors that would blemish the profits of sincere actors.

Corresponding Author: Haiguang Chen, Department of Computer Science, Shanghai Normal University, 200234, ShangHai, China

In this study, we propose a rank-based application-driven resilient reputation framework model for social networks. The actors have different trust ratings for different demands. Our model use watchdog scheme to observe the behavior in different interaction of these actors and broadcast their trust ratings in an organizations. The main contributions in our study are listed as follows:

- Offer a distributed rank-based application-driven resilient reputation framework model (RARRM) to detect malicious actors in different interaction
- Develop a confidence degree based trust rating mechanism for establishing reputation between actors to choose reliable actors and deal with the malicious actors in different application scenario
- Propose a new direction in trust system for social network

The remainder of the study is organized as follows: Section II briefly describes the related works about security in trust system for WSNs and SNs. Section III describes the rank-based application-driven resilient reputation framework model for SNs. In section IV, the implementation of the proposed trust framework model is described and simulation results are shown. The conclusion is drawn in section V.

RELATED WORKS

There has been work done on trust in computer science as well as in social science, Beth *et al.* (1994) present a method for valuation of trustworthiness in open networks (Beth *et al.*, 1994) and such as making selections of trusted route, detecting misbehaving nodes in ad hoc networks or wireless sensor networks (Li *et al.*, 2004) Evaluation of trustworthiness of participating entities is an effective method to stimulate collaboration and improve network security in distributed networks. Similar to other security related protocols, trust evaluation is an attractive target for adversaries and may be vulnerable to attacks, five attacks against trust establishment methods are identified and defense techniques are developed (Sun *et al.*, 2008).

RFSN (Ganeriwal and Srivastava, 2004) is the first reputation and trust-based model designed and developed exclusively for sensor networks it use watchdog mechanism residing in the middleware of each node to collects observable information and build trust rating. Second hand information gathered from nodes in the neighborhood is also included in the statistical computation of reputation. Direct observation and second hand information together facilitate a decentralized reputation based system. This reputation system facilitates punishment of non-cooperating nodes by denying them access to network resources. But the watchdog cannot record all the behavior due to its own fault, so there is uncertainty in the trust system, In (Buskens, 2002) Buskens discusses proposes explanations for the emergence of trust in social networks when actors can label others as untrustworthy and when actors are informed regularly about trustworthy behavior of others. Abdul-Rehman and Hailes (2000) and Aberer and Despotovic (2001) study reputation based trust and trust management. Abdul-Rahman and Hailes present a model in which agent's tune their measures of trust based on observed reputations and Aberer and Despotovic discuss a trust model that is grounded in real-world social trust characteristics and based on a reputation mechanism, or word-of-mouth. Their proposed model in SNs allows agents to decide which other agents' opinions they trust the most and allows agents to progressively tune their understanding of another agents subjective recommendations

In (Kuter and Golbeck, 2007) Kuter and Golbeck describe a different approach for estimating trust in various computing systems. They give an explicit probabilistic interpretation for confidence in social networks. They describe a new trust inference algorithm that uses a probabilistic sampling technique to quantify confidence and trust. They compute an estimate of trust based on only those information sources with high confidence estimates.

Those methods proposed in SNs above use semantic information in some way and/or focus on a static snapshot of a social network which does not capture all of application behavior and dynamics. Conversely, we study the problem of behavioral trust purely from the observed application-driven statistics, using no semantic information. We give measures of behavioral trust which apply to rapidly changing dynamic, Rank-based application-driven networks; We propose a rank based and application-driven protocol to detect the malicious actors in different application-related scenarios. The objective of the proposed scheme is to build trustworthy and security Social Networks.

RANK-BASED APPLICATION-DRIVEN RESILIENT REPUTATION MODEL

These reputation models mentioned in above don't give different trust values for different requirements of application separately and to compare corresponding trust values. All interactions between actors are

considered into the calculation of identical trust value indifferently and then give a mixed trust value for each actors according to the performance in various application requirements. when need to choose a actors to cooperate, don't consider the type of certain application, confidence degree for estimated trust value and the rank of corresponding trust value, these methods will leave malicious actors the opportunities to damage benefits of good actors to gain unwarrantable profits by taking bad behaviors. In this section, we introduce the proposed reputation model: Rank-based Application-driven Resilient Reputation Model (RARRM). Unlike other reputation models, we proposed novel reputation framework model is going to value for different requirements of application respectively, rank trust values belonging to identical kind of application by taking confidence degree into account and then to choose one neighbor actors to provide relative application service. As a result, each actors has several different trust rating values related with different applications in their neighbors. In our proposed RARRM reputation system, we introduce a distributed idea of local-centralization which run watchdog security mechanism just at the middleware of agent, each agent observe those interactions of actors in the agent's Agents calculate trust values regularly and broadcast these trust values. Using agent to collect reputation information can guarantee the accuracy of information about other actor, more importantly it can remove the bad mouthing attack and conflicting attacks. These receiving actors will rank these received calculated trust values and form candidate tables according to the type of application. When one actor needs to choose a neighbor actor for a certain application requirement, a actor in the candidate table related with this application will be selected to do responding task. In addition to the new security mechanism depicted above, we adopt a counter of consecutive malicious behaviors to find the malicious attack quickly. We describe the reputation model in detail in the following subsections.

System architecture: We proposed reputation calculation algorithm that is based on the Bayesian statistical theorem, the Beta distribution is also used as a calculating tool of trust value, The rating value is estimated as:

$$\frac{\alpha+1}{\alpha+\beta+2}$$

where, α is the number of good behaviors (or excepted behaviors) and β is the number of bad behaviors. This calculation is based on the beta function model introduced in (Ganeriwal and Srivastava, 2004). But our scheme introduces the confidence degree for estimated trust value and rank of trust value of different application scenario into the reputation system, for each application, each direct neighbor of the target actor will maintain a corresponding trust value. Consequently, each neighbor actor has to maintain and update several different trust values for identical target actor. When one actor is going to choose one neighbor to complete a certain kind of task, the actor will choose a neighbor with the higher confidence degree and trust value related with this kind of task. Upon finding the malicious attack, for example, the counter of malicious behavior, denoted as MC, surpasses the predefined threshold, denoted by MC_t, during the interactions between actors, the interaction will be stopped immediately. At the same time, remove the target actor from the corresponding candidate table and choose randomly another actor in the identical candidate table to cooperate. The target actor will be punished strictly in order to reduce the probability of being selected in the next transaction to take advantage of trust system and give other good actors more chances to be selected in the next transaction. The goal of RARRM is to choose the relatively reliable neighbor to maximize the probability of success. In order to encourage actors to provide good services all the time, if a actor provides good services continuously, his reputation value should be higher than that of whom just provides good services brokenly, otherwise, if a actor performs some adverse behaviors it should be punished immediately by reducing its trust value rapidly.

Modeling reputation and confidence: In SNs, an actor has several different events or ability or property such as assistant, data collection, borrow money, assist staff etc, to implement various functions of applications. In my opinion, a good computational trust model should provide a metric for comparing trustworthiness of different actors, these trust values involved in this comparison should be related with the same context of application. Otherwise it makes no sense. Based on this idea, we divide the works of actors into a set: $A = \{a_1, a_2,...,a_n\}$. Each actor n_i is of a subset $Ai = \{a_{i1}, a_{i2},...,a_{ir}\}$, our trust model is to estimate different trust values of actor about different $\alpha_{ir}(\alpha_{ir} \epsilon A_i)$. For different neighbors who require the target actor to do a same task, the target actor may provide service with different level of quality, similarly, an actor would have different performance when being asked to provide different services by identical actor, some is good performance and some is bad performance. We call them positive output and negative output. For simplicity of analysis, we only take a type of application α_i to explain our proposed trust rating model in the following sections,

the other is similar. Let n_i and n_j be two actors in SNs and let the interaction results between actors be described by binomial events, the times of successful cooperation and failure cooperation are represented α and β, respectively. Then, the posterior distribution of successful cooperation between n_i and n_j is a Beta distribution with the density function:

$$\text{Beta}(x \mid \alpha, \beta) = \frac{x^{\alpha}(1-x)^{\beta}}{\int_0^1 u^{\alpha}(1-u)^{\beta}\,du} \quad (1)$$

and actor n_i'rating value about trust value of actor n_j is the expected value of beta distribution:

$$E[x \mid \alpha, \beta] = \frac{\alpha+1}{\alpha+\beta+2} \quad (2)$$

where, $0<x<1$ and $\alpha, \beta>0$.

In our proposed trust model, reputation information is consisted of two parts: Direct Reputation and Indirect Reputation.

Definition 1: The Direct Reputation represents the direct experience of interactions of actor i on actor j. We use t_{ij} to denote Direct Reputation in this study. The times of success interaction and the failure interaction are represented by α_{ij}, β_{ij}, respectively. In addition, we introduce the concept of transaction.

Definition 2: The transaction is a set of interactions between actors about a certain application service requirement during one time window, for example, a task of sending 10 data packets can be considered as one transaction in our scheme. For the kth transaction, we define the transaction rating as follow:

$$t_{ij}^{k} = \frac{\alpha_{ij}^{k}}{\alpha_{ij}^{k} + \beta_{ij}^{k}} \quad (3)$$

where, t_{ij}^{k} denotes the kth transaction rating, $\alpha_{ij}^{k}, \beta_{ij}^{k}$ is the times of success interaction and the failure interaction during the kth transaction. In our scheme, we predetermined a threshold t_θ that is used to decide whether the target actor do malicious attack. If $t_{ij}^{k} > t_\theta$, the performance of the transaction is good in some extent, otherwise, the target actor is considered to launch malicious attack. Then the Direct Reputation is updated based on the rating of the last transaction as follows:

$$\begin{cases} \alpha_{ij} = b_{ij} + (1-b)\alpha_{ij}^{k} & t_{ij}^{k} < \theta \\ \beta_{ij} = \beta_{ij} + \beta_{ij}^{k} \end{cases} \quad (4)$$

$$\begin{cases} \alpha_{ij} = pf\alpha_{ij} + \alpha_{ij}^{k} & t_{ij}^{k} > \theta \\ \beta_{ij} = \beta_{ij} + \beta_{ij}^{k} \end{cases} \quad (5)$$

$$t_{ij} = \frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \quad (6)$$

where, b is a predefined aging factor. Pf is a punishing factor.

In our proposed scheme, pf is not a fixed value it varies dynamically with different scenarios it is determined by some factors such as type of application, frequency of malicious attack and rating value of failure transaction. Adopting different punishing factor can protect sincere actors from being punished strictly due to poor services that are caused by some other factors temporally, such as poor communication environment etc.. In subsection A, we defined an indicator of malicious attack. We also deal with trust value with the same equation (6) as depicted above when$MC>MC_t$.

On its own, t_{ij} does not differentiate between cases in which n_i has adequate information about n_j and cases in which it does not. Intuitively, more direct experience would lead to a more accurate estimate of t_{iji}. We need to measure the confidence degree in t_{ij}, for which we define a confidence metric C_{ij}. We use interval estimation to evaluate the confidence degree. Let $(t_{ij}-\varepsilon, t_{ij}+\varepsilon)$ be the confidence interval with degree of c_{ij}, t_{ij} where ε is the error level it influences the C_{ij}. Confidence degree of C_{ij} can be modeled as equation 7:

$$c_{ij} = \frac{\int_{t_{ij}-\varepsilon}^{t_{ij}+\varepsilon} x^{\alpha}(1-x)^{\beta}\,dx}{\int_0^1 u^{\alpha}(1-u)^{\beta}\,du} \quad (7)$$

Definition 3: The Indirect Reputation is obtained from the direct experience of other neighbor actors of target actor n_j during a past period of time. In this study, we use ti_{ijj} to denote the Indirect Reputation. In our reputation model, the Indirect Reputation is calculated as follow:

$$ti_{ij} = \sum_{k=1}^{n} w_{kj} t_{kj}, w_{kj} = \frac{c_{kj}}{\sum_{v=1}^{n} c_{vj}}, v \neq i, k \neq i \quad (8)$$

where, n is the number of neighbors of n_j, C_{kj} is the confidence degree of t_{kj}.

Modeling trust and ranking trust: The final trust value, T_{ij}, is the combination of Direct Reputation, Indirect Reputation and confidence degree. This is a confidence-based selective strategy of calculation. In certain circumstances it may be appropriate for a actor to use Indirect Reputation because a actor may not have

interacted with other actors before or may have few interactions with the target actors which is not enough for us to perform trust evaluation. Using Indirect Reputation can help a actor to boost the trust value about target actor. In particular, if the actor has a low confidence level in its assessment, based only on its own experience. However, using Indirect Reputation would introduce risk that malicious would get higher trust value even though malicious actor have done malicious attack and be punished strictly, therefore, we should consider selectively Indirect Reputation in calculation of T_{ij}. In our scheme if has significant first-hand experience with the target actor, then we give the Direct Reputation larger weight in the calculation, if one actor is of some failure records, we should reduce the proportion of Indirect Reputation. T_{ij} is calculated as follow:

$$T_{ij} = c_{ij}t_{ij} + p(1 - c_{ij})ti \quad (9)$$

where, p is a dynamic adjusting factor, the intention of this factor is to reduce the probability for malicious to gain high trust value and selected into candidate table, for the simplicity of analyses, we set p = pf.

In our scheme, we need to rank trust values of actor, T_{ij} is considered as ranking item in ranking table in relation to a type of application task so that malicious actor will be of less chance to be chosen to fulfill required task even if it is given a high trust value by equation (6). After receiving trust values broadcasted by agents regularly, each actor will rank these trust values and form ranking table R_i.

$$R_i = \{n_{i1}, n_{i2}, \ldots, n_{ir} \mid T_{ii1} \le T_{ii2} \le \ldots\ldots \le T_{iir}\} \quad (10)$$

When an actor n_i needs to choose an neighbor actor n_j to accomplish some tasks it will refer to the corresponding trust ranking table and will define a subset, SR_i, of R_i , each actor in SR_i is a candidate which would be chosen to provide service for actor SR_i in the next transaction, our proposed scheme will choose one of them. This method is of two advantages: One is that it will reduce probability of selecting one malicious actor even though the malicious actor is n_{i1}, another advantage is that each actor of SR_i have the same chance being selected so that can avoid to rely on the actor which is in the first place ,extensively and save energy of the actor to extend life time. When the selected actor is suspected to be a malicious actor, n_i stops immediately cooperating with it and then choose randomly another candidate in SR_i to continue to accomplish the remaining task, at the same time, remove the suspicious actor from Sr_i.

$$SR_i = \{n_{i1}, n_{i2}, \ldots, n_{iv} \mid v < r\} \; SR_i \subset R_i \quad (11)$$

SIMULATIONS

We implement a simulation framework to emulate a SNs, our simulator is composed of the following modules: A small social networks, different application, the actors, the agent actors, intruder actors, events generator. The intruder actor' behavior varies from time to time or varies with different application requirements. The intruder actors except take on-off attack and take the following attack: The intruder cooperates with the actor n_i, when the intruder is asked to provide service in relation to application α_i its performance well, when the intruder is asked to provide service in relation to application a_j its performance bad.

Simulation setup: We have discussed the proposed trust framework model above. We consider a network scenario where the actors and agent actors are organized randomly to do a certain task.

- **Case a:** We consider actor A and M, shown in Fig. 1a. The actor M is a malicious actor. The actor M provides several services for the actor A, such as information collection, message forward and report location. The actor M does well in information collection and report location but does badly in message forward. In order to show the feature of application-driven in our trust model

- **Case b:** Actors A, B, C, D, M are the neighbors of actor E, actor the actor A, B, C, D are also the neighbors of M , here, M is a malicious actor. In the begin of several window times, the actor M performs well for these actor A, B, C, D, E in every requirement of service but it does badly to the actor E in the following time windows. And we suppose that the actor M just provide one service of application. And the service is delivering packet for them

In our trust system, our proposed agent actor use time window function to monitor the behavior of its

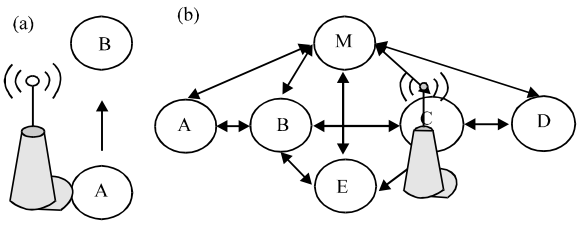

Fig. 1: Simulation setup

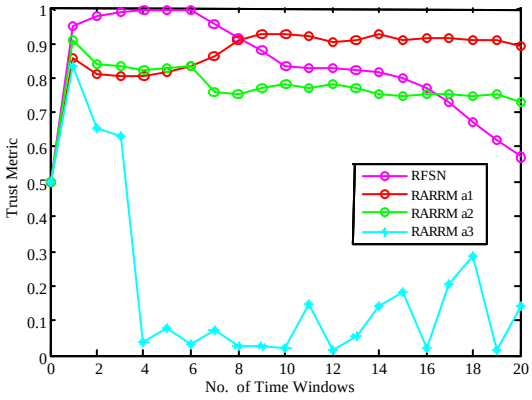

Fig. 2: RFSN VS RARRm

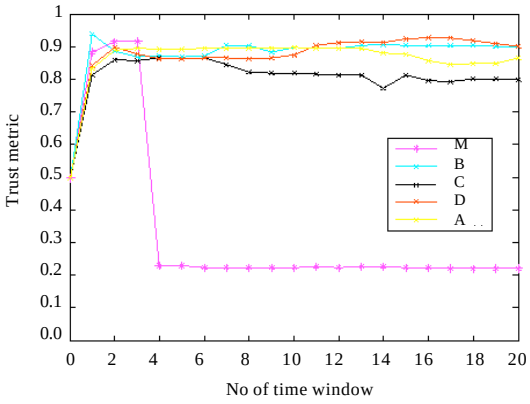

Fig. 3: Different trust rating

neighbor actor. The length of time window is different in different application environment, for those important applications, the window should take shorter length of time than those of less important applications. For simplicity of analysis, we set same length of time window for different application services. The agent actor broadcasts the trust rating at each end of window time. If the agent fined the malicious attack during interactions by MC, agent will broadcast an alert, the malicious actor will be removed from the corresponding candidate table immediately and select another actor in the candidate table to provide service. The agent actors only need to monitor and compute the trust rating. The actors need to rank the trust rating values which distributed by the agent actor.

Result analyses: In Fig. 2, we show the simulation result of Fig. 1a. Actor M does well in date collection (application α_1) and time-synchronization (application α_2), so that the trust rating of α_1 and α_2 are high so that the actor would be of more chances to be selected to provide corresponding application service for actor A after ranking process. But the trust rating of α_3 (delivers packet for actor.) is low. But RFSN just give a fixed trust value that couldn't reflect true performances of actor about different applications. Our proposed trust model is more suitable for WSNs.

In Fig. 3, that is the simulation result of Fig. 1b. actor M has high trust value in the begin of several window times and selected to provide service for actor E in the fourth time window, in this time window, this malicious actor launches malicious attack, from Fig. 2, we can find RARRM takes effect and punish actor M strictly. In the following time windows actor M has no chance to get into candidate table and be chosen to launch malicious attack. Our RARRM can detect On-Off attack (Ganeriwal and Srivastava, 2004) effectively. Our proposed protocol can construct trustworthy SNs.

CONCLUSION

In this study, we propose Rank-based Application-driven Resilient Reputation Model to enforce the security of SNs. The agent actors monitor the behavior of actors to distribute the trust rating. The system is distributed and we selectively make use of the secondhand information to build trust system according to certainty of estimated trust value. Our RARRM scheme is more suitable for trust system in SNs due to its rank-based dynamic selection of actor and its confidence-based trust rating. An actor has several trusting rating in SNs. It can be used in large scale SNs. With the growing importance of SNs applications, our scheme helps to provide a more accurate guarantee to detect the malicious actors in different application in SNs.

ACKNOWLEDGMENT

This study was supported by the Program of Shanghai Normal University(A-3101-12-004005). And the research work in this study was also sponsored by the Innovation Programs of Shanghai Municipal Education Commission and the project numbers are 09YZ154 and 09YZ247.

REFERENCES

Abdul-Rehman, A. and S. Hailes, 2000. Supporting trust in virtual communities. Proceedings of the 33rd Hawaii International Conference on System Sciences, January 4-7, 2000, Maui, Hawaii, pp: 6007.

Aberer, K. and Z. Despotovic, 2001. Managing trust in a Peer-2-Peer information system. Proceedings of the 9th International Conference on Information and Knowledge Management, November 6-11, 2000, McLean, VA., USA., pp: 310-317.

Beth, T., M. Borcherding and B. Klein, 1994. Valuation of trust in open networks. Proceedings of the 3rd European Symposium on Research in Security, November 7-9, 1994, Springer-Verlag, Brighton, UK., pp: 3-18.

Buskens, V., 2002. Social Networks and Trust. Springer, The Netherlands, ISBN: 9781402070105, Pages: 269.

Easley, D. and J. Kleinberg, 2010. Overview. In: Networks, Crowds and Markets: Reasoning about a Highly Connected World, Easley, D. and J. Kleinberg (Eds.). Cambridge University Press, Cambridge, ISBN: 978-0-521-19533-1, pp: 1-20.

Ganeriwal, S. and M. Srivastava, 2004. Reputation-based framework for high integrity sensor networks. Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks, November 3-5, 2004, Washington, DC., USA., pp: 66-67.

Kuter, U. and J. Golbeck, 2007. Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models. Proceedings of the 22nd National Conference on Artificial intelligence, Volume 2, July 22-26, 2007, Vancouver, pp: 1377-1382.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure ad hoc networks. Proceedings of the IEEE Conference on Aerospace, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

Sun, Y.L., Z. Han and K.J.R. Liu, 2008. Defense trust management vulnerabilities in distributed networks. IEEE Communi. Magazine, 46: 112-119.

Wasserman, S. and K. Faust, 1994. Social Network Analysis in the Social and Behavioral Sciences. In: Social Network Analysis: Methods and Applications, Wasserman, S. and K. Faust (Eds.). Cambridge University Press, Cambridge, ISBN: 9780521387071, pp: 1-27.

Zukin, S. and P. DiMaggio, 1990. Structures of Capital: The Social Organization of the Economy. Cambridge University Press, New York, ISBN: 9780521376785, Pages: 449.