ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

A Secure Distributed Peer To Peer Systems

H.Shaheen , M.Baskaran

Assistant Professor, Dept. of CSE., Nehru Institute of Engineering & Technology, Coimbatore, India

ABSTRACT: A P2P network can be an ad hoc connection- a couple of computers connected via a Universal Serial Bus to transfer files. And these networks are vulnerable to peers. The traditional security techniques are insufficient for P2P networks as they are insecure by their very nature. There's no centralized server controlling access to shared resources in a P2P network which have unique challenges including identity management of the peers, secure reputation data management, Sybil attacks, and above all, availability of reputation data. The future actions are predicted where peers are encapsulated in its digital reputation, based on the past behaviour of the peer.Thus a peer's reputation allows it to cooperate and prevent from malicious activities. The cryptographic protocol is coupled with self-certification and cryptographic mechanisms for identity management and countering Sybil attack.

Keywords: Peer-to-peer networks, distributed systems, security, reputations, identity management

I. INTRODUCTION

PEER-TO-PEER (P2P) networks are self-configuring networks with minimal or no central control. P2P networks are more vulnerable to dissemination of malicious or spurious content, malicious code, viruses, worms, and trojans than the traditional client-server networks, due to their unregulated and unmanaged nature. For example, the infamous VBS. Gnutella worm that infected the Gnutella network, stored trojans in the host machine.

The peers in the P2P network have to be discouraged from leeching on the network .The traditional mechanisms for generating trust and protecting client-server networks cannot be used for pure1 P2P networks. This is because the trusted central authority used in the traditional client-server networks is absent in P2P networks. Introduction of a central trusted authority like a Certificate Authority (CA) can reduce the difficulty of securing P2P networks. The major disadvantage of the centralized approach is, if the central authority turns malicious, the network will become vulnerable. In the absence of any central authority, repository, or global information, there is no silver bullet for securing P2P networks.

The Reputation Systems for P2P networks—a more ambitious approach to protect the P2P network without using any central component, and thereby harnessing the full benefits of the P2P network. The reputations of the peers are used to determine whether a peer is a malicious peer or a good peer. Once detected, the malicious peers are ostracized from the network as the good peers do not perform any transactions with the malicious peers. Expulsion of malicious peers from the network significantly reduces the volume of malicious activities.

The experiments show that the proposed reputation infrastructure not only reduces the percentage of malicious transactions in the network, but also generates significantly less network traffic as compared to other reputation-based security solutions for P2P networks.

The main contributions are:

1. A self-certification-based identity system protected by cryptographically blind identity mechanisms.

2. A light weight and simple reputation model.

3. An attack resistant cryptographic protocol for generation of authentic global reputation information of a peer

II. RELATED WORK

In [1] the author states that a system where peers work only for selfish interests while breaking the rules decays to death. Any reputation system is vulnerable to ballot stuffing and bad mouthing as described in [10]. In a centralized system, a trusted authority would have issued these identity certificates. In a decentralized reputation system, self-certification [12] splits the trusted entity among the peers and enables them to generate their own identities. Each peer runs its own CA that issues the identity certificate(s) to the peer. All the certificates used in self certification are similar

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

to SDSI certificates [5]. The reputation of a peer is associated with its identity and the reputation of a CA is the accumulated reputation of the identities. There is a big body of work in Decision Theory, Game Theory, and Probability [14], [15], [16] which can be used for selecting appropriate values of the definition of function F() depending on the levels of the threat faced by the peers in the P2P network.

III. REPUTATION SYSTEM

A Gnutella-like network, has a power-law topology and supports Insert and Search methods. The peers follow predefined Join & Leave protocols. The peers are connected with insecure communication channels. As the peers are likely to have conflicting interests, a source of motivation is needed to reduce the number of leechers. Leechers are peers who derive benefit from the system without contributing to the system. The rogue peers can also spread malware in the network (when other peers download content from them). Finally, peers need a mechanism to judge the quality of the content before making Go/No-Go decision in transactions and thereby develop trust relationships with other peers.

A perfect reputation system can provide the means to achieve the above goals. An imperfect reputation system by itself generates vulnerabilities that can be exploited by attackers. Peers need to have a unique handle to which their reputations can be attached. 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. Finally, there are other vulnerabilities that come in the picture depending on how a given reputation system is designed.

IV. SELF-CERTIFICATION

In order to participate in the reputation system, a peer needs to have a handle. The reputation of a peer is associated with its handle. This handle is commonly termed as the "identity" of the peer even though it may not "identify" a peer, i.e., it may not lead to the real-life identity of the peer. A peer receives a recommendation for each transaction performed by it, and all of its recommendations are accumulated together for calculation of the reputation of a given peer. The reputation of a peer is associated with its identity and the reputation of a CA is the accumulated reputation of the identities.

A malicious peer can use self-certification to generate a large number of identities and thereby raise the reputation of one of its identities by performing false transactions with other identities. The malicious peer does not even need to collude with other distinct peers to raise its reputation, but only needs to generate a set of identities for itself. Such a large set of identities managed by one peer is called an identity farm. The set of identities that issue false recommendations is called a liar farm. This attack belongs to the class of attacks termed Sybil attacks. In simple words, a peer having an identity farm is equally capable of subverting a reputation system as a peer that has colluded with a large number of other peers.

In self-certification, each peer's CA can generate multiple identities. The recommendations received for a peer's identity from different identities of other peers, signed by the other peer's CA(s), are identified as signed by the same CA, and are averaged to counter the liar farms. In a transaction, the requester averages all the recommendations of the provider by CAs of the provider's past recommenders. Hence, all the past recommendations owned by the provider carry equal weight but they get averaged. Finally, it adds the averages of each CA to calculate the reputation of the provider identity. Hence, a peer cannot use its own identities (all generated by the same CA) to recommend its other identities.

Unlike the traditional CA or distributed CA-based approaches, grouping of peers preserves the anonymity of the peers; when combined with self-certification it curtails the possibility of a Sybil attack. In contrast to the traditional CA-based approach, neither the group authority nor the transacting peers can establish the identity of the peer. In addition, certificate revocations are not needed in the group-based approach as the group authority only vouches for the real-life existence of the peer, unlike the traditional certificate-based approaches where various certificate attributes are attested by the authority and necessitate revocation if any of those attributes mutate in time. If a highly reputed identity is compromised, its misuse would be self-destructive as its reputation will go down if misused.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

V. REPUTATION MODEL

Once a peer has obtained its identity, it joins the P2P network using the standard Join method of the particular P2P network. The peer (requester) searches for one or more files using the Search method provided by the network. On the basis of the responses received, as a result of its search request, the requester generates a list of peers who have the requested file(s). The number of peers who offer a particular file is denoted by RANGE. The requester selects the peer (provider) with the highest reputation from the list and initiates the cryptographic protocol. In the protocol, the requester uses the Download method of the network, to download the file from the provider. Subsequently, it verifies the integrity, authenticity, and the quality of the file. Depending on its verification results, it sends a recommendation between MIN_RECOMMENDATION and MAX_RECOMMENDATION to the provider.

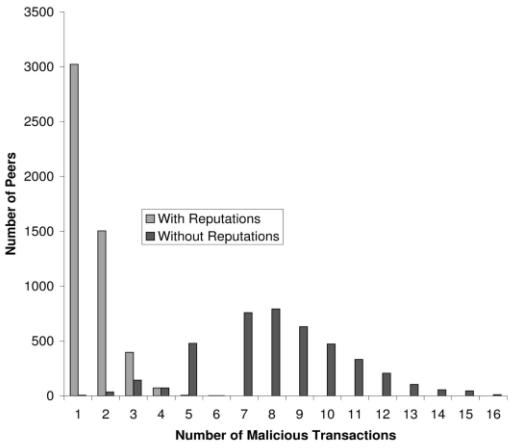
The proposed reputation model is independent of the topology of the P2P network, addressing schemes for its nodes, bootstrap mechanisms, joining and leaving protocols of peers, and the name service. In other words, the choice of any of these components has no impact on the reputation model and vice versa.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

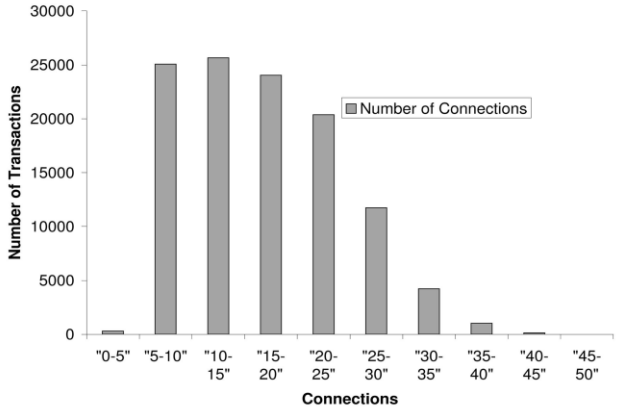
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

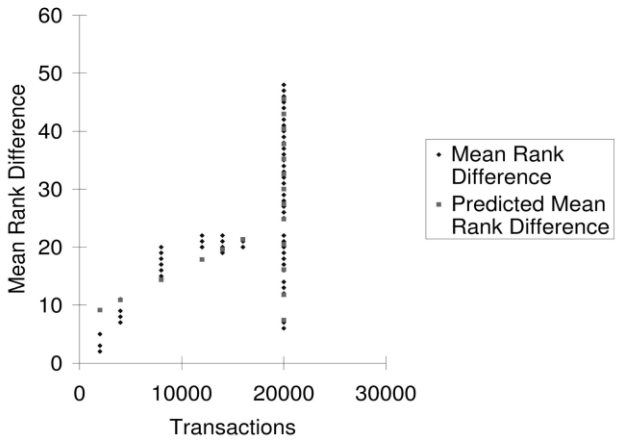
Vol. 2, Issue 1, January 2014



(a)



(b)



(c)

Fig.1. Variation in total number of malicious transactions.
(a) Number of peers versus malicious transactions d =3.
(b) Mean rank difference Versus number of connections
(c) Mean rank difference versus number of transactions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

VI. REPUTATION EXCHANGE PROTOCOL

The steps in the reputation exchange protocol are as follows:

Step 1: R→P: RTS & IDR

The requester sends a REQUEST FOR TRANSACTION (RTS) and its own IDENTITY CERTIFICATE (IDR) to the provider.

Step 2: P→R : IDP & TID & E_{PK2} (H(TID||RTS))

The provider sends its own IDENTITY CERTIFICATE (IDP), the CURRENT TRANSACTION ID (TID) and the signed TID, E_{PK2} (H(TID|| RTS)). The signed TID is needed to ensure that the provider does not use the same transaction id again. In the end of the protocol, this signed TID is signed by the requester also and stored into the network where it will be accessible to other peers.

Step 3: R : LTID =Max (Search (P_{K1} || TID))

The requester obtains the value of the LAST TRANSACTION ID (LTID) that was used by the provider, from the network. The requester concatenates the public key of the provider with the string TID and performs the search.

Step 4: R : IF(LTID ≥ TID) GO TO Step 12

Hence, it is trying to get another recommendation for the same transaction number (TID). The requester suspects foul play and jumps to Step 12.

Step 5: R→P: Past Recommendation Request & r

If the check in Step 4 succeeds, i.e., the requester is sure that the provider is not using the same transaction number, it requests the provider for its previous recommendations

Step 6: P→R: CHAIN, E_{PK2} (CHAIN)

CHAIN =({REC_{N-1}||E_{ZN-1K2} (H(REC_{N-1})} ||{REC_{N-2}||E_{ZN-2K2}(H(REC_{N-2};REC_{N-1})} ||{REC_{N-3}||EZ_{N-3K2} (H(REC_{N-3};REC_{N-2})} || . . . . {REC_{N-4}||EZ_{N-4K2}(H(REC_{N-r};REC_{N-r-1})})

The provider sends its past recommendations (REC_{N-1};REC_{N-2} . . .REC_{N-3}) which were provided by peers (Z_{N-1}; Z_{N-2}; . . .Z_{N-3}).

Step 7: R : Result =Verify(REC_{N-1};REC_{N-2} . . .REC_{N-r}) If Result != Verified GO TO STEP 12

The requester verifies the CHAIN by simple public key cryptography.

Step 8: P→R : File or Service

The provider provides the service or the file as per the requirement mentioned during the search performed for the providers.

Step 9:

R →P : B1 = EB_{Ka}(REC|| TID||E_{RK2}(H(REC, ||TID)})

Once the requester has received a service, it generates a BLINDING KEY, Ka. The requester concatenates the RECOMMENDATION (REC) and the TRANSACTION ID (TID) it had received in Step 2 and signs it.

Step 10: a. P→R : B1||E_{PK2} {H(B1); nonce),nonce

b. R→P : Ka

The requester verifies the signature and then sends the blinding key Ka to the provider which can unblind the string received in Step 10a and checks its recommendation.

Step 11: Insert(IDR, {REC|| TID || E_{RK2} {H(REC) || H(TID)}})

The requester signs: the recommendation that was given to the provider (REC), the transaction id (TID), and its own identity certificate and stores it in the network using the Insert method of the P2P network. This completes the transaction.

Step 12: Step 12 explains the steps a requester executes when it expects foul play:

ABORT PROTOCOL

R: Insert(IDR, {CHAIN| |TID| | E_{RK2}{H(CHAIN) | |H(TID)}})

If the verification in Step 7 fails, the requester takes the CHAIN that was signed by the provider and the Transaction Id (TID), signs it and uses the INSERT method of the network to insert the chain and its own identity certificate into the network. As a result, any subsequent requester

will be able to see failed verification attempt and will assume a MIN RECOMMENDATION recommendation for that TID for the provider. The requester cannot insert fake recommendations into the network because it has to include the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 1, January 2014

TID signed by the provider. If the requester reaches Step 12 from Step 4. It will request for the Chain from the Provider and subsequently will perform R : Insert(IDR;,{CHAIN || TID || E_{N_RK2}{H(TID || RTS))}}).

VII. CONCLUSION

The self-certification-based identity generation mechanism reduces the threat of liar farms by binding the network identity of a peer to his real-life identity while still providing him anonymity. The Identity mechanism is based on the fundamental that the ranks of the peers are more relevant than the absolute value of their reputation. The cost of this security is the difference in the ranks of the providers because of the use of the proposed mechanism. 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 proposed protocol reduces the number of malicious transactions and consumes less bandwidth per transaction than the other reputation systems proposed in its category. It also handles the problem of highly erratic availability pattern of the peers in P2P networks.

REFERENCES.

1. H. Garett, "Tragedy of Commons," Science, vol. 162, pp. 1243-1248, 1968.
2. I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M.F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," Proc. ACM SIGCOMM, pp. 149-160, Aug. 2002.
3. S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A Scalable Content-Addressable Network," SIGCOMM Computer Comm.. Rev., vol. 31, no. 4, pp. 161-172, 2001.
4. G.Networks,"Groove Networks," http://www.groove.net/ products/workspace/securitypdf.gtml, 2009.
5. R.L. Rivest and B. Lampson, "SDSI: A Simple Distributed Security Infrastructure," Proc. Crypto '96, pp. 104-109, Aug. 1996.
6. N. Li and J.C. Mitchell, "RT: A Role-Based Trust-Management Framework," Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX III), Apr. 2003.
7. D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., May 1992.
8. D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Advances in Cryptology (Crypto '82), 1983.
9. L. Zhou, F. Schneider, and R. Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.
10. C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," Proc. ACM Conf. Electronic Commerce, pp. 150-157, Oct. 2000.
11. C. Dellarocas, Building Trust On-Line: The Design of Reliable Reputation Mechanism for Online Trading Communities. MIT Sloan School of Management, 2001.
12. P. Dewan, "Injecting Trust in Peer-to-Peer Systems," technical report, Arizona State Univ., 2002.
13. A. Clausen, "How Much Does it Cost to Buy a Good Google Pagerank?" unpublished, Oct. 2003.
14. G. Shafer and J. Pearl, Readings in Uncertain Reasoning. Morgan Kaufmann, 1990.
15. F.K. Robert and A. Wilson, The MIT Encyclopedia of the Cognitive Sciences (MITECS). Bradford Books, 1999.
16. D.P. Foster and H.P. Young, "On the Impossibility of Predicting the Behavior of Rational Agents," technical report, John Hopkins Univ., 1999.