Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 5 (2013) 281 – 286

AASRI Procedia

www.elsevier.com/locate/procedia

2013 AASRI Conference on Parallel and Distributed Computing and Systems

TrustP2PNet: P2P Social Network with Admission Control Model based on Trust

Wu Liu [1)], Ping Ren [2)], Donghong Sun [1)], Ke Liu [3)], Jianping Wu [1)]

1)Network Research Center of Tsinghua University, Beijing, China
2) College of Mathematics Science, Chongqing Normal University, Chongqing, China
3)Tsinghua University Park, China Citic Bank, Beijing. China

Abstract

This paper proposed a Trust based Admission Control Model (TACM) for P2P network, and implemented a P2P social network system TrustP2PNet based on TACM. The TrustP2PNet is composed of application layer proxies with P2P structure. Additionally, a admission control model based on recommendations from trustable friend in social networks is proposed to prevent malicious peers fromthe TrustP2PNet. Both the simulation results and the practical application of TACM in the system TrustP2Pnet show that, with our model, it can not only effectively protect the system from malicious peers but alsopossessvery good scalability.

KeyWords: Trust; Network Security; P2P Network; Access Control.

1. Introduction and Related Work

The Internet brings us great benefit[1][2][3] for work, studying, life and entertainment etc. Ideally speaking, you can get accessed to anyplace that is willing to provide information for you. However, for some reasons, such case is not always true[4][5][6]. We can tolerate that the website with bad content such as sex and violence are banned for the common good of society, but it may be a big pity that some websites with academic disputations are banned so not reachable only for political reason. Moreover, one path may be broken down resulting in some websites not available to certain people, but actually they can still visit the

doi:10.1016/j.aasri.2013.10.090

webs after many attempts of trying other way only if the websites have other paths. In addition, sometimes though the websites are still available to us, we can always find a best way, i.e. with the highest speed to use.

In one word, we need a put up way which can make the accessibility of Internet more robust with better performance. P2P systemis answer we find. In a typical P2P system, there is not any center server, and only a register server generate identifications for the nodes who want to join the system, but not one is responsible for monitoring the behaviors single nodes. When strange nodes come to certain nodes and request for service, the requested nodes make their own opinions on response positively or negatively, according to their knowledge of the coming nodes.

The P2P work style bring huge advantages to the system. First of all, the Internet is more accessible for the users. Those banned websites to certain people for political or technical reasons may now be available to them. Only if the websites have links with nodes in the system, there is hope that they can be visited hence make useful information be shared by more people. Secondly, no central node which is responsible for the authentication or data transferring of all nodes exists in the system, hence avoid the bottleneck. The maintenance of central server always costs heavy economical and technical load and affects the performance of the system when large data in running. Thirdly, all the nodes in the system are of the same importance and function, hence have good robust for no of the broken down of single node can cause disasters to the system. Even no disaster happens, when more than one path exists, the nodes can find a better way to enjoy better performance.

As to the problem that how the nodes join the system, currently popular P2P software does not put up an effective way. A common way as BitTorrent adopts is to let all nodes join in the system only if they wish. They do not care whether a certain node is honest or malicious in the beginning. They put up sets of methods to evaluate and stimulate the behaviors of nodes---- sometimes the stimulation is too weak to make sense, and such mechanism shall cause delay between the coming of malicious nodes and the finding of them. There is no effective mechanism to make sure the good identification of nodes hence cause hidden insecure trouble to the system.

And on the other hand, for the nodes within the system, when they want to demand some service, they may not know the better choice. The ones with the highest evaluation in the system do not necessarily mean the best service provider for every node. They may even been not available to some of them.

In order to solve the two problems mentioned above, we put up the trust system based on social networks to work.

2. TrustP2PNet

Here, the TrustP2PNet which we proposed is proxy working in the application layer overlaid above the physical networks of Internet. It is consist up with the nodes and their available parts of the Internet. When a node wants to visit some place inaccessible for him, he pack the destination in the datagram and sent to the nodes who might reach the destination. When another node receives the datagram, he picks up the destination and transfers the data for the original node.

The TrustP2PNet works as a typical P2P system without the intervention of center server. Only a register server generate identifications for the nodes who want to join the system, but not one is responsible for monitoring the behaviors single nodes. When strange nodes come to certain nodes and request for service, the requested nodes make their own opinions on response positively or negatively, according to their knowledge of the coming nodes.

The TrustP2PNet and its P2P work style bring huge advantages to the system. First of all, the Internet is more accessible for the users. Those banned websites to certain people for political or technical reasons may now be available to them. Only if the websites have links with nodes in the system, there is hope that they can

be visited hence make useful information be shared by more people. Secondly, no central node which is responsible for the authentication or data transferring of all nodes exists in the system, hence avoid the bottleneck. The maintenance of central server always costs heavy economical and technical load and affects the performance of the system when large data in running. Thirdly, all the nodes in the system are of the same importance and function, hence have good robust for no of the broken down of single node can cause disasters to the system. Even no disaster happens, when more than one path exists, the nodes can find a better way to enjoy better performance.

In order to solve the two problems mentioned above, we proposeda trust system based on social networks which run on the application layer.

3. Trust based Social Networks

The area of trust and reputation in P2P systems has been a hot subject.However, so far away they do not have favorable mechanisms. Most of their solutions are based on an accumulative credit system. They don not refuse any peers, honest or malicious, to join in the system, but confine their behaviors according to their score. This way necessarily causes delay between malicious nodes. Moreover, such mechanism often deploys a center server to record and update the credit score of the peers. It introduce more risk of attacks on the center server for the malicious peers want to rise their scores to gain more service. If the system is totally distributed, they may have to conquer many of the other peers to realize their aim, however now they only have to attack one server. Compared with the huge benefits they may gain, such energy is worth.

In order to overcome such disadvantages listed above, we proposed the trust system based on social networks. We suppose that people can always trust their friends who they know well, and can rely on their opinions of unknown people. Experientially people always believe in themselves better than others, but when they have no idea of something, the knowledge from their friends is better than just guessing out of all reason. The initial users of the system are always honest until malicious peers join in to generate the unfairness. And when people in system find malicious peers they are willing to inform their friends to erase them. Based on these common senses we proposed our model as follows.

4. Trust based Admission Control Model (TACM)

Before discuss the model, we define two basic concepts: Trust Value $TV_{pq}$and Recommendation Value RV_{pq}between node P and node QTV_{pq} is theprobabilitythatreflects the degree of how node Ptrust node Q. thevalues of TV_{pq}vary from 0 to 1. For the most trustable node (say M)of P and P itself, the Trust value can be equal to 1, i.e. $TV_{pm} = 1$, and $TV_{pq} = 1$; And for a node N which is stranger for P, the trust value is 0, i.e. $TV_{pn} = 0$. The Recommendation Value RV_{pq} reflects the trust degree that node P recommends node Q to other nodes. Here we restrict the Recommendation Valuebetween 0 and 1.For node P itself and nodes M with very high Trust Value TV_{pm}, the Recommendation Value $RV_{pm}$to 1, i.e. $RV_{pm} = 1$. And for some node Mwith whom we do not familiar, the RecommendationValue RV_{pm}will be small. And for node Q whom we do not recognize or do not trust, the RecommendationValue RV_{pm}will be 0, i.e. $RV_{pm} = 0$.

Initially, all the nodes in the system are supposed to be honest. And at the beginning, only those who know each other directly can construct Trust relationship and recommend for each other. Here define some $0<TV_{\Delta}<1$ as the trust threshold. If $TV_{pq} \geq TV_{\Delta}$, we say that node Q is trustable for node P, and if $TV_{pq} < TV_{\Delta}$, then node Q is not trustable to node P. Here the above assumption is just used to simplifystructure of our trust model. For any two nodes A and B that do not exist any direct connection, we set $TV_{ab} = 0$and $RV_{ab} = 0$.

The nodes with Recommendation to each other construct the initial system. When a new node N comes and tries to join the system, N has to find at least one node in the system already to trusts and recommends it,

we called it becomes the friend of the node in the system, otherwise it can only be anisolated node out of the system. And once it gainsthe trust of somenode, it can be regarded to join in the system successfully.
Then when a new node X comes to node P and ask for its permits to join in, P can make two choices:

1) ifP knows X well and regard it believable, then set:

$$\begin{cases} \mathrm{TV}_{px} = 1 \\ \mathrm{RV}_{px} = 1 \end{cases}$$

2) ifP does not know X well, the trust value TV_{px} is calculated via recommendation: P ask for its friends forX's credit:

$$\mathrm{TV}_{px} = \theta \cdot \mathrm{TV}_{px} + \mu \cdot \frac{\sum_{i \epsilon F_P} \mathrm{TV}_{pi} \cdot \mathrm{RV}_{ix}}{\sum_{i \epsilon F_P} \mathrm{RV}_{ix}}$$

Where, i stands for the set of all the friends for node P, and RV_{ix} is the Recommendation value that node i recommends x. TV_{px} is theinitialtrust value that node P trust node X. $0<\theta<1$, $0<\mu<1$, and $\theta + \mu = 1$.

If $\mathrm{TV}_{px} \geq \mathrm{TV}_{\Delta}$, it is said that node P trust node X, set $\mathrm{RV}_{ix} = 0.5$, which means that node P knows node X indirectly and recommend it with reservation;

If $\mathrm{TV}_{px} < \mathrm{TV}_{\Delta}$, it is said that node Pdoes not trust node X, and set $\mathrm{RV}_{ix} = 0$.

θ(and $\mu = 1 - \theta$) is a control factortwo adjust the weight of trust value between itself and its friends.

And$\frac{\sum_{i \epsilon F_P} \mathrm{TV}_{pi} \cdot \mathrm{RV}_{ix}}{\sum_{i \epsilon F_P} \mathrm{RV}_{ix}}$ reflects multiple nodes'trust on to a single one: if some node is more trustableto node P, it will get more recommendationtrust which will increase itstotaltrust value.

5. Implementation of the Model TACM in TrustP2PNet

We apply the formula into the TrustP2PNet Project and design the TrustP2PNet system which is an application overlay of the physical networks. It is constructed by thenodes and their accessible parts of the Internet. every peer in the systemis a proxy which voluntarilyrelay the traffic of pass through it . Each node of TrustP2PNet is composed of 4subsystems: The Functional-Module, the Calculation-Engine,the Friends-List and the Evaluation-Engine. Where, theFunctional-Module is used fortransferring traffic, registering andother functions. Our policy model for admission control is implemented inthe calculation engine.When a new node comes, the calculate engine is responsible to calculate its trust value and reflect to the friend list to record, and when the node interact with some new node, as the functional module offers or demands the service, the evaluate engine estimate the Recommendation and record in order for further calculation for the calculate engine.

6. Parameters and Simulations

Obviously, whether a node can join the system depends on the parameterθ, which reflects the degree a node believe in itself or believe in the friends, and TV_{Δ}, which reflects a node adopts a strict policy on making friends or a loose one.

Consider a random system as below. There are twenty nodes initially, most of the honest nodes in red have constructed the system but left a few honest nodes in the out as well as some malicious nodes in green.

If the system does not offer knowledge about the new nodes and let single nodes to make judgments by themselves, they may choose to accept or refuse to add the new node randomly due to an absence of effective way to evaluate the new comer. The result is obvious that malicious nodes join in the system as easily as

honest ones. That's a common way adopted by most of current P2P systems. It depends much on mechanisms in later phase to erase the malicious nodes.

And if nodes in the system adopt very strict policy on permitting new comer, namely they only add who they know directly to the system, in other words let θ equals to 1 and omit all friends' recommendation, we can deduce another result: malicious nodes cannot be added in easily nor can the system expand easily.

And with our model, depending on different $\theta$and TV_{Δ}, considering the portion of new coming nodes and total nodes in the system as the result of the system development, we can gain a three-dimensional picture.

And other points of values of θ and TV_{Δ} do not seem to have much affection on the curves, so we set:$\theta = 0.8$ and $TV_{\Delta} = 0.8$

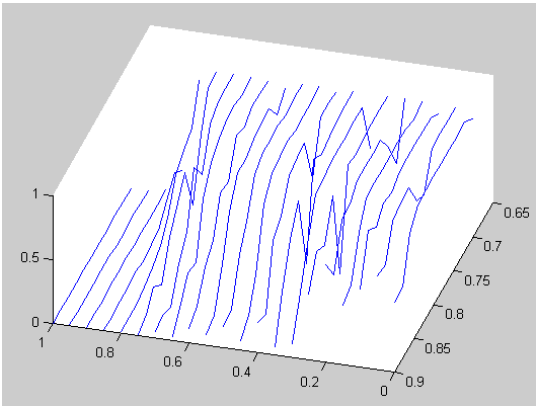

Figure 1.we can see when the abscissa: θ is bigger than 0.8, hardly does the portion of new nodes to total nodes increase. It reflects the abovediscussion, if one over emphasize its own opinion and omit friends' recommendations, the system is hard to expand. So θ in our model should be smaller than 0.8.

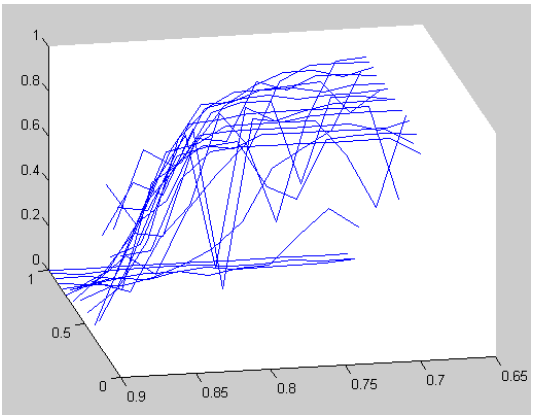

Figure 2.we can see when TV_{Δ} is between 0.9 and 0.85 the proportion is always increasing and not stable. So we can set TV_{Δ} smaller then 0.8 to gain a stable status.

7. Conclusion

In this paper, we proposed a Trust based Admission Control Model TACM for P2P network, and implemented a P2P social network system TrustP2PNet based on TACM. The TrustP2PNet is composed of

application layer proxies with P2P structure. Additionally, an admission control model based on recommendations from trustable friend in social networks is proposed to prevent malicious peers fromthe TrustP2PNet. Both the simulation results and the practical application of TACM in the system TrustP2Pnet show that, with our model, it can not only effectively protect the system from malicious peers but alsopossessvery good scalability.

8. Acknowledgment

This work is supported by grants from the National Natural Science Foundation of China (Grant No. 61272427), and the China 863 Project (Grant No.2011AA010704 and 2012BAH38B03).

References

[1]Giovanni Neglia, Giuseppe Reina, Honggang Zhang, Don Towsley, ArunVenkataramani, and John Danaher. Availability in BitTorrent Systems. Proceedings of IEEE INFOCOM. IEEE CS, 2007.
[2]D. Qiu and R. Srikant. Modeling and performance analysis of bittorrent-like peer-to-peer networks. Proceedings of ACM SIGCOMM, 2004.
[3]J. Douceur. The Sybil Attack. Proceedings of the first International Workshop on Peer-to-Peer Systems (IPTPS'02). Springer, 2002.
[4]Saroiu S, Gummadi P.K, Gribble S.D. A measurement study of peerto-peer files sharing system. In: Multimedia Computing and Networking, 2011, San Jose: SPIE, 156-170
[5]H. Rowaihy, W. Enck, P. McDaniel, and T. La Porta. Limiting Sybil attacks in structured peer-to-peer networks. Technical Report NASTR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July 2005.
[6]Atul Singh, Tsuen-Wan .Johnny. Ngan, Peter Druschel., and Dan S. Wallach. Eclipse Attacks On Overlay Networks: Threats and Defends. Proceedings of IEEE INFOCOM, 2006.
[7]Richard Thommes and Mark Coates. Epidemiological Models of Peer-to-Peer Viruses and Pollution. Proceedings of IEEE INFOCOM, 2006.
[8]S. Marti and H. Garcia-Molina. Limited reputation sharing in p2p systems. Proceedings of 5th ACM conference on Electronic commerce, pp.47-55, 2004.
[9]E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. Proceedings of the Ninth ACM Conference on Computer and Communications Security, pp.207–216, 2002.
[10] BimalViswanath，Krishna P. Gummadi，Ansley Post and Alan Mislove.An Analysis of Social Network-Based Sybil Defenses. Proceedings of ACM SIGCOMM, New Delhi, India, August 30–September 3, 2010.
[11] S. Ratnasamy, M. Handley, R. Karp, and S. Shenker. Topologically- Aware Overlay Construction and Server Selection. Proceedings of IEEE INFOCOM, pp. 1190–1199, Jun. 2002.
[12] Zhang H, Duan HX, Liu W, Wu JP. RRM: An incentive reputation model for promoting good behaviors in distributed systems. SCIENCE IN CHINA SERIES F-INFORMATION SCIENCES,vol.51, no. 11, pp. 1871-1882
[13] Chakraborty S, Ray I. TrustBAC-Integrating Trust Relationships into the RBAC Model forAccess Control in Open Systems. Proceedings of ACM Symposium on Access ControlModels and Technologies. Lake Tahoe. ACM Press, 2006. 49–58.