CHAPTER 7

SECURING MESSAGES WITH OPTIMAL REPUTATION MODEL

7.1 INTRODUCTION

Peer-to-Peer (P2P) networks offer higher robustness against failure, easier configuration and are generally more economical as compared to their client-server counterparts. A P2P based approach solves the load and cost issues but leads to new challenging security issues for secure communication and data access. The P2P security problem is complicated by the dynamic nature of these networks and the overall lack of a central authority or the infrastructure to enforce security. P2P systems generally require a remarkable amount of trust from their participants. A node must trust that other nodes implement the same protocols and will respect the goals of the system.

In P2P networks users continuously access resources provided by other unknown users which, therefore, can be untrustworthy. All these interactions in which the nodes act both as clients (asking for resources) and servers (Providing resources) can be used to know the degree of confidence that can be put into the nodes with which one has interacted (reputation). This reputation information can be stored and shared using reputation systems. This way, a reputation system could be used to determine which nodes are trustworthy and which are not. Usually, reputation is used in the process of request for resources to decide what the best supplier is. In fact, reputation may be taken into account when making any kind of decision that requires interaction with other nodes.
However, most reputation model needs the central authority to keep track of the transaction information. This is against the idea of the pure P2P network and there is the potential risk of single system failure. Thus, it is proposed to build a reputation-based model called Optimal Reputation Model (ORM) which provides the security by identifying the trustworthy peer in pure decentralized P2P environment. It is the responsibility of ORM to identify the trustworthy peer based on the behaviour of past transactions.

From a survey of the recent approaches to the reputation model, the following observations have been made:

1. Identity based certificates are used to identify the trustworthiness of a peer. The reputation of a given peer is attached to its identity and all peers maintain their own (and hence trusted) certificate authority which issues the identity certificate(s) to the peer.

2. 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.

3. 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.

4. 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.
5. 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.

6. In fine-grained reputation system, reputation scores submitted to the central server are encrypted and can only be decrypted by it.

Due to the anonymity and autonomy characteristics of P2P system, the security issue becomes a hot topic. The characteristics of P2P systems include efficiency and reliability to provide healthier environment, which demand the development of new methods to address these issues. Therefore, a P2P system which provides more security during message transactions in P2P network, could well suit the needs.

This thesis has been motivated to propose the security policy by applying trust factor to control the access permission of transactions among peers in the P2P system. The proposed ORM method is designed to have an effective security policy to help requester locate trustworthy partners and exchange query messages securely with confidence. No central server is maintained during transaction to store the information.

This chapter is organized as follows. Section 7.2 introduces the individual steps of the proposed Optimal Reputation Model in detail. Section 7.3 describes the experimental results obtained for dataset, and compares them to other reputation-based and cryptographic-based models reported in the literature. Section 7.4 summarizes the chapter.
7.2 SECURITY POLICY BASED ON REPUTATION MODEL AND CRYPTOGRAPHIC PROTOCOL

The optimal reputation model (ORM) approach for identifying trustworthy peer and providing secured communication between peers are proposed in this chapter, works across different kinds of P2P overlay network with a unified framework and takes care of dynamic joining of peers and leaving from the overlay connection. Here, the idea is to apply a security policy based evaluation of trust in P2P systems (Cuihua et al 2010) instead of public key cryptographic technique. However, current P2P trust models almost take no consideration for the dynamic characteristic of trust, which results in low efficiency in resisting the act of malicious peers.

This thesis has been motivated by the fact that P2P environments must have an effective security policy to help requester locate trustworthy partners and exchange information securely with confidence. The objective of this thesis is to design a reputation based model, which eliminates the malicious act and thereby controls the access permission of transactions among peers in the network.

7.2.1 P2P security models and analysis

Trust and reputation systems have been extensively investigated in Peer-to-Peer (P2P) communication to distinguish and avoid malicious peers. The traditional mechanisms for generating trust and protecting client-server networks cannot be used for pure P2P networks. This is because the trusted central authority used in the traditional client-server network is absent in P2P networks. In the absence of any trusted central agency, an attacker can gather infinite identities and start issuing recommendations to itself. A peer might
modify the reputation data stored in the network to maliciously raise its own reputation. So, cryptographic mechanisms alone cannot be used to fully solve this problem because internal adversarial peer nodes could also have valid cryptographic keys to access the other nodes of the networks.

In order to cope with malicious behavior, some reputation-based P2P trust models have been proposed.

### 7.2.1.1 P2P Rep model

The basic idea of P2P Rep approach is to allow peer (p), before deciding from where to download the resource, to enquire about the reputation of offers by polling its peers. The approach complements the Gnutella protocol with two phases: polling and vote evaluation. After receiving the responses to its query, peer can select a servant (or a set of servants) based on the quality of the offer and its own past experience. Then, p polls its peers by broadcasting a (Poll) message requesting their opinion about the selected servants. All peers can respond (Poll Reply) to the poll with their opinions about the reputation of each of such servants.

A little complication is introduced by the need to prevent exposure of polling to security violations by malicious peers. In particular, it is a must to ensure authenticity of servants acting as offerers or voters (i.e., preventing impersonation) and the quality of the poll, ensuring the votes and detecting possible dummy votes expressed by servants acting as a clique under the control of a single malicious party. Also, this approach encourages persistence of the servant identities as the only way to maintain history of a servant id across transactions.
7.2.1.2 A Role-based trust model

In this model, interests are represented by attributes, which are used to determine the peer communities in which a particular peer would participate. There are of course privacy and security concerns in using such information, also it divide the interests into two classes – personal and claimed. The full set of attributes for a peer is called personal attributes. However, for privacy and/or security reasons, all these attributes may not be used to determine community membership. A peer may not want to reveal some of her personal attributes because she might not consider them relevant amongst the peers that she knows. Hence, a peer explicitly makes only a subset of these attributes public, which are called claimed attributes.

7.2.1.3 Eigen trust model

This is a reputation-based trust model for P2P file sharing systems. Here, each peer is assigned a unique global reputation value. However, it is not clear whether this approach if feasible for large-scale P2P systems, in which some local reputation values are unreachable for the requesting peers. Also, it assumes that peers are honest and therefore cannot defend some attacks like deceptions and rumors.

The Trust Guard that is a safeguard framework for providing a highly dependable and efficient reputation system is presented (Srivatsa et al 2005). PET proposes a personalized trust model to help the construction of a good cooperation, especially in the context of economic-based solutions for the Resource sharing (Zhengqiang and Weisong 2005). The multi-level reputation system maintains or raises each peer’s reputation level according to its periodic contribution to other peers in the network and can encourage free-
riders to share their resources (Ziyao et al 2007, Mol et al 2008). In addition some systems adopt cryptography to attain security authentication.

7.2.1.4 RSA blinding technique

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 attack 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.

7.2.2 Observations from various security models

From the above discussion, the characteristics of various reputation-based and cryptographic-based models are observed and summarized as follows:-

- P2P Rep Model
  - This produces an incomplete experience to get the trust rating in P2P systems.
  - Do not consider the dynamic characteristic of peer’s behavior and the uncertainty nature of trust.
- A Role-based trust model
• This model considers a P2P system containing self-organizing, overlapping, interest-based communities that can be uncovered using decentralized techniques.

• Eigen trust model

• This only aims at reducing the number of unauthentic files in the network.

• This method has many assumptions.

• RSA blinding technique

• An initiator has to perform asymmetric key based cryptographic encryptions which do not work always.

In this work, it is decided to apply the reputation-based model to identify the trustworthy peers. To achieve this, the past transactions of overlay network and query messages are to be handled in a good manner. One main aspect of identifying trustworthy peer is to control the transactions with malicious peer. To design such system where transactions are done only through trustworthy peers, an appropriate reputation model should be chosen and which can do the following:

• The model is independent of the topology of the network, addressing schemes for its nodes, joining and leaving of peers.

• Can be powerful in representing the trust of a peer.

• Captures all malicious transactions.
• Transactions are categorized as satisfied transactions (ST) and unsatisfied transactions (UST).

Here, the proposed method is to apply the reputation based trust model, so that peers can quantify and compare the trustworthiness of other peers and perform transactions based on their past transaction histories. The transaction details present in the history table are analyzed to detect the transaction category such as satisfied or unsatisfied transactions. The proposed system is designed to identify the trustworthiness of a peer so as to implement security policy and also considers the contribution of peers to control the access permissions in P2P systems.

The major contributions of the Optimal Reputation Model (ORM) system are as follows:

• It works across different kinds of P2P overlay network.

• It works independently with unstructured P2P systems by applying event driven approach.

• This system works without any trusted central agency.

• The reputation data are protected against any malicious modification.

7.3 SYSTEM DESCRIPTION: OPTIMAL REPUTATION MODEL (ORM)

In P2P networks users continuously access resources provided by other unknown users which, therefore, can be untrustworthy. All these interactions in which the nodes act both as clients (asking for resources) and servers (Providing resources) can be used to know the degree of confidence
that can be put into the nodes with which one has interacted (reputation). This reputation information can be stored and shared using reputation systems. This way, a reputation system could be used to determine which nodes are trustworthy and which are not.

The proposed ORM consists of the following processes as shown in Figure 7.1 namely, Identification of requester and responder, Identifying trustworthy peer and Computation of trust value.

![Figure 7.1 Block diagram of the transaction procedure](image-url)
7.3.1 Identification of requester and responder

The main objective of identifying the requester and responder is to identify the optimal path, through which transactions are done. Suitable path is identified to avoid the unnecessary traffic during interaction between peers. Here, when a peer needs a data, it initiates a request for the data in the network by forwarding query message using flooding technique. If a peer who has the data receives the request, it responds the requester by respond message. The requester may also receive respond messages from different responders. Based on the response time of different responders, the requester will make its choice. If the amount of response time is minimum among all responders then that peer is identified as responder peer.

7.3.2 Identification of Trustworthy peers

P2P systems require a remarkable amount of trust from their participants. A node must trust that other nodes implement the same protocols and will respect the goals of the system. Trust is an accumulative value for the past behavior and reflects the overall evaluation on the valued peer. The following are the steps involved in identifying trustworthy peer in a P2P overlay network.

- The provider is accountable for all its past transactions.
- Let “n” be the number of peers connected in the network.
- At initially request for data by flooding query messages from requester.
- Query message gets hit with one or different responders.
• Based on the response time (with minimum) identify the responder.

• Peer i request a data from peer j, it may rate the transaction as $T_{ij} = 1$ (or) $T_{ij} = -1$.

• If the data is authentic then 1 is stored against the satisfied transaction, and if not authentic (or) interrupted -1 is stored against the unsatisfied transaction.

• Every peer maintains its past transactions say local trust value $S_{ij}$ as the sum of ratings of the individual transactions that a peer I has respond from j: $S_{ij} = \sum T_{ij}$.

• By keeping track of transactions from source peer to destination peer and store it in data base.

• Based on the transactions label it as satisfied transactions (ST) or unsatisfied transactions (UST)

• From the set of total transactions find the trustworthy peer.

• Peer trusting(trust worthy peer) = Number of satisfactory transactions (NST) – Number of Unsatisfactory transactions (NUST).

   In a Peer-to-Peer environment if NST is greater than NUST then that peer can be labeled as trust worthy peer. Trust worthy peers always produces satisfactory transactions.
7.3.3 Computation of Trust Value

Definition 1: Define $T_{ij}(n)$ as the trustworthy of peer $j$ in the view of peer $i$ for the $n$-th direct transaction. The value of $T_{ij}(n)$ can be gained according to the satisfaction level of peer $i$ to the $n$-th service from peer $j$.

Definition 2: Define $W_{ij}(n)$ as the adaptive transaction importance in the $n$-th transaction between peer $i$ and peer $j$. The bigger the value of $W_{ij}(n)$ is the more important transaction.

Definition 3: The symbol $T_{ij}$ expresses the total trustworthiness of peer $j$ in the view of peer $i$ based on its direct interactions with peer $j$.

$$T_{ij} = \frac{\sum T_{ij}(n) \cdot W_{ij}(n) \cdot (1-\mu)(M-n)}{\sum W_{ij}(n) \cdot (1-\mu)(M-n)} \quad (7.1)$$

Where, $\mu$ is time delay and it determines the weight given to the most recent past observations. $M$ denotes the total number of direct interactions between $i$ and $j$.

Definition 4: The transaction successful ratio (TSR) is defined as

$$TSR = \frac{\text{Number of satisfied transactions (NST)}}{\text{Total number of transactions (TST)}} \quad (7.2)$$
7.4 RESULTS AND PERFORMANCE ANALYSIS

7.4.1 Comparison with Other Reputation models

In this section, the results of the proposed ORM method are presented. Test sets are selected to cover a wide variety of transactions in an unstructured P2P environment. The performance of the proposed method is compared with well-known Reputation models, including Pseudo Trust (2008) for zero knowledge authentications, P2P Reputation management (2010) for using distributed identities to apply security policy and also compared with Cryptographic technique called RSA blinding. From the experiments it was observed, that the P2P reputation management model perform well as long as the network is in static environment and they failed to identify the trustworthy peer in dynamic environment since peers join and leave the network randomly. As Cryptographic model is designed to handle the signature based authentication, it doesn’t show a good performance when trust value is applied during query message transactions. Even though Fine-Grained reputation method is designed for unstructured P2P networks, it could not produce a better performance since central servers are used to store the data which does not support the concept of pure P2P networks.

Table 7.1 shows the data set arrived through transactions with the proposed ORM and transactions without ORM. At initially five peers were connected in an overlay network and 50 transactions are done through the network. Based on the past transactions, the trust value is evaluated and trustworthy peers are identified. ORM uses trustworthy peers for transactions, the trustworthy peers are identified based on the value which is arrived from Equations 7.1 and 7.2.
Table 7.1 Recognition results with ORM and without ORM

<table>
<thead>
<tr>
<th>S.No:</th>
<th>Number of Transactions (in 10's)</th>
<th>Average number of malicious transactions with ORM</th>
<th>Average number of malicious Transactions without ORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>2.60</td>
<td>12.75</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>3.01</td>
<td>15.01</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>4.20</td>
<td>17.98</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>3.72</td>
<td>19.21</td>
</tr>
</tbody>
</table>

Figure 7.2 shows the variation in average number of malicious transactions with ORM and without ORM, where x axis shows the number of transactions and y axis shows the average number of malicious transactions. As visible in Figure 7.2, the total number of malicious transactions increased considerably by about 80 percent when the proposed model was not used but are less when the proposed model was used. From the solution it is proved that the ORM method reduces the number of malicious transactions from the perspective of the overlay network and from the perspective of each peer.
Figure 7.2 Variation in average number of malicious transactions

Table 7.2. Show 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 the RQR design and applied both the cryptographic algorithm namely RSA blinding and optimal reputation model (ORM) and arrived with the following data.
Table 7.2 Comparison of average number of satisfactory transactions

<table>
<thead>
<tr>
<th>S.No</th>
<th>Number of queries (in 10’s)</th>
<th>average number of satisfactory transactions (P2P Optimal Reputation Model in %)</th>
<th>average number of satisfactory transactions (RSA Blinding Technique in %)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>1.75</td>
<td>0.73</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>1.96</td>
<td>0.92</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>2.07</td>
<td>1.20</td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>2.15</td>
<td>1.42</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>2.22</td>
<td>1.58</td>
</tr>
</tbody>
</table>

Figure 7.3 shows the comparative results of RSA Blinding cryptographic and Optimal Reputation Model, where x-axis indicates the number of queries (or transactions) (in 10’s) and y-axis represents average number of satisfactory transactions (in percentage). The graph shows that the average number of satisfactory transaction of optimal reputation model is about 50 percent more compared to RSA Blinding cryptographic algorithm. From the result it is observed that the number of messages destroyed in RSA Blinding is higher, so its overall performance in dynamic environments is not as good as Optimal Reputation model. Overall, Optimal Reputation model outperforms RSA Blinding cryptographic algorithm.
The results from Table 7.3 show that the proposed method is effective and outperforms the other methods by interacting through trustworthy peers. The average number of satisfied transaction is more in the proposed method than in the others due to the system design and lagging of trustworthy peers.

**Figure 7.3 Comparison on number of satisfactory transactions**

The graph illustrates the comparison of average number of satisfactory transactions for different methods: P2P optimal reputation model, RSA blinding technique, and the proposed method.
Table 7.3 Recognition results with ORM and without ORM

<table>
<thead>
<tr>
<th>S.No:</th>
<th>Number of query messages (In 10’s)</th>
<th>Average Number of satisfied transactions (in %)</th>
<th>Pseudo Trust</th>
<th>Average Number of satisfied transactions (in %)</th>
<th>P2P Reputation Model</th>
<th>Average Number of satisfied transactions (in %)</th>
<th>Optimal Reputation Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>0.79</td>
<td></td>
<td>0.85</td>
<td></td>
<td>1.75</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>0.99</td>
<td></td>
<td>1.14</td>
<td></td>
<td>1.96</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>1.32</td>
<td></td>
<td>1.49</td>
<td></td>
<td>2.07</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>20</td>
<td>1.58</td>
<td></td>
<td>1.75</td>
<td></td>
<td>2.15</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>1.97</td>
<td></td>
<td>2.01</td>
<td></td>
<td>2.22</td>
<td></td>
</tr>
</tbody>
</table>

7.5 SUMMARY

Here a novel ORM method is proposed to identify the trustworthy peer through which the transactions can be done. This method clearly shows the total number of transactions done through the existing overlay network and also categorizes the transactions based on their past history, such as number of satisfied transactions and number of unsatisfied transactions. The formulae use all the parameters effectively to compute the trust value of peers in P2P environment. Since the overlay network is unstructured it supports dynamic characteristics of P2P systems. The experimental results show an increased performance of the proposed method with the other security policies.
The major benefits addressed by this ORM with security measures of P2P overlay network are as follows:

- Reputation system maintains the data of periodic contribution of other peers in the network which makes an accumulative value for the past behavior (History Table).

- Trustworthy peer is identified based on the number of satisfied transactions (i.e. number of satisfied transactions should be more than that of unsatisfied transactions).

- Transactions made through the trustworthy peers produce minimum number of malicious transactions.

- From the total number of transactions this model identifies the number of satisfied transactions so as to evaluate Transaction Success Rate (TSR).

- Trustworthy peer can estimate the authenticity of data other peers share by their trust value.

- This model resulted in high transaction success rate.

From the experimental result it was observed that

- It is effective to prevent malicious act and encourage peers to share resources in P2P network.

- By implementing ORM security policy, requester exchanges their resources securely with confidence.

- This model supports the dynamic characteristic of P2P systems.