

A Markov-chain based Analytical Approach to Resilience of Structured P2P Systems

Shengquan Wang and Dong Xuan

I. INTRODUCTION

A peer-to-peer (P2P) networked system is a group of Internet nodes, which construct their own special-purpose networks on top of the Internet. Such a system performs application-level routing on top of IP routing. Consider a few scalable P2P systems that support distributed hash table (DHT) functionality such as CAN/Chord/Tapestry/Pastry. Because of their rich structural arrangement they have efficient key lookups and also somewhat resistant to failures of nodes. However, almost all protocols are designed as an ideal overlay structure under which the key lookups are efficient. P2P nodes are notoriously transient and the resilience of routing to failures is a very important consideration. This is a serious concern since performance constraints in an ad hoc network are critical to the existence of the network itself. Most P2P architectures assume forwarding nodes are benign and trustworthy. Although justifiable in an isolated network, it is not in the case of the Internet. The system should operate in the presence of malicious nodes.

The goal of this study [1] is to systematically analyze the features of resilience to failures and attacks of the current structured P2P systems in terms of average path length and hit ratio and understand the causes, which lead to better resilience features.

II. A MARKOV-CHAIN BASED APPROACH

In structured P2P systems, once a node receives a query, with different *purposes*, it can either forward the query to some node or drop the query. The purpose can be benign or malicious:

- *Benign forwarding*: The decision on which node the query is forwarded to is influenced by availability of its neighboring nodes. A failure of a neighboring node or a connection to it will lead to unavailability of the neighboring node. However, the best one among available next-hop candidates according to the routing semantics of the P2P system is always selected (The best one means the closest next hop to the destination).
- *Malicious forwarding*: A compromised node forwards the query to a bad next hop with its own malicious purpose. Where the query is forwarded depends on different attacks, which generally will disobey the correct semantics of routing (The bad next-hop may be far away from the destination).
- *Benign dropping*: Once all good next-hop candidates are not available, the query will be dropped at the node.
- *Malicious dropping*: A compromised node can drop the query no matter whether there is any available next-hop candidate.

The routing behaviors in structured P2P systems are illustrated in Fig.1. P_f^b and P_d^b denotes the probabilities that a node takes benign forwarding and benign dropping respectively. They are determined by the routing semantics and the availability of the node's neighboring nodes. P_f^m and P_d^m denote the probabilities that a node takes malicious forwarding and malicious

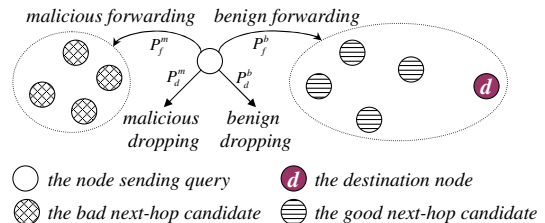


Fig. 1. Routing in Structured P2P Systems

dropping respectively. The summation $P_f^m + P_d^m$ reflects the degree of a node being compromised.

In this study, we are interested in the system being in a stable state, where (1) nodes are uniformly distributed in the system, and (2) the number of nodes in the system changes not much over time although nodes keep leaving and joining.¹ As we know, in P2P systems, during the data look-up process, a node forwards a query to the next node based on its current status. The routing process can be further modelled as a discrete absorbing *Markov chain*. Define a stochastic process $\{X_h : h = 0, 1, \dots\}$, where random variable X_h is the state of a query forwarding during a look-up process. The query is forwarded to the destination (“destination state”) or dropped finally (“drop state”). These two states are absorbing and the others are transient.

In a system with n nodes, the nodes are named starting from 0 to $n-1$. Without loss of generality, we consider node 0 as a destination, and all other nodes $1, 2, \dots, n-1$ as sources. We define the state i ($0, 1, \dots, n-1$) as the state when the query is at node i . We denote n as the “drop state”. We know that $1, 2, \dots, n-1$ are transient states and $0, n$ are absorbing states. We define the *transition probability* as $p_{i,j} = \Pr[X_h = j | X_{h-1} = i]$. Assume that Q is an $(n-1) \times (n-1)$ matrix and U, V are $(n-1) \times 1$ matrices, then the matrix of transition probabilities $P = (p_{i,j})_{(n+1) \times (n+1)}$ can be easily written as follows:

$$P = \begin{pmatrix} 1 & 0 \dots 0 & 0 \\ U & Q & V \\ 0 & 0 \dots 0 & 1 \end{pmatrix}. \quad (1)$$

In this work, resilience is measured in terms of *average hit rate* and *average path length* between the source and the destination. They can be obtained by the following theorem [1]:

Theorem 1: The average *hit ratio* \bar{a} and the average hit path length \bar{m} for the algorithm sending query from any source to the destination 0 are given by $\bar{a} = \frac{1}{n}(\pi^0 A + 1)$, $\bar{m} = \frac{1}{n}\pi^0 M$, where $A = (I - Q)^{-1}U$, $M = ((I - Q)^{-1}A) \div A$ and $\pi^0 = (1, 1, \dots, 1)$.²

III. ANALYZING RESILIENCE TO FAILURE AND ATTACK

A. Resilience to Failure

At some time instant, to one node, its neighbors may be up or down. As define in [2], there are two main kinds of neigh-

¹For detailed discussion of this state, please read [1].

²Define $Z = X \div Y$ as $z_{i,j} = x_{i,j}/y_{i,j}$ for any i, j .

bors: *local neighbors* (such as the successor list in Chord and the Leaf Set in Pastry) and *remote neighbors*. In this section, we would like to investigate the impacts of local neighbors and remote neighbors on resilience of structured P2P system. We define τ_1 and τ_2 as the probabilities that a local neighbor and a remote neighbor are in failure state in terms of this node at some point of time respectively (Generally $\tau_1 < \tau_2$). In this model, we assume there are no malicious attacks. We need only consider benign forwarding and benign dropping, *i.e.*, for each node, we have $P_f^b + P_d^b = 1$.

The key to apply the Markov-chain based approach is computing the transition probability $p_{i,j}$ from node i to node j for a given structured P2P system. The transition probabilities of CAN are, for $i = 1, 2, \dots, n-1$,

$$p_{i,j} = \begin{cases} (1 - \tau_1^{|N(i)|})/|N(i)|, & j \in N(i) \\ \tau_1^{N(i)}, & j = n \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

We apply the above formulae to compute the average path length and the hit ratio for CAN, Chord, Pastry and Tapestry systems. Here we only report data of CAN and Pastry system in Fig. 2.³ We have the following observations:

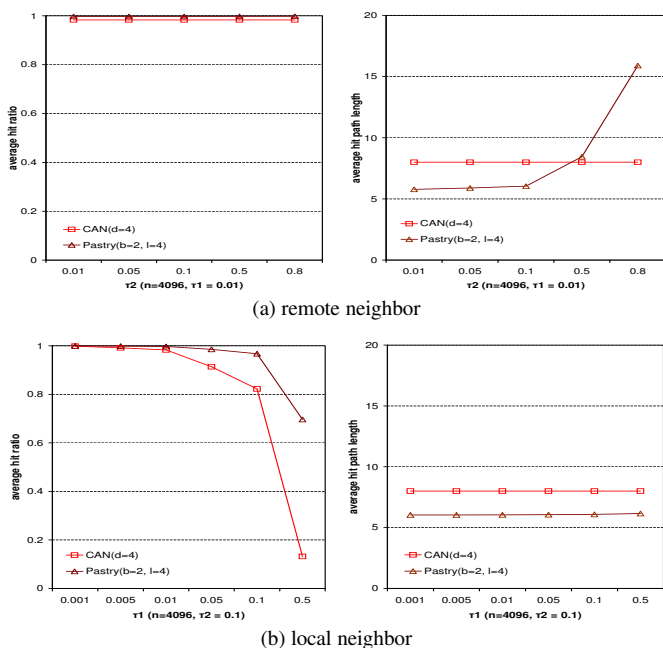


Fig. 2. Performance evaluation of resilience to failure

- The *average path length* is very sensitive to the failure of *remote neighbors*, but the *average hit ratio* is not.⁴ Hence, the *remote neighbors* have significant impact on resilience in terms of the *average path length*.
- The *average hit ratio* is very sensitive to the failure of *local neighbors*, but not the *average path length*. Hence, the *local neighbors* have significant impact on resilience in terms of the *average hit ratio*.

³We choose $n = 4096$ for CAN and Pastry. We choose the dimension $d = 4$ for CAN, the base $b = 2$ and leaf set size $l = 4$ of Pastry.

⁴Note that CAN has no remote neighbors.

B. Resilience to Routing Attack

There are different formats of routing attacks [3]. However, the common point of such attacks is forwarding the query to some node incorrectly, aiming to delay the receipt of the query or even to congest and damage the P2P system. It is very difficult, if not impossible, to analyze all the possible routing attacks. We define a so-called *super routing attack*. We use this to represent the worst form of incorrect routing. Under this attack, the malicious nodes tend to pick the farthest node (to the destination) from their routing tables for detouring the request. Obviously, in terms of attack damages, the super routing attack is the upper bound of all the routing attacks. In this study, we analyze P2P systems under such a routing attack. We assume that there is no malicious dropping, *i.e.* $P_d^m = 0$.

Similar with the analysis on failures, the transition probabilities for CAN system under attack are, for $i = 1, 2, \dots, n-1$,

$$p_{i,j} = \begin{cases} (1 - P_f^m)/|N(i)|, & j \in N(i) \\ P_f^m/|W(i)|, & j \in W(i) \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

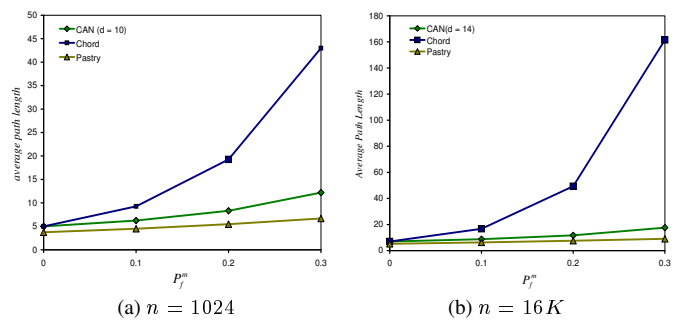


Fig. 3. Performance evaluation of resilience to super routing attack.

Fig. 3 shows the performance comparison in terms of average path length for systems of size 1024 and 16K. It can be seen from Fig. 3 that even though Chord performs well under normal conditions, its performance degrades dramatically under hostile conditions. This can be explained by the fact that among the three systems, only Chord follows uni-directional routing. CAN and Pastry can go either way they want. Thus Chord is more susceptible to hostile attacks, compared to CAN and Pastry.

IV. FUTURE WORK

The future work lies in two directions: i) Analysis: our approach can be applied to systems with relatively stable size and uniformly distributed nodes. It will be interesting to extend this approach to more complex and dynamic systems. ii) Enhancement: based on the analytical results, we have enhanced CAN system using small-world and Chord system by adding reverse edges. We are planning to investigate more systematical ways to enhance the resilience of the current structured P2P systems.

REFERENCES

- [1] Shengquan Wang and Dong Xuan, *A Markov-chain based Approach to Resilience of Structured P2P Systems under Failures and Attacks*, Technical Report, Department of Computer Science, Texas A&M University, <http://students.cs.tamu.edu/swang/papers/markovchain.pdf>.
- [2] Sylvia Ratnasamy, Scott Shenker and Ion Stoica, *Routing Algorithms for DHTs: Some Open Questions*. In Proc. of IPTPS, March, 2002.
- [3] E. Sit and R. Morris, *Security Considerations for Peer-to-Peer Distributed Hash Tables*. In Proc. of IPTPS 2002.