Securing Information in Peer-to-Peer Environment

Velvizhi N
Department of Computer Applications
RMD Engineering College
Chennai, India

D. Manjula
Department of CSE
Anna University
Chennai, India

ABSTRACT
As an emerging model of communication and computation, Peer-to-Peer(P2P) networking has recently gained significant acceptance in today's internet computing, Suffers from the problem of securing information while transferring from one peer to other peer. In existing direct path was established between source and destination peer to secure the data. We analyzed the problem of security and constructing direct path between source and destination peer which led p2p systems might compromise user privacy. To overcome the above issue we proposed an algorithm to find out the optimal path among the existing paths, through which the information can be sent and received. To enhance the system performance by implementing security measures we compared two asymmetric cryptographic algorithm with our application model(ICRQR),which is decentralized and unstructured and proved that p2p reputation model is more secured and hence increases the system performance.

Keywords:- Unstructured peer to peer, Decentralized, privacy, asymmetric key, cryptographic, reputation.

1. INTRODUCTION
PEER-TO-PEER(P2P) networks are self-configuring networks with no central control. P2P network increases system robustness by enabling receiver to obtain data from multiple sources without relying on centralized servers. The peer-to-peer(P2P) model such as Gnutella,KazaA and BitTorrent,aims at utilizing and managing increasingly large and globally distributed information and computing resources [6]. Information security applies to all aspects of safeguarding (or) protecting information or data. It is necessary to protect the information systems against unauthorized access or modification such as deletion or addition of some part into the information in transit. It is also necessary to protect the information system against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats[7].Preventing peers from returning corrupt responses to queries and routing through malicious peers, is an important security issue in P2P networks. To enhance the integrity of routing, it is important to reduce the number of queries forwarded to malicious nodes. In existing P2P systems are in secured and attacks on the routing of queries. To address the limitations of existing works and meet the Requirements we built a decentralized unstructured P2P system supporting the following constraints.

1. Distributed Database: User locations are indexed in a table distributed among peers.
2. Availability: Users are unique, attacks targeting single users may be addressed both to the distributed index and to the user's device directly.
3. Integrity: Attackers may want to impersonate different users in order to handle calls directed to them; constitute a particular threat for the user as, in ease of success, the attacker acquires full control on the victims personal communications.
4 Confidentiality: Communications are usually meant to be private and need to be encrypted, evesdropping may reveal sensitive data and is a serious threat for users.

P2P networks are highly dynamic, with peers frequently joining and leaving. We simulate the joining and leaving behavior of peers by turning on and off logical peers, respectively.

1.1 Problem Statement
We consider the examples of "n" peers which are connected through common network and want to communicate each other. Note that an attacker does not have to be located close to the peer which is already existing, but during transmission of message, attacks on networks happened for a variety of reasons such as monetary gain, personal enemity or even for fame in the hacker community. In this work our goal is to find out the destination node by using ICRQR and routing the queries in secured way by applying reputation model cryptographic algorithm[11]. Also it finds the trust worthy peer by computing Number of satisfactory transactions in account.

2. RELATED WORK
P2P networks can be categorized into structured and unstructured P2P networks. The proposed system can be used on the unstructured P2P networks. The unstructured P2P networks do not have well-known architecture. In unstructured networks, there is no relationship between the data or metadata and its location. As a result search is of the order of O (N) in these networks, where N is the number of nodes(Each node will receive a query message at least once)

Many trust models and a recommendation protocol focusing on decentralized systems. There are more trust models, which are identity based, which means that for one peer to trust another, it needs to know the identity of the other peer [6]. Generally, most P2P trust designs are identity based, where one peer does not trust another before knowing its identity. Several solutions achieve mutual anonymity for both initiators and responders in P2P systems, which generally aim at concealing the real identities of users during transaction. ID based cryptography (IBC) allow the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for public key verification in the conventional public key infrastructure [13].Blind signatures scheme allows a receiver to obtain a signature on a message Such that both the message and resulting signature remain unknown to the signer [2].

In Collaborative network security platform the bootstrap server is initialized first when system is starting. It maintains the authorities of joining nodes, the list of p2p hub nodes and keys for secure information exchange [8]. ICP (Internet content provider) tries all the methods of enhancing security schemes to protect the content they deliver from one peer to other, they unfairly ignore its impact in degrading user experience. The QoS (Quality of service) –Qop (Quality of protection) collaborated scheme aims to provide highest service security to end users in the best – effort internet[5]. Co operative signature authentic ation scheme called collaboration signature trust (CST) for clustered p2p systems, where each peer, instead of using its real identity, owns and un-forgeable and verifiable identity signature. The identity signature is signed by a trusted peer through a collaboration signature method [15].

In fine-grained reputation system, reputation scores submitted to the central server are encrypted and can only be decrypted by it. Even if the DHT is used, no user can learn the content of the encrypted reputation scores he saves. In addition the central server only returns to the querying user an aggregated reputation score instead of collected raw reputation scores. Therefore, it is impossible for any server to know the reputation score a particular client gives for him, and clients can be assured of offering honest reputation scores without incurring retaliation [14].The SAT (A security architecture achieving Anonymity and Traceability) strives to resolve the conflicts between the anonymity and traceability. Adoption of the hierarchical identity based cryptography (HIBC) for interdomain authentication avoiding domain parameter certification [12].

Preventing peers form returning corrupt responses to queries and routing through malicious peers, is an important security issue in p2p networks[10].In reputation based system the central server mainly comprises an account manager in charge of registering users and crediting / debiting user accounts, a query processor dealing with reputation queries from system users[9].The shard password technique is used to secure data which is not efficient[3]. In Dos (Denial of Service) attacker model, the possibilities to compute optimal attacks in polynomial time are strictly limited [4].

2.1 RSA Blinding Algorithm

In cryptography, blinding is a technique by which an agent can provide a service to (i.e, compute a function for) a client in an encoded form without knowing either the real input or the real output. Blinding techniques also have applications to preventing side-channel attacks on encryption devices. Authentication systems are implemented based on an asymmetric cryptographic algorithm, such as RSA. There are two application models in the Public Key Infrastructure (PKI).The most widely accepted method is RSA blinding. With RSA blinding, randomness is introduced into the RSA computations to make timing information unusable. Before decrypting the cipher text C, We first compute $X=r^e c \bmod N$, where r is a random value and e is the public exponent. We decrypt X as usual i.e. compute $x^d \bmod N=r^{ed} c^d \bmod N =rc^d \bmod N$ by Eluer's Theorem. We then multiply the output by r^{-1} to obtain $c^d \bmod N$ which is the plaintext we want. Since a different r is used for each message, the original message is changed in a random way before the exponentiation operation. Thus, blinding prevents an attacker from entering a known input to the exponentiation function and using the resulting timing information to reveal the key.
The original Schindler's attack was based on a simple idea: if the value u1Rmod p is small the probability of ER is small, thus not many would be realized during the exponentiation. On the other hand, if value u2Rmod p is (relatively) high, many reductions would take place and the whole process would take much longer. Thus, it was sufficient to find two messages with significantly different times taken to generate their signatures. In such case a multiple of p had to lie between u1R and u2R. Having a look at the time it takes to generate the signature of (u1+u2)R/
2 the attacker can decide which half of the interval to look at. To defend agains this simple timing attack RSA blinding can be employed. Ideally, with each signing operation a random value r 2 ZN is chosen. Instead of computing md modN, we compute (mr)d modN and multiply the result by rd modN at the end. By doing so, the attacker can no longer choose the messages being input to Montgomery multiplication algorithm.

2.2 P2P Reputation Model

A dynamic one, where the topology changes along the time, with nodes joining and leaving the network. This scenario could be used in order to test the reaction of a trust and reputation model against changes in the size and topology of the network, and the specific nodes composing it. For instance, it could be checked the reaction of the model if a very reputable (or, equally, a very fraudulent) node enters or leaves the system. Trust and reputation management has arisen as one of the most innovative and accurate solutions to most of these threats. By using a trust and reputation system a peer who wants to interact with another peer in the community has more information and, therefore, more opportunities to select the right partner to have a transaction with, rather than with a fraudulent one.

Once a peer has obtained its identity, it joins the P2P network using the standard Join method of the particular P2P network. The proposed reputation model is independent of the topology of the P2P network, addressing schemes for its nodes, bootstrap mechanisms, joining and leaving protocols of peers, and the name service. In other words, the choice of any of these components has no impact on the reputation model and vice versa.[17]

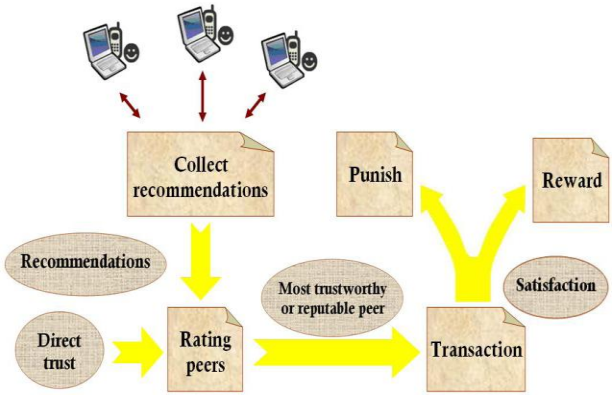

Fig.1 Reputation Model

We have seen that the main target followed by every trust and reputation model is, in summary, to identify those peers who are most reliable supplying a certain service or more trustworthy carrying out a certain task. How those peers are selected differs from one model to other but, for instance, in most of them we can observe more or less the same generic steps, as depicted in figure 1. First of all an entity checks its previous experiences with a given peer in order to form what is usually called direct trust. This direct trust can be assessed using complex expressions which usually take into account the number of previous transactions, the importance given to each transaction, the satisfaction obtained in each one, the time when it was performed, etc. Or it could even be computed as the difference between the number of satisfactory transactions and unsatisfactory ones, like in Eigentrust. Additionally the indirect experiences (or experiences of other peers) are taken into account as well, obtaining what is commonly known as the reputation of a peer. At this point, some models (like [18, 19, 20]) even distinguish between the trust given to a peer as a service provider, and as a recommender, filtering out this way State of the Art in Trust and Reputation Models in P2P networks .How this reputation value is obtained is also very specific for each model, but the main idea is to collect information about the behavior of the target peer from other peers who have had previous interactions with it. This information or recommendations are influenced in some models by the reliability of the recommender, as we mentioned. Otherwise, a collusion could be established where a set of malicious peers rated each other with the maximum value. Therefore, an aggregation between the direct trust or direct experiences and the reputation or indirect experiences, weighted by the reliability of each recommender is performed in order to obtain a unique global trust value for a certain peer. Most of the models do not specify which peer is finally selected. It could be just the one with highest score, but not necessarily.

Once the peer to interact with has been selected, the transaction is effectively carried out. Then, the user who applied for a service or a task assesses her satisfaction with the received service or performed task. According to this satisfaction, a last step of punishing or rewarding the entity the transaction was done with, is performed. However, not many models apply a specific and independent step of punish and reward, but they rather implicitly incorporate it in the rating step. Legitimate global reputation information with respect to a given provider is available to all peers at one place

2.3 Reputation model steps

- The provider is accountable for all its past transactions
- As the global information of the provider is stored by the provider itself, this protocol is not affected by erratic availability of past recommenders or any other peer in the network.
- The requester cannot (gainfully) maliciously abort the transaction in the middle.
- This protocol cannot stop a requester from giving a "bad" recommendation to the provider even if the latter provides a legitimate file.

Advantages

- The primary advantage of public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone.
- Another major advantage of public-key systems is that they can provide digital signatures that cannot be repudiated.
- Public-key cryptography is best suited for an open multi-user environment.

3. PROPOSED ALGORITHM (OPTIMAL PATH ALGORITHM)

This algorithm finds the all possible paths from source to destination peer, and hence finds the optimal path. Unlike the above mentioned algorithms, this algorithm computes the waiting time and query processing time. The complexity of this algorithm is $O(n^2)$[16].

1. Initialize TTL = 0
2. Get the Adjacency Matrix [A] for the Network and copy it to path [][].
3. Get all possible path based on matrix A
4. **Procedure** Optimal Path ()
   For k: = 1 **to** no of vertices
   For I := 1 **to** no of vertices
   For j: = 1 **to** no of vertices

Path[i][j] = minimum (path[i][j],
path[i][k]+path[k][j]);

Where i,j are the source and the destination ,k is the intermediate node and path[i][j] stores the shortest path.

5. Get the system time at the time of sending the query
6. Calculate the Actual Time.
7.Processingtime=A[source,destination]+A [destination,source] (Time to send the request and receiving acknowledgment)

8 Waiting time WT(n)=Waitingtime(n-1)+processing time](n-1)(in general)
9. Response time(n) = Processing time(n)+ waiting time(n)

10. Calculate Average Waiting Time(AWT) = $\frac{\sum_{i=1}^{n} WTi}{n}$

11. Average Response time(RT) for "n" number of queries

$$= \frac{\sum_{i=1}^{n} RTi}{n}$$

Where i = 1,2,3…n.

12. In case of not receiving the response apply

```
If (Waiting Time == Systemtime)
   If(Response Received)
     If(flag==1)then
          Success(process completed)
      Exit
          End if
Else Resend the queries
          End if
    End if
```

The above algorithm finds the optimal path for any given network. From the resulting path we can communicate information to other peers which are connected in the network. When we are communicating the information to other peers it is necessary to protect the information against unauthorized access or modification such as deletion or addition of some part into the information in transit. It is also necessary to protect the information system against the denial of service to authorized users. To overcome the above issue we compared two asymmetric cryptographic algorithm namely RSA blinding algorithm and P2P reputation model with our application ICRQR [16].

4. RESULT AND DISCUSSION

Table 1 shows the comparison of unauthorized access during the query processing in P2P environment. At the regular interval the set of queries ranges from 50 to 250 were sent through our application (ICRQR) and applied both the cryptographic algorithm namely RSA blinding and Reputation model and arrived with the following data.

Table1: Comparison of average number of malicious attacks (RSA blinding AND P2P Reputation model.)

S.No :	No.of Queries (in 10's)	average number of malicious attacks (RSA blinding in %)	average number of malicious attacks (P2P Reputation model in %)
1	5	1.75	0.73
2	10	1.96	0.92
3	15	2.07	1.20
4	20	2.15	1.42
5	25	2.22	1.58

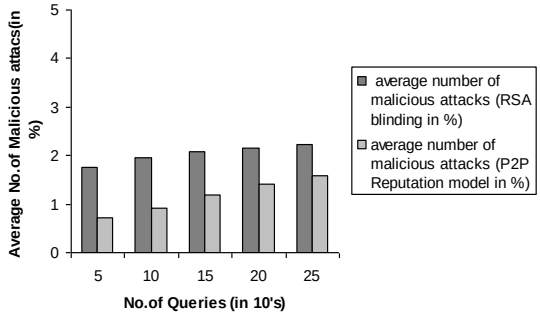

Fig.2. Comparison on No.of Malicious attacks.

Figure.2 shows the comparative results of RSA Blinding cryptographic and Reputation Model , where x-axis indicates the number of queries (in 10's) and y-axis represents average number of malicious attacks(in percentage).The graph shows that the average number of malicious attacks of reputation model cryptographic is about 50 percent less compared to RSA Blinding cryptographic algorithm. In the figure, we can see that the number of messages destroyed in RSA Blinding is higher, so its overall performance in dynamic environments is not as good as Reputation model. Overall, Reputation model outperforms RSA Blinding cryptographic algorithm.

5. CONCLUSION AND FUTURE WORK

We have illustrated our approach on two application scenarios namely RSA Blinding and Reputation Model in the area of Peer-To-Peer networks, Networks with decentralized and unstructured. This cryptographic reputation model that facilitates generation of global reputation data in a P2P network, in order to expedite detection of malicious attacks. The global reputation data are protected against any malicious modification by the third party peer and are immune to any malicious modifications by their owner. The Reputation model protocol reduces the number of malicious transactions. It also handles the problem of highly erratic availability pattern of the peers in P2P networks. In future we planned

to device an Message Security Algorithm (MSA) which will prevent all information and data from other causes.

6. REFERENCES

[1] Dhruv Chopra, Henning Schulzrinne, Enricomarocco, ”Peer-to-peer overlays for real time communication: Security issues and solutions”, IEEE Comm.Surveys and tutorials,Vol.11,No.1 2009.

[2] Jinyvan Su n, Chi Zhang, Yanchao Zhang, Yuguang Fang,”SAT:A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks” IEEE Trans.on dependable and secure computing vol8.No.2,March2011.

[3] Srdjan capkun, Jean-pierre hubaux, Levente Buttyan “ Mobility Helps peer – to – peer security “ IEEE Trans. On Mobile computing Vol 5, No1. Jan 2006

[4] Sascha Grau, Mathias Fischer, “On complexity and approximability of optimal Dos attacks on multiple – Tree p2p streaming Topologies “IEEE trans on dependable and secure computing, Vol.8, No.2 March 2011.

[5] Z.Chen, H.yin,C.Lin, Y.chen, M.Feng “Towards a universal friendly peer – to peer media streaming metrics, analysis and explorations” ,IET Comm. April 2009.

[6] Li Lu, Jinsong Han, Yunhao Liu, Lei Hu, “Pseudo Trust : Zero – knowledge authentication in anonymous p2p” , IEEE Trans on parallel and distributed Systems. Vol. 19, No.10, OCT 2008.

[7] Srdjan Capkun, Mario Cagalj, Ghassan O Kalame, “Integrity Regions: Authentication through presence in wireless networks” , IEEE Trans on mobile computing, Vol 9,No11. Nov 2010.

[8] Chun–Hsin, Chun-Wei Huang “A Collaborative network security plat form in p2p networks” Intel. Conf on new trends n infn and service science 2009.

[9] Yanchao zhang, Yuguang fang, “ A Fine grained reputation system for reliable service selection in peer-to – peer network’s” , IEEE Trans on parallel and distributed systems Vol 18, No.8, Aug 2007.

[10] Yunhao Liu,Li Xiao,Lionel M Ni,”Building a scalable Bipartite P2p overlay Network”IEEE Trans.on parallel and distributed systems,vol.18,No.9,Sep 2007.

[11] Prashant Dewan and Partha Dasgupta “p2p reputation management using distributed identities and decentralized recommendation chains”IEEE Trans. On Knowledge and Data Engg.Vol22,No.7,July2010.

[12] M.Brinkmeier, G.Schaefer,and T.Strufe, “Optimally Dos resistant P2P technologies for live multimedia streaming, “IEEE Trans. Parallel and Distributed systems”,Volume 20 , No.6, June 2009.

[13] Y.Zhang.W.Lio,W Lou and Y.Fang” Securing mobile Adhoc networks with certficateless public keys”, IEEE Trans. Dependable and secure computing Volume 3 , No.4, October 2006.

[14] R.H.Wouhaybi and A T Campbell, “ Building Resilient Low – Diameter Peer-to- Peer Topologies”, Computer networks, Volume 52 , No.5, 2008

[15] Xiaoliang wang, Xingming Sun, Guang Sun, “CST: P2P Anonymous authentication system based on collaboration signature” IEEE con.2010.

[16] Velvizhi N,D Manjula “ICRQR: Improving Computation Power by Reducing Query Response Time in P2P Environment”Journal of computer science,Vol.7,No.3,2011.

[17] R. Chen, X. Chao, L. Tang, J. Hu, Z. Chen, CuboidTrust: A Global Reputation-Based Trust Model in Peer-to-Peer Networks, in: Autonomic and Trusted Computing, No. 4610 in LNCS,4th International Conference, ATC 2007, Springer, Hong Kong, China, 2007, pp. 203–215.

[18] F. Yu, H. Zhang, F. Yan, S. Gao, An improved global trust value computing method in P2P system, in: Autonomic and Trusted Computing, No. 4158 in LNCS, Third International Conference,ATC 2006, Springer, Wuhan, China, 2006, pp. 258–267.

[19] Y. Wang, Y. Tao, P. Yu, F. Xu, J. Lu, A Trust Evolution Model for P2P Networks, in: Autonomic and Trusted Computing, No. 4610 in LNCS, 4th International Conference, ATC 2007,Springer, Hong Kong, China, 2007, pp. 216–225.

[20] Y. Zhang, H. Chen, Z. Wu, A social network-based trust model for the semantic web, in:Autonomic and Trusted Computing, No. 4158 in LNCS, Third International Conference, ATC2006, Springer, Wuhan, China, 2006, pp. 183–192.