International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.1, January 2014 DOI:10.15693/ijaist/2014.v3i1.10-14

Secure Shell Transfer Through Malicious Nodes From Peer To Peer

R.Gayathri
PG Scholar
MNSK College of Engineering
Vallaththirakottai, Pudukkottai

V.Vaishnavi
Assistant Professor
MNSK college of Engineering
Vallaththirakottai, Pudukkottai

***Abstract*: The locality of peer to peer communications offers more and more cruel attack in entirely different ways. In existing system minimize the attacks in such communities is to use community based reputations which help to estimate the honesty of peers. It collects the feedback from other peers on the network to improve the fedility.The proposed system presents the peer system create a secure structure of file based on IP address of transmitter and receiver and then transmit to another peer. The secured transmitted file is only opened by the beneficiary peer and this structure safeguards the file from intruders and hackers. The privacy of file is maintained to the maximum level. The secure transmission is established with the help of Blow fish algorithm. It doesn't based on past interactions and also do not try to learn global trust information In this experiments good peers are able to form trust relationship in their proximity and isolate malicious peers.**

***Keywords: security, trustworthy, service, recommendation and recentness*.**

I.INTRODUCTION

PEER-TO-PEER (P2P) systems rely on group effort of peers to accomplish tasks. Ease of performing malicious activity is a risk for security of P2P systems. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. However, establishing trust in an unknown entity is difficult in such a malicious environment. Furthermore, trust is a social concept and hard to measure with numerical values. Metrics are needed to represent trust in computational models. Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases. Metrics should have precision so peers can be ranked according to trustworthiness. Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trustworthiness a challenge.

A central server is a preferred way to store and manage trust information, e.g., eBay. The central server securely stores trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other [13], [9].Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT)-based approaches, each peer becomes a trust holder by storing feedbacks about other peers [13], [14], [18]. Global trust information stored by trust holders can be accessed through DHT efficiently. In unstructured networks, each peer stores trust information about peers in its neighborhood or peers interacted in the past [9], [15], [16]. A peer sends trust queries to learn trust information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers.

In this paper we introduce an Secure file structure based on sender and receiver that aims to decrease cruel doings in a P2P system by establishing faith relations among peers in their proximity. No a priori information or a trusted peer is used to pull faith organization. Peers do not try to collect trust information from all peers. Each peer develops its own security feature based on this technology. In this way, good peers form lively faith groups in their nearness and can isolate malicious peers. It completely blocks the performance of man-in-the-middle attack by the hacker's personal computer. The reputable receiver peers IP address is already known to the transmitter to make good transmission of files between authorized transmitter and receiver.

It doesn't depend on other peer's feedback to increase the trustworthiness of peers to establish hopeful communication.

The remainder of this paper is organized as follows. in section II summarize the implementation of this experiment, Section III discuss the relatedwork,section IV explain the system model, section V for attacker model and section 6 presents the conclusion of the process

II.RELATED WORK

Ahmet Burek Can [1] defines a distributed algorithm to create a separate trust network for each peer based on local available information and do not try to get feedback from global network. It allows trustworthiness among peers based on past exchanges. A distributed hash table used with each peer to become a trust holder by storing feedback about other peers [14], [15], [19].In SORT, peers are assumed as stranger to each other at beginning. A peer becomes an acquaintance of another peer after providing service (or) Uploading a file. A. Seluk [2] uses a protocol to establish trust among good peer as well as for identifying malicious one. This protocol creates a network based on some reliable reputation based system. The reputation systems are grouped together as authentic. The malicious peers are detected by some simulations such as naïve, hypocritical, collaborative and pseudo spoofing. Each peer has its hash value to improve confidentiality. A

different method introduced by S.Kamvar [19], this method develop an Eigen trust algorithm to reduce the number of downloads of inauthentic files in peer to peer file sharing network. It assigns a unique global value for each peer based on peer's history of upload. This global trust value to choose the peers, from whom they download, the network effectively identifies malicious peers and isolates them from the network. A new technique for trust management of peer to peer system proposed by K.Aberer [14] that provides solution to frequently encounter unknown agents in peer to peer system. Scalable data structure and algorithm construct a routing table to allow access trust by agent's reputation from its past interaction with other agent and it allow full edges peer to peer architecture.

A measurement study of peer to peer file sharing system proposed by S.Saroiu[20],it provide a detailed measurement study seeks to precisely characterize the population of end user host that participate in peer to peer system. It chooses the peers based on characteristics of peer to peer system. The characteristics such as bandwidth, latency, availability and degree of file sharing. In [21],The internet content delivery system are proposed based on isolating and characterize the traffic belonging to delivery classes such as increasing importance of internet content delivery system characterize the behaviour of these system and derive implications for caching in these systems. Li.Xiong[15] about a system for e-commerce communities. It is a transaction based feedback system. It receives the feedback from other peer and compares its trustworthiness and also calculates the total number of transaction peer performs.

R.Zhou [17] introduces the model with scalable, accurate, robust and fault tolerant architecture by computing global reputation score for the particular network. And also each system store feedback about all nodes in the network. M.Ripeanu[16] says about mapping gnutella Network, it create a virtual network with its own routing mechanism. It built a crawler to extract the topology. It operates based on analyzing the topology graph and evaluated generated network traffic.

Jon Kleinberg[10] create a small world phenomenon to allow peoples communicate with each other over short chains of acquaintances. It is an algorithm perspective. It is not a decentralised algorithm, operates only with local information. J.Douceur[11], it isolate faulty remote computing elements. The Sybil attack is based on trusted agency certify identities and co-ordination among entities. This approach have some conditions such as all entities operates over nearly identical recourse constraints and all presented identities are validated simultaneously all entities coordinated across the system.

III.IMPLEMENTATION

A. Existing development

Trust models on P2P systems have extra challenges comparing to e-commerce platforms. Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority.

The implementation of our system overcome lack of issues arises on the existing techniques to communication between peers through malicious node.Fig.1 shows the existing process with its difficulties

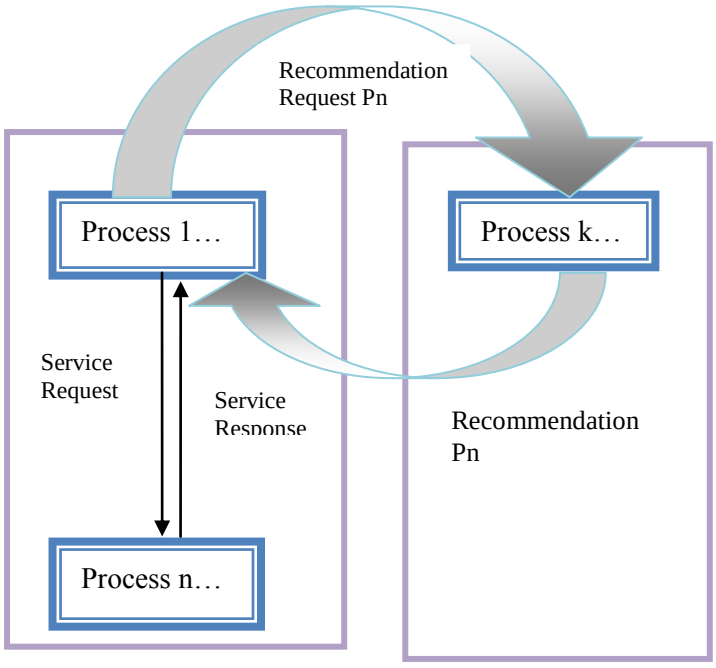
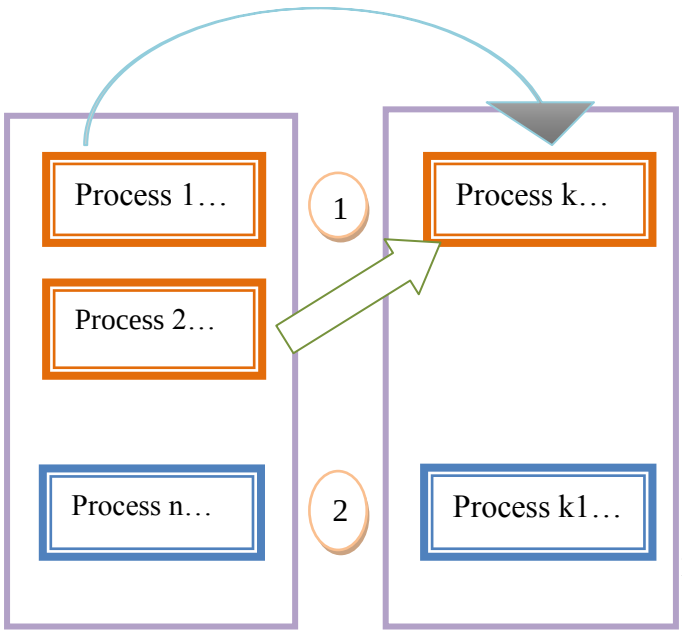


Fig 1: Existing techniques

That p1 wants to get a particular service. pN is a stranger to p1. To learn p1's reputation, p1 requests recommendations from its acquaintances. Assume that pk sends back a recommendation to p1. After collecting all recommendations, p1 evaluates pk's recommendation, stores results. Assuming pN is trustworthy enough, p1 gets the service from pN. Then, p1 evaluates this interaction and stores the results

B. Proposed technique

The following comparison defines the operation involved on implementation of secure transmission of file over the network using proposed blow fish algorithm. This algorithm helps to encrypted transaction of file to receiver. The proposed system compared with existing system in Fig.2,that define how the proposed system avoid collisions compared with the existing system when get recommendations from its neighbors of the Network.



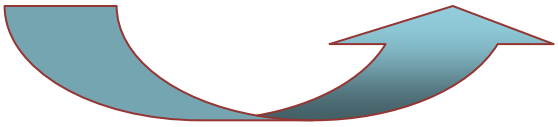


Fig 2: Proposed system

1 Problem occurring while communication

2 In order to avoid the collision make over the server

Process communicate with authorized one without Collision. Don't get any recommendations from its Acquaintances or global knowledge from other peer's Network. The implementation of our secure transmission system implemented with the help of Blow fish Algorithm

C .Algorithm Explanation

- Blowfish is a symmetric encryption algorithm designed in 1993 by Bruce Schneider as an alternative to existing encryption algorithms such as DES.
- Unlike DES, however, the Blowfish algorithm has a variable key length, which can be extended from 32 bits to 448 bits, making this a more secure alternative.
- Blowfish is a 64-bit cipher (i.e. a cryptographic key and algorithm are applied to a block of data rather than single bits.
- Manipulates data in large block. Has a 64-bit block size. It a scalable key, from 32 bits to at least 256 bits.
- Uses simple operations that are efficient on microprocessors.
- It does not use variable-length shifts or bit-wise permutations, or conditional jumps.
- Blowfish is a variable-length key, 64-bit block cipher.
- The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several sub key arrays totalling 4168 bytes.
- Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key- and data-dependent substitution.
- All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

IV.SYSTEM MODEL

The peer to peer network operates in a distributed manner. That is the computer programming and the data to be worked on are spread out over more than one computer. The process implemented on the peer to peer network based on IP address. Its process is described using a separate node called sender and a particular node consider as a receiver within the network. The sender performs the secured data transfer to receiver in following manner of step by step process execution.

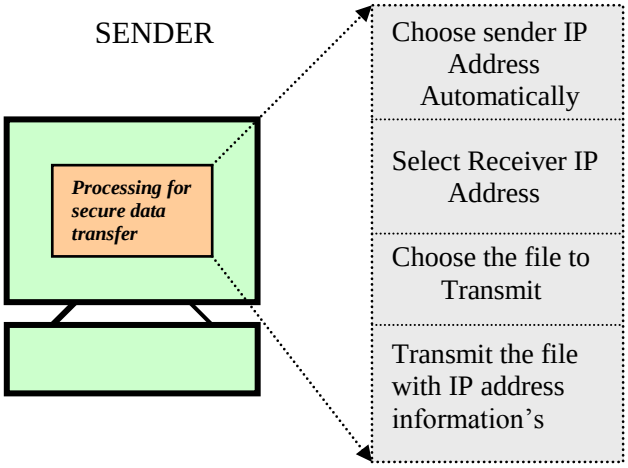


Fig 3: Process on sender

The sender sends the file in encrypted manner with sender and receiver IP address. The IP address are selected on the sender side before choose the file which is to be transmitted to the receiver. After collecting all information from sender the file is ready to transmit then the file is transmitted over the network using traditional transmission medium.

The receiver performs the operation in following manner like sender. The receiver also performed without decentralized algorithm and it only refer the available local information such as IP address .Only the authorized receiver can open the file. Even an acquaintance in the proximity other then sender and receiver cannot open it while try to trace the file during transmission.

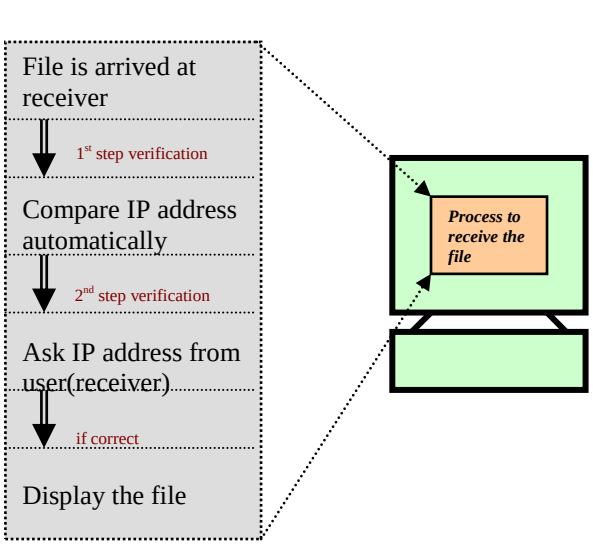


Fig 4: Process on Receiver side

At the receiver side the encrypted file from the sender is Arrived and it automatically compare the receiver IP address with the receiver IP address entered by the sender. If it is correct then again ask the IP address from user

(receiver).Compare the IP address entered by the user with system IP address. After the success of verifications the file is decrypted and displayed to the receiver. The file is not opened by user when the IP address is mismatch.

V. ATTACKER MODEL

This model deals with the intruder identification. If an intruder enters the network group the intruder is identified and the location of the intruder is displayed to the receiver side. This is any entity that is allowed by a data server to provide content service in response to request by clients. Intermediaries include caching proxies and transforming proxies. They check for the IP address and the packet security by providing content providing.

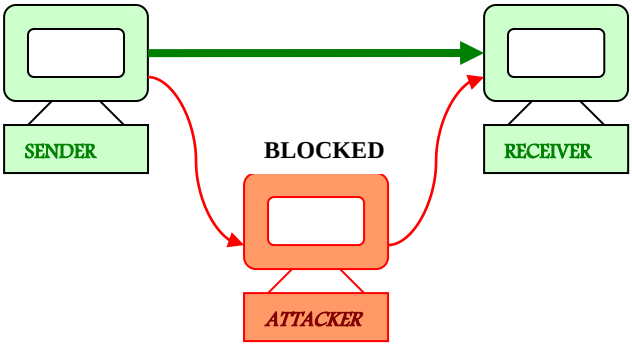


Fig 5: Attacker model

Attack detection:

In the attack detection instead of relying on cryptographic-based approaches.Furthermore,our work is novel because none of the existing work can determine the number of attackers when there are number of adversaries masquerading as the same identity. Additionally our approach can accurately localize multiple adversaries varying their transmission power to trick the system of their true locations.

VI CONCLUSION

A conviction model for P2P networks is presented, in which a peer can develop a faith network in its nearness. It can enhance security and effectiveness of systems. A peer can isolate malicious peers around itself as it develops faith relationships with good peers.. It completely rescue the file transmission from man in the middle attack. This method offers some difficulties like this secure shell transmission technology is maintaining trust all over the network. If a peer system which wants to receive the file is repaired then the problem occurred to receive the file. If interactions are modelled correctly, It can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and P2P gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

REFERENCES

[1] Ahmet Burek Can *et al* (2013), SORT: A Self-Organizing Trust model for peer-to- peer System

[2] A.A.Seluk, E.Uzun, and M.R.Pariente,"A Reputation – Based Trust Management System for P2P Networks,"Proc.IEEE/ACM Forth Int'l Symp.Cluster Computing and the Grid (CCGRID).2004.

[3] A. Barab´asi and R. Albert, "Emergence of Scaling in random networks," Science **286**, pp. 509–512, 1999.

[4] B. Holmstrom, "Managerial Incentive Problems: A Dynamic Perspective," Rev. Economic Studies, vol.66, no.1, 1999.

[5] B.A. Huberman and F. Wu, the Dynamics of Reputation. 2002.

[6] C. Dellarocas, "The Digitization of Word-of-Mouth: Promise and Challenges of Online Reputation Mechanism," Management Science, vol. 49, no. 10, 2003.

[7] D. Roselli, J. Lorch, and T. Anderson, "A comparison of file system workloads," in Proceedings of the 2000 USENIX Annual Technical Conference, (San Diego, CA, USA), June 2000.

[8] E. Friedman and P. Resnick, "The Social Cost of Cheap Pseudonyms,"J. Economics and Management Strategy, vol. 10, no. 1, 2001.

[9] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002.

[10] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp.Theory of computing, 2000.

[11] J. Douceur, "The Sybil Attack," Proc. 1st Int'l Workshop Peer-to-Peer Systems (IPTPS), 2002.

[12] J.Kangasharju, K.W, Ross and J.W.Roberts. Performance evaluation of redirection schemes in content distribution networks. Computer communications, 24(2):207–214, 2001.

[13] J. M. Kleinberg, R. Kumar, P. Raghavan, S. Rajagopalan, and A. S. Tomkins. The Web as a graph: Measurements, models, and methods. In T. Asano, H. Imai, D. T. Lee, S. Nakano, and T. Tokuyama, editors, Proc. of the 5th Annual Int. Conf. Computing and Combinatorics, number 1627.Springer-Verlag, 1999.

[14] K.Aberer and Z.Despotovic,"Mnaging Trust in a Peer-to-Peer information system," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM), 2001.

[15] L. Xiong and L. Liu, "Peer trust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, July 2004.

[16] M. Ripeanu, I. Foster, and A. Iamnitchi, "Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design," IEEE Internet Computing, vol. 6, no. 1, pp. 50-57, Jan. 2002.

[17] R. Zhou, K. Hwang, and M. Cai, "Gossip trust for Fast Reputation Aggregation in Peer-to-Peer Networks," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

[18] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, "Resilience of the internet to random breakdowns, "Physical Review Letters **85**, November 2000.

[19] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigen trust) Algorithm for Reputation Management in P2P Networks," Proc. 12th World Wide Web Conf. (WWW), 2003.

[20] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002.

[21] S. Saroiu, K. Gummadi, R. Dunn, S.D. Gribble, and H.M. Levy, "An Analysis of Internet Content Delivery Systems," Proc. Fifth USENIX Symp. Operating Systems Design and Implementation (OSDI), 2002.

AUTHORS PROFILE

R.Gayathri Received her B.E degree in computer science and Engineering from sudharsan Engineering College, Anna university,Chennai,India,in 2012.Currently pursuing M.E in computer and communication from MNSK College of Engineering,Anna University Chennai,India.Her research includes routing and network security

Vaishnavi.V is an Assistant Professor of Electronics and Communication Engineering in MNSK college of Engineering Pudukkottai. She received her B.E. degree in electronics and communication engineering from Shanmuganathan engineering college, Anna University Trichy, India, in 2011. She has received her M.E**.** in Computer and Communication from Sethu Institute of Technology, Anna University Chennai India in 2013 .Her research interests include Routing and Wireless Network Communication and she has published 1 paper in international journal.