SEPastry: Security Enhanced Pastry

Madhumita Mishra, Somanath Tripathy, and Sathya Peri

Indian Institute of Technology Patna, India
{madhumita,som,sathya}@iitp.ac.in

Abstract. Pastry is one of the most popular DHT overlay used in various distributed applications, because of its scalability, efficiency and reliability. On the other hand, Pastry is not resistant against the more generous attacks include Sybil attack, Eclipse attack etc. In this paper, we propose SEPastry (security enhanced pastry) to heighten the security features of Pastry without using any computational cryptographic primitives. SEPastry is found to be resistant against various forms of node-id attacks like Sybil attack, Eclipse attack, etc..

Keywords: Structured p2p, Pastry, Security, node-id attack.

1 Introduction

Structured Peer to Peer (P2P) systems are the distributed hash table (DHT), which provides an efficient decentralized look up facilities. P2P network services are characterized by features like high scalability and efficiency, well capable of handling random node failures. Mostly structured P2P is used in various distributed network applications. Sharing of file, audio, video, mails, document and electronic commerce are the widely used distributed application. Security concern rises with the increase of the connectivity and sharing.

In structured systems peers and keys of content objects are identified by using a set of IDs. DHT provides a self organizing substrate for large scale P2P applications. Structured overlays guarantee that the number of hops required to reach any node in the network is upper-bounded by O(logN) where N is the number of participating nodes [9]. Additionally there is the guarantee that a document if present in the network will definitely be reached. P2P network uses distributed hash table (DHT) to establish an association among peers and resources. Structured overlays allow applications to locate any object in a probabilistically bounded, small number of network hops, while requiring per-node routing tables with only a small number of entries. There are various structured peer to peer overlay architectures such as Chord, Pastry, CAN, etc. impose a specific linkage structure between nodes, Pastry posses huge potential to build self organizing applications to today′ s programmers. Pastry provides scalability with a low management overhead, reliability and are theoretically able to find data in O(log n) steps [1]. Applications like SCRIBE, PAST have been built on top of pastry because of its inherent advantages. SCRIBE [2] is used for group communication and event notification while PAST [11] is a peer to peer archival

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 789–795.
springerlink.com

storage utility implemented using Pastry. The popularity of pastry, in real world distributed application is rapidly increasing. However, to make it more acceptable, the security of Pastry needs to be heightened.

In a Pastry network a node is randomly assigned a nodeId, given a message and numeric key, the node routes the message to a nodeId numerically closest to the key. While routing a given message the node first checks the leafset. The leafset of node i contains the L/2 nodes numerically greater closest to node i and the L/2 nodes numerically smaller closest to node i. If the given key falls within it then the message reaches its destination in one hop else refers to the routing table. The nodeId of the network can be harnessed by attackers to induce malicious behaviour in the network. Tampering the nodeId in the Pastry networks gives rise to several security issues in the network. In this paper we propose a mechanism named Security Enhanced Pastry (SEPastry), to secure Pastry from the most generous attack called nodeId attack. At any instant of time a node attached to the internet may wish to join the existing the overlay network for obtaining services or can even leave the P2P network. The protocol design aims to mitigate the threat of joining of bogus node. The attractive feature of this scheme is that it disallows the non-registered nodes to join into the network without involving any computational complex cryptographic mechanisms.

The paper is organized as follows. The related work is elucidated in Section 2. The SEPastry protocol to secure the node Id and node joining process has been revealed in Section 3. Section 4 illustrates the security analysis of the protocol. A brief comparison with other protocols is presented in Section 5 and concluded in Section 6.

2 Related Work

Exploitation of nodeId in structured P2P network is possible in various ways.By taking advantage of this fact attackers induce hazardous impact on the working of network protocol. Effort to secure structured P2P network is the area of focus of several researchers. In [4], NodeId attacks are categorised into two types ID mapping attack and Sybil attack. ID mapping attack[3] is utilized to obtain a set of particular identifiers. User can choose its own identifier and can obtain a desired position in the overlay network. This eventually allows a malicious user to gain control over certain resources. In Sybil attack [6], a single malicious user creates multiple fake peer identities and pretends to be multiple, distinct physical nodes in a system.

Approach to detect and recover the structured overlays from identity attacks is attempted in [7]. Mechanism proposed is based on the reliable performance of nodes in the presence of malicious peers. Periodically nodes construct and disseminate existence proofs for each name space regions to the set of proof managers for that region. A node queries the proof manager , successful replies provides indisputable evidence of an attempted identity attack.The mechanism proposed by

them is based on the reliable performance of nodes in the presence of malicious peers. After detecting and identifying the malicious node , the set of other nodes constantly avoid them when routing the KBR requests.

An admission control system(ACS) for structured P2P systems is given in [4]. The system constructs a tree-like hierarchy of cooperative admission control nodes, from which a joining node has to gain admission via client puzzles. ACS defends against Sybil attacks by adaptively constructing a hierarchy of cooperative admission control nodes. A node wishing to join the network is serially challenged by the nodes from a leaf to the root of the hierarchy. Nodes completing the puzzles of all nodes in the chain are provided a cryptographic proof of the examined identity. Borisov proposes to add computational challenges to Chord in order to defend against Sybil attacks. Castro et al. suggest using a set of trusted certification authorities to produce signed certificates that bind a random node identifier to a public key and node's IP address. According to them inclusion of IP address in the certificate makes it difficult for an attacker to swap certificates between nodes it controls and also allows optimization based on minimizing communication delays.This mechanism works well with DHTs such as Chord, Pastry and Tapestry, where the identifiers are fixed. Distributed registration procedure is proposed in [5] for Chord. According to this system, each virtual node registers r registration nodes in the Chord ring. The r registration nodes are computed using the hash of the IP address and an integer j ($1 < j < r$) .Registration nodes maintain a list of registered virtual nodes for each IP address and reject registration if the number of registered nodes for each IP address exceeds a system wide constant a. This approach provides a reasonable level of protection by regulating the number of identities that a malicious IP address can get. Wang et al. proposed a concept called net-print to build a secure DHTs.Net-print of a node is built using a node's default router IP address, its MAC address and a vector of RTT measurements between the node and a set of designated landmarks. According to them physical network characteristics can be used to identify nodes. The proposed mechanism attempts to make identity theft difficult. Bazzi and Konjevod proposed a defence mechanism based on physical network characteristics. The proposed mechanism aims to identify individual nodes and guarantee that identities in different groups are not controlled by the same entity. Informant protocol proposed in [10] based on game theory principles to detect rather than prevent Sybil attack. SEPastry has been designed with an approach to completely delimit the fact of existence or joining of malicious node with two simple operational phases.

3 SEPastry: The Proposed Mechanism

The Security Enhanced Pastry (SEPastry) comprises of the following two operational phases: Registration Phase and Joining Phase. A node willing to (access/) provide the services to (/from) p2p network, needs to register with a centralized server called registration server (RS), before it joins. Thus the non-registered

nodes can be prevented easily, to participate in the networking operation during the joining phase. Note that if a node leaves from the network, it informs to RS, which makes the RS to exclude that node from the potential leafset in future.

Registration Phase: Each node X executes the registration phase before joining/ accessing to the network services. X sends the registration request comprising of IP address to the Registration Server (RS). RS generates a random number and assigned it to nodeId of X (ID_X). RS replies with the node-id (ID_X) to X in a secure way. Further, RS sends the (ID_X) and corresponding IP address (IP_X), to the potential leafset through a secure channel. Figure 1 illustrates the phase of registration.

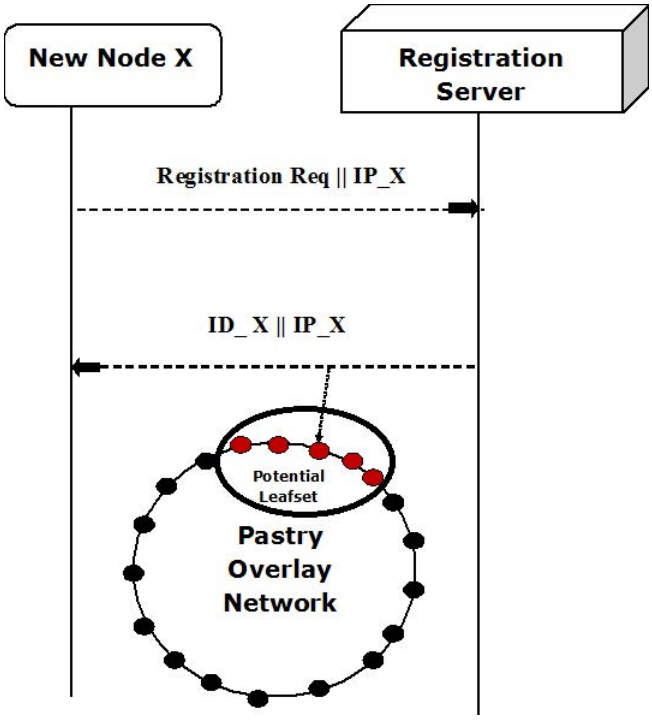

Fig. 1. Registration Phase

Joining Phase: The new node X willing to join, is assumed to know about node A on the basis of proximity metric.Node X then asks A to route the joining request message which comprises of the nodeId (ID_X) and IP address (IP_X).

This request needs to be routed to the existing node Z whose Id is numerically equivalent to ID_X. Now the leafset NodeIds of node Z verifies the validity of the given parameter in the request and responds with a positive or negative acknowledgement message accordingly.The new node receives positive responses greater than or equal to threshold value(β) from the potential leafset Ids.In such a situation the nodes A, Z and all nodes encountered on the path from A to Z send their state tables information to node X. Otherwise the new node is refrained from initializing its state table.The joining phase is as shown in figure 2.

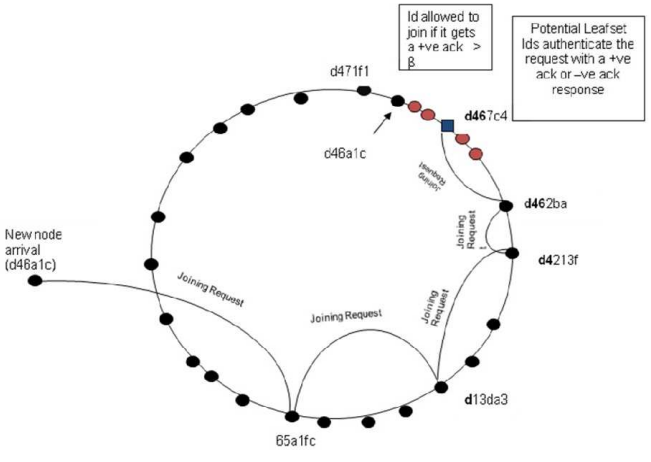

Fig. 2. Joining Phase

4 Security Analysis of SEPastry

The level of defence offered by SEPastry against the various possible attacks in the structured P2P network is illustrated as follows:

Sybil Attack: In Pastry, nodeId is obtained as the hash digest of the node's IP address. A malicious user can simultaneously spoof many IP addresses to quickly obtain a multitude of identities.The registration phase in SEPastry restricts the possibility of creating multiple identities. As a result the proposed protocol provides high level of security against Sybil attack.

Eclipse Attack: Successful restriction of Sybil attack in a way reduces the possibility of Eclipse attack. However Eclipse attack is also possible in presence of defence against Sybil attack such as nodeId certificate solution [9].

A small set of malicious node with legitimate identities is sufficient to carry out Eclipse attack . The two phases of SEPastry provides strong defence against

Eclipse attack as no malicious node is allowed to place itself in between the nodes and reroute the message.

Message Forwarding Attack: In case of an honest node where all the entries are valid, the message is delivered to the root node for the key after an average of number of hops. There are two cases in this category of attack, presence of faulty node in the path or the root node may be faulty. Routing may fail in the presence of a faulty node along the path. Presence of faulty node along the path may simply drop the message, route the message to the wrong place of the node. As SEPastry restricts to join the illegitimate node into the network, the message forwarding like attacks are reduced. However, if an inside node becomes malicious, it requires detection mechanism to exclude the said node. This is beyond the scope of this work.

5 Discussion

In comparison to Bootstrap server mechanism this provides additional security as the joining node contacts a set of leafset Ids and waits for threshold response. Failure of one or two leafset Ids does not have an impact in the joining process. In contrast to identity based cryptography protocol, SEPastry does not involve the computational complexity of cryptographic technique. During the joining phase the cost incurred in sending request messages and getting response from Leafset nodeId is negligible. The process of securing the node joining procedure improves the overall routing performance of the network as it mitigates the threat of routing table poisoning. Overall scalability, reliability and efficiency of the network improves. SEPastry boost up the process of safe and sound node joining as compared to any other proposed protocol. The mechanism guarantees the process of assigning each peer with a unique nodeId. Strongly forbids attacks like Sybil attack and eclipse attack. SEPastry provides optimized flow control, load balancing and QoS routing. In this proposed mechanism, there is no issue of assigning certificate. Issuing certificate mechanism to authenticate the joining process is time consuming. SEPastry protocol secures the whole structure relatively in shorter time span. In Eigen trust algorithm to establish trust in the system it requires a large number peers to cooperate. In contrast SEPastry protocol requires only a few set of Ids to secure the joining procedure.

6 Conclusion

NodeId attacks have the potential of completely paralysing the whole network structure. This paper proposed SEPastry to enhance the security features of the existing Pastry without using any computational intensive cryptographic operations. SEPastry is found to be robust against Sybil attack, Eclispse attack, etc.

References

1. Rowstron, A., Druschel, P.: Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems. In: Guerraoui, R. (ed.) Middleware 2001. LNCS, vol. 2218, pp. 329–350. Springer, Heidelberg (2001)
2. Rowstron, A., Kermarrec, A.-M., Druschel, P., Castro, M.: Scribe: The design of a large-scale event notification infrastructure. In: Intl. Workshop on Networked Group Communication (NGC 2001) (June 2001)
3. Cerri, D., Ghioni, A., Paraboschi, S., Tiraboschi, S.: ID mapping attacks in P2P networks. In: IEEE Global Telecommunications Conference, GLOBECOM 2005, December 3 (2005)
4. Rowaihy, H., William, E., Patrick, M., Porta, T.L.: Limiting sybil attacks in structured peer-to-peer networks. Technical Report NAS-TR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA (2005)
5. Dinger, J., Hartentstein: Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges,and a Proposal for Self-Registration. In: Proc. 1st International Conference on Availability, Reliability and Security, Vienna, Austria, pp. 756–763. IEEE Computer Society Press, Los Alamitos (2006)
6. Douceur, J.R.: The Sybil Attack. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002)
7. Puttaswamy, K., Zheng, H., Zhao, B.: Securing structured overlays against identity attacks. IEEE Transactions on Paralleland Distributed Systems 2010, 1487–1498 (2009)
8. Aiello, L.M., Milanesio, M., Ruffo, G., Schifanella, R.: Tampering Kadmelia with a Robust Identity Based System. Computer science Department - Universit'a degli Studi di Torino, Italy
9. Castro, M., Druschel, P., Ganesh, A., Rowstron, A., Wallach, D.S.: Secure routing for structured peer-to-peer overlay networks. In: Proc. of the 5th Usenix Symposium on Operating Systems Design and Implementation, Boston, MA (December 2002)
10. Margolin, N.B., Levine, B.N.: Informant: Detecting Sybils Using Incentives. In: Dietrich, S., Dhamija, R. (eds.) FC 2007 and USEC 2007. LNCS, vol. 4886, pp. 192–207. Springer, Heidelberg (2007)
11. Druschel, P., Rowstron, A.: PAST: A large-scale, persistent peer-to-peer storage utility. In: Proc. HotOS VIII, Schloss Elmau, Germany (May 2001)