Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 13 No. 2, June, 2022 - www.cisdijournal.net

Trust Management in a Friend-to-Friend Network

Aderibigbe, O.S.
Department of Computer Sciences
Lagos State University of Science and Technology
Ikorodu, Lagos State, Nigeria.
E-mail: aderibigbe.os@lasustech.edu.ng

ABSTRACT

Trusting a person that one has not had any collaboration with is risky, but when there is a trust relationship the feeling of being vulnerable or that others can take advantage of the trustee will not be there. Moreover, a trusted friend can equally change and become dubious since trust is not immutable and it changes from time to time. There is a need for mechanisms that will guarantee and enforce normative behaviours and at the same time, increase online collaboration by stimulating potential users' trust towards the friends on the network. This research leveraged on Distributed Hash Table (DHT) and the Symmetric Replication Technique (SRT) to ensure availability of trust data for trust computation. To be able to use the DHT and the SRT, the concept of trustworthiness was conceptualized and operationalized into personal trust, reputational trust and recommendation trust. The architecture of the Trust Aware Model deployed on the F2F network, performed the function of peer trust update with respect to a peer's collaborating level of trustworthiness thereby enabling effective management of trust in an F2F network that will bring about a robust F2F collaboration.

Keywords: Trust Management, Collaborative Model, Distributed Hash Table, Symmetric Replication Techniques

CISDI Journal Reference Format
Aderibigbe, O.S. (2022): Trust Management in a Friend-to-Friend Network. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 2. Pp 73-.80. Available online at www.computing-infosystemsjournal.info
CrossREF DOI No - dx.doi.org/10.22624/AIMS/CISDI/V13N2P7

1. INTRODUCTION

Trust is defined as the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action that is important to the trustor, irrespective of the ability to monitor or control the other party (Mayer *et al.,* 1995). Rousseau *et al.* (1998) defined trust as the psychological state, in which the intention to accept vulnerability is based upon the positive expectations of the intentions or behaviour of another. Also, Lewicki *et al.* (1998) described trust as an individual's belief in, and the willingness to act based on, the words, actions, and decisions of another. Kramer and Carnevale (2001) argued that trust involves a set of beliefs and expectations that a partner's actions will be beneficial to one's long-term self-interest. This is expected in situations in which the partner must be counted on to provide unique benefits or valuable outcomes. Trust-relevant situations typically activate two cognitive processes: (a) feelings of vulnerability, and (b) expectations of how the partner is likely to behave across time, particularly in strain-test situations. Trust-relevant emission and detection mechanisms should have evolved in humans, given the importance of gauging accurately the intentions of others (Tooby and Cosmides, 1996).

There are two types of trust between peers in P2P networks, which are direct trust and recommended trust. Direct trust is trust between two peers that directly exchange information while direct reputation is based on previous experience. In recommended trust, the two peers never exchange information directly but they establish trust relationship based on the recommendation from other peers (Cheng *et al.,* 2012). In the theoretics of trust; trust-like values are of different types, each of which can be represented formally.

2. LITERATURE REVIEW

Several researchers have recently focused on trust and reputation management, attributed to the growth in interpersonal communication and collaboration. Trust must be considered for effective collaboration. Wang and Vassileva (2003) proposed a trust model based on the quality of service provided by an agent using the Bayesian network. Two types of trust were considered: trust in an agent's ability to provide quality service, and trust in the ability of the agent to provide quality recommendation. In the context of their work, trust was defined as peers believing in another peer's reliability based on previous interactions, while reputation was described as a peer's belief in another peer's reliability based on recommendations from trusted peers. Both trust and reputation were used to calculate the trustworthiness of other peers.

The system was not tested under other performance measures such as the speed of locating trusted peers. Nguyen *et al.* (2008) proposed a probabilistic model to handle trust in a P2P setting. The model supports local computation and a simple form of propagation of the trust of peers into classes of other peers. In the work, it was shown that the model was able to handle the dynamics of P2P networks. The freedom enjoyed by each peer within the network to have different viewpoints towards the peers with whom they interact was maintained by the model. The approach was based on a Bayesian estimation of trust, giving priority to direct experiences. It is only when this information is not available or sufficient that observations from other peers in the network are collected.

Researchers also developed the Eigen Trust Algorithm (ETA) for Reputation Management in P2P Networks. In Kamvar *et al.* (2003), the ETA was developed to handle the decrease in the number of downloads of inauthentic files in a peer-to-peer file-sharing network. This type of network assigns each peer a unique global trust value, based on the peer's history of uploads. The work contributed to knowledge by presenting a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network. The result of the research showed a significant decrease in the number of inauthentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately subvert the system. Akinboro (2014) proposed a trust management framework in mobile ad-hoc networks to secure home devices and communication channels against attacks. In the work, the trust management for the device attack was modelled using Adaptive Neuro-Fuzzy (ANF) that considered the global reputation of the client and indirect communication of the home device and remote devices. Results show that it enhanced the activities in the home by securing the home network against unforeseen attack disruption and node misbehaviour. Although activities of malicious users impersonating authorized or trustworthy devices on the network were not considered. In Tan *et al.* (2011), a distributed trust model named P2PETrust (peer-to-peer E-commerce trust model) based on social networks' principles was developed. The result from simulating the model shows that trust can resist single and team malicious nodes.

But there were still several issues that were not resolved in the work. They include: How to improve the distributed communication algorithms for the P2P Trust model, and how to use more trust principles of social networks for the P2P Trust model. The work of Xiong and Liu (2004) also contributed to the trust management literature by proposing the Peer Trust model. The model supported the Reputation-Based Trust for Peer-to-Peer electronic communities. The reputation-based trust represents a framework, which includes a coherent adaptive trust model. The model was also useful for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. The model decentralized the implementation of the model over a structured peer-to-peer overlay network. Based on experimental results, the model showed a lot of promise in terms of feasibility, effectiveness, and the benefit of the approach.

3. METHODOLOGY

Trust management in a friend-to-friend network requires accessing existing collaborative models for trust awareness. This is done with a view of detecting which collaborative model(s) perform what tasks in ensuring that trust data is available when required. The tasks that were determined include lookup, availability, and trust computation. Moreover, peer-to-peer networks are susceptible to churn. Therefore, trust data must be available for trust computation to determine the trustworthiness of the participating peers in the network. The philosophy of trust is contingent upon the issue of reliability and effectiveness. This highlights the need for both a theoretic and a pragmatic methodology for this research. Hence, this work presents a discourse on the methodology that was applied in achieving the overall goal. The Trust-Aware model was created using the Distributed Hash Table (DHT) and Symmetric Replication Techniques (SRT).

As earlier discussed, this work draws on the theory of trust (Kramer and Carnevale, 2001), which is built around processes that connote feelings of vulnerability and the expectations of how a partner is likely to behave over time. An example of a trust-relevant situation is the strain-test situation. Therefore, trusting a person with whom one has not had any collaboration is risky. This is because there will be a feeling of being vulnerable, and at the same time, a trusted friend can equally change and become dubious. Moreover, trust is not immutable and it changes from time to time, hence a trust model becomes necessary for a friend-to-friend network (Truong *et al.,* 2011). When a trustor takes a risk on a trustee that leads to a positive outcome, the trustor's perceptions of the trustee are enhanced. Likewise, the perceptions of the trustee will decline when trust leads to unfavourable conclusions (Mayer *et al.,* 1995). This means that when engaging in trusting behaviour, trust will be affected directly. No matter the type of trust model, two pieces of basic information - self-experience information (interaction-derived or first-hand information) and ratings (or second-hand information) - are necessary to calculate their trustworthiness (Liang and Shi, 2008). These necessitate getting recommendations from trusted friends and also the continuous computation of the trustworthiness of friends on a network.

The foregoing scenario was modelled following the practice demonstrated by Netrvalova and Safarik (2009, 2012). Based on this, personal trust, reputational trust, and recommendation trust were integrated into the trust model in this work. The purpose of the integration is to enable the model to effect updates of peer trust after each collaboration. Each node on the friend-to-friend network maintains local trust data of all the nodes it had interacted with. An effective lookup service feature was required to achieve this. The DHT structure was used in the research work to provide decentralized and effective access to trust information (Manju and Govindaraj, 2014).

This was also required in order to ensure easy location of trust data for the computation of personal, reputational, and recommendation trust. In this research work, the Chord distributed hash table, owing to its simplicity, provable correctness, and performance, was introduced to provide the lookup service feature in the model. The lookup feature was used to handle challenges that pertain to issues of churn, scalability, decentralization, availability, and flexibility naming.

3.1 The DHT Lookup Services for Trust-Aware Model

A DHT data structure was designed and used to ensure that an identified item is found. Given a key, the developed model was able to map the key to a node that is responsible for storing the data associated with the key. The choice of the Chord DHT type of DHT is because it is able to scale thousands of nodes and handle rapid arrivals and failures. With the introduction of the Chord DHT, the developed trust-aware model was able to use the lookup service to acquire information on a specific node, including its IP address, service port, and the location of a peer. The DHT service also enables the trust-aware model to easily locate nodes with trusted data on the F2F network. Chord nodes usually maintain two sets of neighbours, which are its successor and its finger. The successor is the node that immediately follows in the identifier space, while the finger nodes are spaced exponentially around the identifier space.

Each node has a successor and a predecessor. Peer-to-peer networks always experience situations where nodes leave the network abruptly. Based on this experience, it was necessary to ensure that each node keeps the record(s) of the preceding nodes and the ones following it. Each node also needs to maintain information about its fingers in a finger table. It is interesting to state that each of the nodes in a network, say N, is either a successor or a predecessor node, such that each of them also maintains a finger table. Each of the finger tables of the nodes was adapted to ensure that the first information to be found is information about a successor node.

The main reason for data replication was to ensure increased data availability, improved performance, and then achieve load balancing. In this research, the main reason for data replication was availability. This makes it necessary to make trust data available. The way to solve this problem was to replicate trust data to other nodes in the network. The Symmetric Replication Algorithms (SRA) were employed. It was therefore possible for peers to decide what should be replicated, how many replicas should be created, where to replicate them, and the replica replacement strategy. The SRA made the foregoing possible.

4. TRUST EVALUATION

The evaluation of the trustworthiness of a peer by another required the use of an appropriate trust mechanism or function that computes trust value from available trust information or trust data. This was introduced in the trust-aware model following the practice in Reddy and Seshadri (2014). The rationale for this is to ensure that this work is consistent with existing work. Thus, the rating degree and value of reputation that was used in this research work is as shown in Figure 4.1 and Table 4.1. The values assigned to each level of trustworthiness was based on the previous interaction experience during collaboration.

The level of trust that was used ranges from complete distrust to blind trust. These trust values formed the basis for peer ratings after collaboration or based on previous collaborative experiences. Moreover, trust in real life can be quantified by a value in an interval say $\langle a,b \rangle$ where $a,b,(a<b)$ are integer or real numbers.

In this research work, trust was represented by a value from the continuous interval say $\langle 0,1 \rangle$ where 0 represented complete distrust and 1 represented complete trust (Netrvalova and Safarik, 2012).

Additionally, considering *n* subjects that are representable as the set $P = \{p_1, p_2, ..., p_n\}$, the measure of personal trust between the subjects p_i and p_j was modelled and introduced as follows:

$$t_{ij} = t(p_i, p_j), t_{ij} \in \langle 0,1 \rangle, \quad (4.1)$$

where

$$i, j = 1, ..., n, \quad i \neq j,$$

and

$$\sum_{j=1, j \neq i}^{n} t_{ij} = 1 \quad (4.2)$$

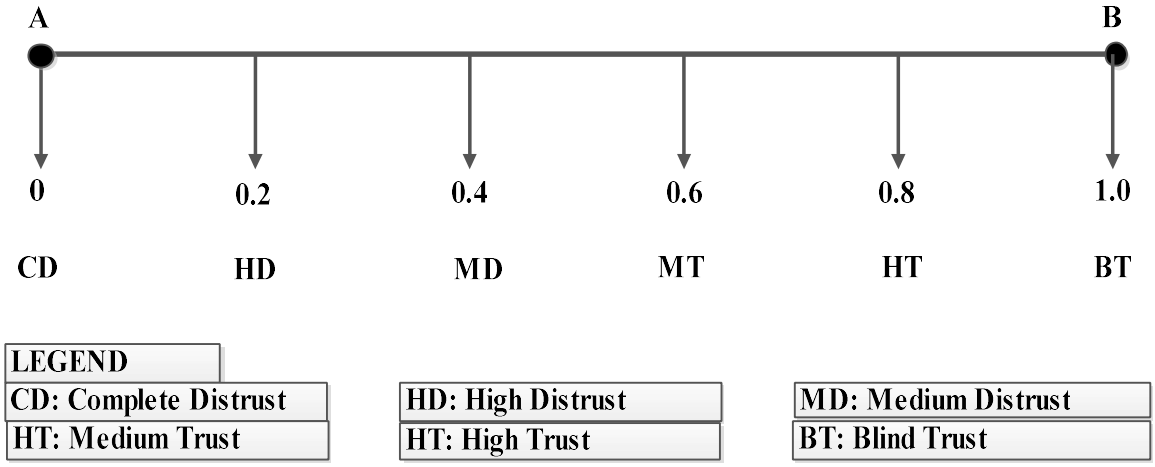

Figure 4.1: Trust Rating Scale
(Source: Netrvalova and Safarik, 2011)

Table 4.1: Rating degree and value of reputation

Rating	Degree	Value
Complete Distrust	0	0
High Distrust	1	0.2
Medium Distrust	2	0.4
Medium Trust	3	0.6
High Trust	4	0.8
Blind Trust	5	1.0

After a collaboration a peer was able to update its trust in the collaboration. It was also able to do so for the peer that provided the recommendation on behalf of others. This will be made possible following the proposals of Wang and Vassileva (2003).

This proposal was enforced using the technique provided by the reinforcement model as follows:

$$tr_{ij}^{n} = \alpha * tr_{ij}^{0} + (1-\alpha) * e_{\alpha} \qquad (3.3)$$

Where

tr_{ij}^{n} = the trust that i^{th} peer has in j^{th} peer's recommendation.

tr_{ij}^{0} = the old trust value.

α = the learning rate, a real number in the interval [0, 1].

e_{α} = the new evidence value which is -1 or 1.

In the reinforcement model in (3.2), when the value of the recommendation is greater than 0, the collaboration was successful, then e_{α}=1.

But, if there is a mismatch between the recommendation and actual recommendation then e_{α}= -1. For Reputational Trust (RT); a peer's RT is the arithmetic mean of the peer's neighbours rating values. The RT trust provided by all the peers in the network that had collaborated with j^{th} peer given by r_t was modelled using the computational model for reputation as practiced in Netrvalova and Safarik (2012) following best practice.

This model is expressed as:

$$r_t = \frac{\sum_1^n r_{jv}}{n} \qquad (3.4)$$

Where

r_{jv} = peer's trust rating of j^{th} peer given by n actors in the friend-to-friend network.

This model required some algorithms to perform specific tasks in ensuring that trust data are available when needed. These tasks included lookup activities and trust computation. Additionally, since peer-to-peer networks are often susceptible to churn, it was therefore necessary to ensure that trust data would be available for trust computation. To create the intended computational model, a Distributed Hash Table (DHT) and the Symmetric Replication Technique (SRT) were leveraged. To be able to use the DHT and the SRT, the concept of trustworthiness was conceptualized and operationalized into personal trust, reputational trust and recommendation trust. As a result, an effective lookup service feature was introduced using the Chord technique of the DHT.

The lookup feature was able to handle challenges that bothers on issues of churn, scalability, decentralisation, availability and flexibility of naming. The model is intended to invoke the social trust manager in order to initiate the lookup service feature so as to acquire information on a specific node including its IP address, service port and location as a peer on the F2F network. To ensure that trust data is available during lookup, the data must be replicated to appropriate nodes using appropriate data replication strategy. This was achieved using the symmetric replication algorithm, which implemented the replication strategy.

5. CONCLUSION

This research work presented a Trust-Management Model for Friend-to-Friend Networks. The developed Trust-Management Model for friend-to-friend collaboration was necessary since the effective management of trust in an F2F network can bring about a robust F2F collaborative knowledge sharing. The introduction of philosophy of trust using social trust provided a novel approach towards ensuring a secured online collaboration.

REFERENCES

1. Akinboro, S. A. (2014). Development of a Trust Management Model for Mobile Ad-hoc Network. A Ph.D Thesis Submitted to the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria.
2. Kamvar, S.D., Schlosser, M.T, and GarciaMolina, H, (2003). The EigenTrust Algorithm for Reputation Management in P2P Networks. In *Proceedings of ACM WWW*, pp. 640-651.
3. Cheng, C.L., Xu, X.L., and Gao, B.Z. (2012). METrust: A Mutual Evaluation-based Trust Model for P2P Networks. *International Journal of Automation and Computing,* 9(1): pp. 63-71.
4. Kramer, R.M., and Carnevale, P.J. (2001). Trust and Intergroup Negotiation. In R. Brown & S. Gaertner (Eds.), Blackwell handbook of social psychology: Intergroup processes (pp. 431–450). Malden, MA: Blackwell Publishers.
5. Lewicki, R. J., McAllister, D. J., and Bies, R. J. (1998). Trust and Distrust: New Relationships and Realities. *Academy of Management Review, 23: pp.* 438-458.
6. Manju, J., and Govindaraj, F. (2014). A Survey of Trust Management in Peer-to-Peer Systems. *International Journal of Computing and Technology* (IJCAT), 1(2), pp. 2248-6090.
7. Mayer, R. C., Davis, J.H., and Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20(3), pp. 709-734.* Available at: http://www.jstor.org/stable/ 258792.
8. Netrvalova, A. and Safarik, J. (2009). Interpersonal Trust Model. Proceedings *MATHMOD* 2009 Vienna, pp. 530-537.
9. Netrvalova, A. and Safarik, J. (2011). Trust Model for Social Network. ESM 2011, pp. 102-107.
10. Nguyen, G.H., Chatalic, P., and Rousset, M.C. (2008). A probabilistic trust model for semantic peer to peer systems. In *Proceedings of the 2008 International workshop on Data management in peer-to-peer systems* (pp. 59-65). ACM.
11. Reddy, T.C., and Seshadri, R., (2014). Reputation-Based Dynamic Trust Evaluation Model for Multi-Agent Systems Based on Service Satisfaction. *International Journal of Emerging Technology and Advanced Engineering*, 4(6): pp. 158-168.
12. Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so Different After All: A Cross-Discipline View of Trust, In Academy of Management Review, 23: pp. 393-404.
13. Tan, Z., Cheng, W., Ma, Y., Zhu, Z., and Chang. G, (2011). P2PETrust: A novel distributed transaction history vector-based trust appraisal model for peer-to-peer ecommerce Networks. Scientific Research and Essays, 6(18), pp. 3845-3857.

14. Tooby, J., and Cosmides, L. (1996). Friendship and the Banker's Paradox: Other Pathways to the Evolution of Adaptations for Altruism. In Proceedings of the *British Academy*, 88: pp. 119–143.
15. Truong, H. T. T., Bouguelia, M. R., Ignat, C. L., and Molli, P. (2011). Collaborative Editing with Contract over Friend-to-Friend Networks. Retrieved from http:// homep ages.la as.fr/mkilliji/APVP2011/Site/ Programme_files/Artigle_4.pdf on 21/10/2014 @11:30pm
16. Wang, Y., and Vassileva, J. (2003). Trust and Reputation Model in Peer-to-Peer Networks. In *Proceedings of IEEE Third International Conference on Peer-to-Peer Computing*, (pp. 150-157).
17. Xiong, L, and Liu, L (2004). PeerTrust: Supporting Reputation-based trust for peer-to-peer electronic communities, Knowledge and Data Engineering, *IEEE Transactions on* 16(7), pp. 843-857.