http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (19): 5195-5200, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5195.5200
© 2013 Asian Network for Scientific Information

Network Topology Based on Unstructured Mapping and Adaptive DHT IN P2P Network

Jirong Hu and Cong Wang
Hunan Information Science Vocational College, 410151, Changsha, China

Abstract: Distributed retrieval and routing algorithm based on adaptive DHT have better distribution, self-organization and scalability. These algorithms are becoming structured P2P network researches and application of international hot but relative to the traditional Client/Server network. The decentralization of the P2P network characteristics and the possibility of strong autonomy are dynamic nature of nodes in the network. They are making node implementation malicious behavior greatly increased which made the adaptive DHT node security requirements are difficult to meet. The study has presented adaptive security DHT protocol based on unstructured mapping mechanism. The mechanisms by identifier are grouped in the P2P network nodes are mapped to an unstructured mapping space and through the rational design of routing algorithms. The security work has positioning to the relatively simple node area. Theoretical analysis and experimental results show that this mechanism can be simplified existing adaptive DHT security mechanisms, effectively inhibit the malicious routing behavior to improve the success rate of the resource search.

Key words: P2P Network, unstructured mapping, routing attacks, adaptive distributed hash table, safety

INTRODUCTION

DHT (Distributed Hash Table) is a research and key technologies of structured P2P (Peer-to-Peer) network which uses the Distributed Hash algorithm to solve the structure of the distributed storage P2P network using DHT technology node peer and resources by Hash calculated relative to other nodes and resources unique identifier, its most prominent feature is the node does not need to record the entire network information but stores only with its own identifier specific node and resource information and resources according to the specific relationship search, thus eliminating flooding algorithm in unstructured P2P network to improve routing efficiency and reduce the routing network overhead. DHT-based distributed retrieval and routing algorithm, with its good distribution, self-organization, scalability, etc. DHT technology is becoming a hotspot of structured network research in the field representative study P2P network research and application (Rescorla, 2006) projects, including MIT Chord, Pastry, of Microsoft). At present, based on the DHT-structured P2P network research in the field representative study projects, including MIT Chord, Pastry, of Microsoft Research and UC Berkeley, CAN, Tapestry (Holohan and Schukat, 2010).

However, the correct operation of the premise of DHT mechanism nodes in the system can be trusted, that have high requirements for the security of the node relative to the traditional C/S (Client/Server) network (Hu *et al*., 2010).

UNSTRUCTURED MAPPING MECHANISM DESCRIPTION

This section first the typical malicious node behavior for example and then on this basis leads to the unstructured mapping mechanism to improve the specific principles of DHT security and measures (Marti *et al*., 2005).

Malicious routing case analysis example: In order to meet the structured P2P network scalability the maintainability and found that the requirements of the efficiency of the algorithm. DHT agreement provides for a small number of nodes in each node stores only network which led to the node network global information the lack vulnerable to malicious routing attacks.

Figure 1 has listed several possible routes attack, wherein the node Q to search the key the query information k (Search k), k information of the node B is responsible for storing the node A of the query information for the current network state where the correct routing immediate predecessor node to node B in the path when the node A will query the correct routing information to the node B, if the node B is a malicious

Corresponding Author: Jirong Hu, Hunan Information Science Vocational College, 410151, Changsha, China

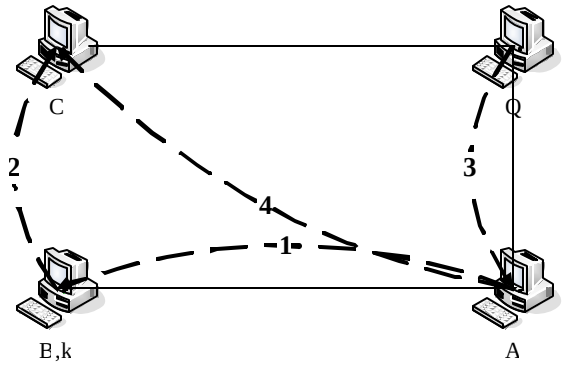

Fig. 1: Example of attack from DHT malicious routing

node, it may be: (1) To deny their storage k information discards the query message and returns the information of the lookup fails. (2) To deny their own storage k and continue to query information is routed to the next node C, failed to find the information returned by the C or its successor node if the node A is a malicious node. (3) A may discard the query and return to the lookup fails information; (4) A node error is routed to the correct destination node outside the scope of the query information and ultimately failed to find the information returned by the nodes receive the query (Hahm *et al*., 2005).

The analysis of the several possible routing attacks, it is not difficult to find the fundamental reason is that each node stores only a few nodes information which led to very limited transparency of information between nodes if the node Q, node A, B, C can get the stored the keys related information, then B can't be successfully implemented, such as (1), (2) The malicious behavior, Q, C and keys stored in the node A can be obtained related information, such as (3), (4) Routing attack also can not to the success of carried out (Sanchez-Artigas *et al*., 2008). But the number of node in the in P2P network is numerous, they have joined and the exit the operating frequent makes the node information sharing in the large within the scope is too difficult to achieve. The study has put forward to these problems. The study has proposed unstructured mapping mechanism, it will the node information and Inclusion problem naturalized to the relatively small node regional within DHT security mechanisms to be simplified.

The original node space S_1 (node identifier $p_{1l} \in \{p_{10}, p_{11}, \ldots, p_{1(n-1)}\}$, where n is the node space can accommodate the maximum number of nodes) in the relevant part of the operation of the remaining routing node $p_{1l} \in \{p_{a1}, p_{a(a+1)}, \ldots, p_{1b}\}$ is mapped to a relatively small space independent node, the node identifier $p_{2l} \in \{p_{20}, p_{21}, \ldots, p_{2(m-1)}\}$, where m can accommodate the maximum number of nodes and $m = 2^{[\log_2(b-1+1)]}$.

Unstructured space planning: Unstructured P2P network node resources are given corresponding identifier is calculated by the Hash function integer equal length and each node resource corresponding to the globally unique identifier, the identifier different from each other in the same structured P2P network node resource equal or closest to the node is responsible for storing the resource identifier for the key information about the distribution of resources in the network by a node identifier and key while successful search network resources. Query information can be properly routed to the node is responsible for storing the resource by the node to return its information (Yu *et al*., 2009). Based on the grouping of nodes resources identifier (as in Rule 1) and proposed the corresponding mapping mechanism to achieve the division of the unstructured space (as in Rule 2).

Rule 1

Packet identifier: Let identifier length is n bits, divided into m groups. Each group corresponding to the length of p_i bits, where I??[1, m] that satisfy the formula of:

$$\sum_{i=1}^{m} p_i = n, (1 \le i \le m)$$

Rule 2:

Unstructured space mapping: i dimensional space corresponding to the identifier of the group of $[p_i, \ldots, p_m]$. The i dimensional space contains the number of nodes:

$$s_i \le 2^{n-\sum_{j=1}^{i-1} p_j}$$

or:

$$s_i \le 2^{\sum_{j=i}^{m} p_j}, (1 \le i \le j \le m)$$

It is below in conjunction with Fig. 2 of the rules and rules interpretation. Order the node is mapped to a relatively small area, thereby simplifying the DHT security mechanisms. We first grouping operation identifier, group i corresponding to the length for the p_i bits, where $i \in [1, m]$, m for the pair identifies character divided by the total number of groups and then in accordance with the mapping space corresponds to the node gradually narrowing the scope of the principle. The diminishing number of identifiers allocated for the mapping space group. The i-dimensional space corresponding to the identifier length:

p1, p2, p3, ……pm(1st dimensional space)
p2, p3, ……pm(2nd dimensional space)
p3, ……pm(3rd dimensional space)
……
pm (mth dimensional space)

Fig. 2: Principle of unstructured mapping mechanism

$$n-\sum_{j=1}^{i-1}p_j(1\le i\le m)$$

or:

$$\sum_{j=i}^{m}p_j(1\le i\le j\le m)$$

and then nodeId of i dimensional space corresponding range:

$$\left(CurId,CurId+2^{n-\sum_{j=1}^{i-1}p_j}\right)(1\le i\le m)$$

or:

$$\left(CurId,CurId+2^{\sum_{j=i}^{m}p_j}\right)(1\le i\le j\le m)$$

(CurId enable spatial mapping mechanism node to nodId). One-dimensional space (i = 1) corresponding to the complete identity character, the initial the P2P topology of space. The unstructured space also has been known as multi-dimensional space (Yu, 2007).

Quickly location and initial security routing inspection mechanism: In order to effectively control the routing overhead introduced by the unstructured mapping mechanism, i.e. reduce the query message routing process with respect to the traditional DHT increased number of steps (hop count). One-dimensional space still adopt the traditional DHT routing mechanisms such as the use of Chord routing algorithm, the routing table of the node 1-dimensional space of the one-dimensional space corresponding to the one-dimensional ring is divided into n regions, n i.e. identifier length. With the P2P network line number of nodes N should satisfy the relationship n = floor(log N) (floor is the rounding function). The i-th area corresponding to the identifier range $[(nodeId+2^{i-1})mod2^n, (nodeId+2^i)mod2^n)(1\le I\le n)]$ and select the first online node as a routing query to the

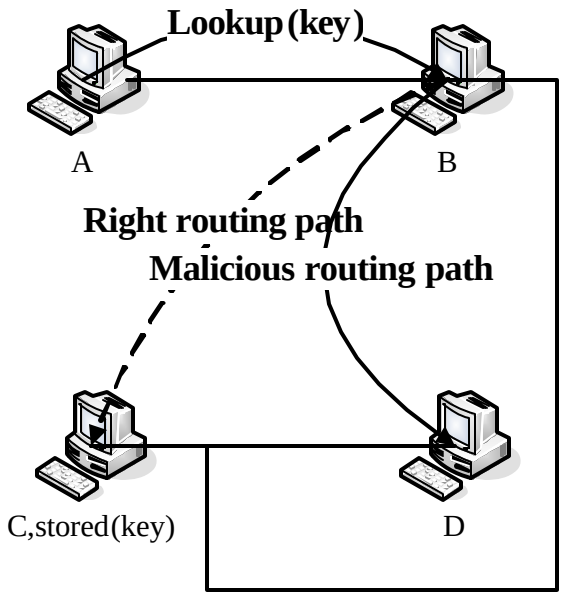

Fig. 3: Example of wrong routing

region information of the next hop node resource identifier for the key of the shared resource allocation information in the network by the first meet nodeId≥key node is responsible for storage (Xiong and Zhang, 2010).

On the basis of the mechanism, we have proposed the mechanism of initial security routing inspection mechanism in order to avoid security problems that exist in the traditional DHT routing process node routing of the initial security inspection mechanism for routing correctness of the received query information validation and as a judgment routing the query information is the basis of the first hop security traditional DHT agreement. When the node receives the resource query information forwarded by the previous hop, if its own identifier is still in the current routing algorithm initiates a resource query node identifier corresponding to query the resources corresponding to the identifier range between a next hop. The selection method had been used in accordance with the previous hop node resource query message continues backwards routing. If node now fall outside the identifier of the node corresponding to area, depending on the resource search fails to initiate the resource search operation node returns the query failure message. It is not difficult to see, the traditional DHT protocol of routing algorithm in order to the routing operations meet the requirements of the structured P2P routing efficiency in large-scale dynamic network environment. While ignoring some of the routing correctness of the necessary checks, the traditional DHT agreement vulnerable to malicious node implementation of routing attacks.

Figure 3 has listed a simple the misrouted phenomenon, node A has issued by the resource key

query information, the query and the information is forwarded to the node B. current network environment, the resource key distribution information in the network node C is responsible for storing. If the node B in the routing table according to the current network status update operation, yet the query routing and forwarding to the node D, the node D returns to A query failed, you can node B in this step-by-step routing operation malicious routing attacks worth noting here and can't simply be based only on the node B to node D in this step misrouted operation node B determines the malicious nodes, as described above, the node is not properly select a next hop node C may be this is also not the main reason for the introduction of a reporting mechanism in the course of the study of the method in DHT secure routing problem to solve because it is not timely update the status of the node C to its routing table.

EXPERIMENTAL COMPARISON AND ANALYSIS

To compare the test the traditional DHT load this study is based on the secure routing unstructured mapping mechanism, referred to unstructured Mapping Mechanism based on Secure Routing DHT average search success rate difference, this section first mentioned method is applied to traditional Chord protocol and then compared with the existing typical security methods, specifically selected redundant routing mechanism and reputation mechanism.

Compared with redundant routing mechanism: The Chord protocol had selected here as experimental subjects, analog node spatial scale for $N = 10^4$ node implementation of the malicious routing behavior normal circumstances, the probability p = 0, an average of 10 analog redundant routing mechanism and load unstructured mapping mechanism based on secure routing mechanism Chord group 1000 analog routing experiments.

Figure 4 is a the average find success rate in the course of the experiment and the average cost of the route statistical results shown in Fig. 4, when no the node embodiment malicious routing behavior in the analog network, both the average search rate close to the theoretical value of 0.5 but because of redundant routing mechanism using two routing path search of resources, so the average routing overhead is maintained at about two times the average routing overhead of the traditional Chord protocol this study unstructured mapping mechanism based on Secure Routing mechanism due to increased necessary safety Inspection measures the average routing overhead than traditional DHT increased slightly.

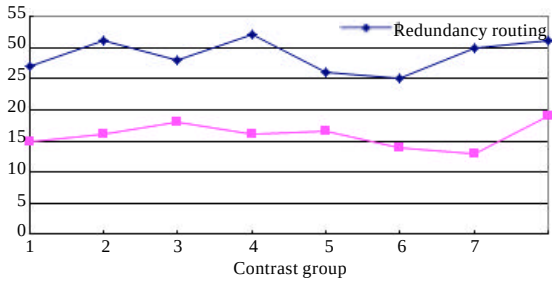

Fig. 4: 1st comparison between adaptive DHT security mechanism and redundancy routing mechanism

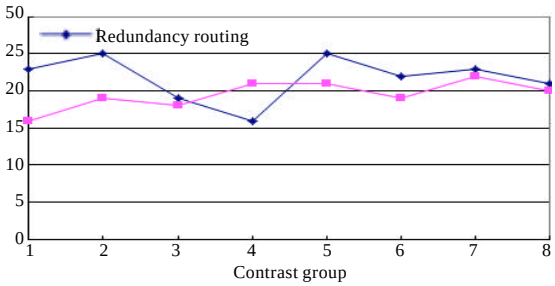

Fig. 5: 2nd comparison between adaptive DHT security mechanism and redundancy routing mechanism

It is described in Fig. 5 is malicious routing behavior when a node implementation probability p = 0.3 when both this part of the comparative study was designed to compare the results of the experiment, routing attacks defense the contrast unstructured mapping mechanism based on Secure Routing mechanism redundant routing mechanism effects and routing efficiency, malicious routing selected probability p = 0.3 is only the experimental results corresponding to the experimental parameters, there is no special meaning.

It is been shown in Fig. 5, when the node to participate in the routing process with probability p = 0.3 malicious routing behavior of embodiment, the redundant routing mechanism will result due to the two query paths by the routing attacks increases the probability of the final query success probability decreases and the unstructured mapping mechanism based on secure routing mechanism makes the entire routing process with strict safety inspection and corrective action Chord protocol did not show a significant decline in average search success rate than the normal case load of the security mechanisms for each resource search operation corresponding to the average routing overhead, as with the traditional DHT contrast experimental results, the average routing overhead of redundant routing mechanism is a direct result of malicious node forwards misrouted query fails than normal decrease, unstructured

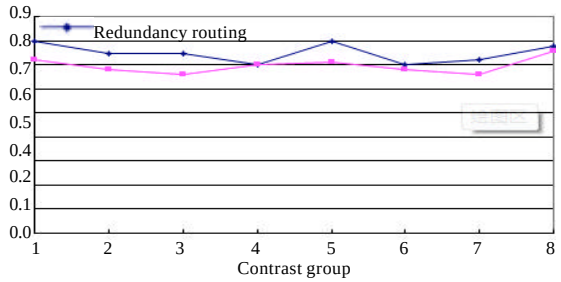

Fig. 6: Comparison between adaptive DHT security mechanism and creditworthiness mechanism

mapping mechanism based on Secure Routing mechanism due to the misrouted inspection and corrective measures, the implementation of a few routing number of steps.

The comparison of experimental results are shown that the proposed unstructured mapping mechanism based on secure routing mechanism for malicious routing attacks not only has a slightly better than traditional redundant routing mechanism research program-based defense effect and more effective control of the security measures the impact of the routing efficiency lower part with another typical routing security program credibility mechanism similar comparative experiments.

Comparison with the credibility mechanism: Unstructured mapping mechanism based on Secure Routing mechanism and credibility in the process of comparative experiments, still call unstructured mapping mechanism based on secure routing mechanism inspection routing the correctness API provide the basis for trust. The Fig. 6 is the Chord protocol average 1000 sets of experiments corresponding experimental results, experimental take the node implementation malicious routing probability p = 0.3 under the same experimental conditions, the credibility mechanism of this study unstructured mapping mechanism based on secure routing mechanisms have similar average query correctly but because of the credibility mechanism introduced for feedback node trust information reporting mechanism, the node to send information related to the traditional DHT routing algorithm but also to increase the trust of a large number of query, the trust reporting information, leading to node communication pressure also increases as shown in Fig. 6 as shown in the experimental network of the analog reputation mechanism average number of messages sent per second for each node how much about 130, simulation experiments load unstructured mapping mechanism based on Secure Routing mechanism, this value is only about 50.

CONCLUSION

This study has proposed the new security used adaptive DHT based on unstructured mapping mechanism, the mechanism through identifiers are grouped, the introduction of unstructured space is divided mechanism in the P2P network nodes are mapped to a unstructured space and through the rational design of routing algorithms, malicious routing behavior effectively inhibit the case of safety to relatively simple node region. The experimental results show that this mechanism can be simplified existing DHT safety mechanism, in the traditional DHT on the basis of introducing a small amount of overhead work positioning, in order to improve the success rate of the effect of resource search.

REFERENCES

Hahm, S., Y. Jung, S. Yi, Y. Song, I. Chong and K. Lim, 2005. A self-organized authentication architecture in mobile ad-hoc networks. Proceedings of the International Conference Information Networking: Convergence in Broadband and Mobile Networking, January 31-February 2, 2005, Jeju Island, Korea, pp: 689-696.

Holohan, E. and M. Schukat, 2010. Authentication using virtual certificate authorities: A new security paradigm for wireless sensor networks. Proceedings of the 9th IEEE International Symposium on Network Computing and Applications, July 15-17, 2010, Cambridge, MA., USA., pp: 92-99.

Hu, J.L., X.H. Li, B. Zhou and Y.H. Li, 2010. A reputation based attack resistant distributed trust management model in P2P networks. Proceedings of the 3rd International Symposium on Electronic Commerce and Security, July 29-31, 2010, Guangzhou, China, pp: 237-241.

Marti, S., P. Ganesan and H. Garcia-Molina, 2005. DHT routing using social links. Proceedings of the 3rd International Workshop on Peer-to-Peer Systems III, February 26-27, 2004, La Jolla, CA., USA., pp: 100-111.

Rescorla, E., 2006. Introduction to distributed hash tables. IETF-65 Technical Plenary, pp: 130-138.

Sanchez-Artigas, M., P.G. Lopez, A.F.G. Skarmeta, 2008. Bypass: Providing secure DHT routing through bypassing malicious peers. Proceedings of the IEEE Symposium on Computers and Communication, July 6-9, 2008, Marrakech, Morocco, pp: 934-941.

Xiong, Z.G. and X.M. Zhang, 2010. Resource management architecture and genetic ant algorithm for P2P grid system. J. Comput. Inform. Syst., 6: 79-88.

Yu, M., M.C. Zhou and W. Su, 2009. A secure routing protocol against Byzantine attacks for MANETs in adversarial environments. IEEE Trans. Veh. Technol., 58: 449-460.

Yu, Z.H., 2007. Analysis of malicious behaviors in peer-to-peer trust model. Comput. Eng. Appl., 43: 18-21.