Analysis for ALTO privacy and load issues
draft-wang-alto-privacy-load-analysis-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 19, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info).
Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

The goal of Application-Layer Traffic Optimization (ALTO) is to provide guidance to applications, which have to select one or several
hosts from a set of candidates, which are able to provide the desired
resource. Now the members in alto group propose many solutions, such
as P4P and PROXIDOR. These solutions still have unsolved problems
regarding privacy and workload. The privacy and load issues are
crucial aspects for the benefits of ISP and P2P. This draft is to do a
comparative study to analyze and compare the privacy and workload of
several existing solutions, hence to provide guidance in order to
improve, optimize and deploy the protocol.

Table of Contents

1.  Introduction ................................................. 3
    1.1.  Overview ............................................. 3
2.   Terminology and Concepts ................................. 4
3.   Privacy consideration ...................................... 4
    3.1.  ISP privacy .......................................... 4
    3.2.  P2P privacy .......................................... 5
4.   Workload considerations ................................... 5
    4.1.  ISP load ............................................. 5
    4.2.  P2P load ............................................. 6
5.   Solution space analysis .................................... 6
    5.1.  Solution 1 ........................................... 7
    5.2.  Solution 2 ........................................... 7
    5.3.  Solution 3 ........................................... 7
    5.4.  Solution 4 ........................................... 8
    5.5.  Solution 5 ........................................... 10
    5.6.  Merged solutions ..................................... 11
    5.7.  Conclusion ............................................ 11
6.   Security Considerations .................................. 12
7.   IANA Considerations ...................................... 12
8.   References ............................................... 12
    8.1.  Normative References ................................ 12
    8.2.  Informative References .............................. 12
8.   Authors’ Addresses ....................................... 13
1. Introduction

Many Internet applications, including the widely used overlay applications like peer-to-peer file sharing and video streaming, need to access the resources which are available in several equivalent replicas on different hosts, such as pieces of information or server processes. The goal of Application-Layer Traffic Optimization (ALTO) [I-D.ietf-alto-problem-statement] is to provide guidance to applications, which have to select one or several hosts from a set of candidates, which are able to provide the desired resource. is to provide guidance to the applications, which have to select one or several hosts from a set of candidates, which are able to provide the desired resource.

This memo discusses the privacy and load issues which are important for the benefits of ISP and P2P. Although these issues have been extensively discussed on the ALTO mailing list, ALTO WG is still lack of an ideal solution satisfying all the requirements. PROXIDOR, P4P and other similar solutions all have their pros and cons regarding all these aspects. This draft is to do a comparative study to analyze and compare the privacy and workload of several existing solutions, hence to provide guidance in order to improve, optimize and employ the protocol.

1.1. Overview

The essential reason for risks in privacy consideration is that the ISP and P2P can not trust each other fully. Network inefficiency caused by the emerging P2P applications challenges the Internet traffic controlled by ISP. Network providers have tried various traffic control techniques including charging and rate throttling. However, different P2P protocols may use different encryption and dynamic ports to avoid being identified and message types are also various. Furthermore, unilateral rate limiting by network providers may significantly degrade P2P performance and be problematic with consumers’ needs. ISP will also face the legal suits from its customers if it blocks the traffic.

ALTO proposes an ISP-P2P cooperating method to solve the network traffic problem. The first issue for P2P applications to be considered when using ALTO is whether ALTO can improve their performance in a safe way. In ALTO’s idea, P2P is guided by ISP in peer selection. Some experiments, such as P4P field test, shows that P2P performance can be improved in many aspects such as downloading speed. But in terms of privacy, existing solutions have the problem that they need some P2P operation information, to provide guidance accordingly, and it is easy to figure out P2P traffic from this information. If ISP wants to shape this traffic, P2P applications
can do nothing. On the other hand, though ISP has high pressure in P2P traffic optimization, providing guidance means disclosing part of their privacy information, which may lead to lots of attacks or other risks. Moreover, providing new service introduces new costs to ISP. Due to the huge number of peers, ISP servers need high capability and optimal designation to provide ALTO service. Existing solutions such as P4P, PROXIDOR have their strong points and weak points regarding these aspects.

2. Terminology and Concepts

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

This document also reuses the concepts defined in [I-D.ietf-alto-problem-statement] and [I-D.ietf-alto-reqs].

3. Privacy consideration

As declared in ALTO problem statements [I-D.ietf-alto-problem-statement], ISPs are required to provide their intimate knowledge of their network topology to address the ALTO problem. However, they usually think the revealed details of such network information are confidential. On the other hand, the ALTO client needs to provide some data that they think private in its query to the ALTO server, which could help to increase the accuracy level in the replies. Thus, the privacy issues need to be considered in ALTO protocol design.

3.1. ISP privacy

The security issue of ISPs concerns the potential risk of disclosing network topology and provision information through peer locations and the costs among peers. ISPs must evaluate how much information to reveal and the resulted risks. For example, if an ISP reveals extremely fine-grained information, it may be easier for attackers to infer network topology information. ISPs should also take into account that revealing overly coarse-grained information may not provide much benefit to either themselves or applications. If ALTO fails to improve the performance of P2P applications, it will not become popular and be used by the P2P community. Even using authentication or encrypt techniques, the ISP privacy can still be gotten by P2P applications. It can resolve the security problem of information transformation and security problem of server and client, but not the problem of privacy disclosing. Thus in
The defined protocol is required to support different levels of details in queries and responses, in order that the provider of an ALTO service can be able to control the amount of disclosed information (e.g., about the network topology).

### 3.2. P2P privacy

In some existing solutions, in order to obtain the ranking of destination peers for a source peer, P2P applications need to send the source and destination peer pairs to ALTO server. In this way, ISP can easily infer the communication pattern so that P2P traffic may suffer from rating or limiting actions from ISP. It is important to note that there is no protocol mechanism requiring ALTO for P2P applications. If P2P applications were required that the clients send their operational information to the server, they may be agitated by disclosing their information and ALTO service will be discarded. Thus different levels of details in queries and responses also need to be supported in requirement of user privacy protection, in order to protect the privacy of users, to ensure that the operators of ALTO servers and other users of the same application cannot derive sensitive information.

### 4. Workload considerations

In the ALTO problem statements and requirements, the overload protection and caching mechanism are required for ALTO protocol. However, if overload happens frequently, even with protection mechanism, it will cause bad performance of P2P applications and also ISP network.

#### 4.1. ISP load

The amount of peers an ALTO server needs to deal with could be millions. Especially in some busy time, ALTO server may receive millions of requests from the client at the same time. It causes overload of servers without high capability. Therefore, the solution should be highly scalable when the number of clients increases fast.

Assuming that there are n peers which are separated into t groups (one PID per group) requesting ALTO service at one time, if there are m candidates in average for each request peer, for PROXIDOR n times sorting are needed and for P4P n times IP-PID mapping and t*t times pDistance mapping are needed. Therefore, ALTO server should be charge with a huge n of requests at the same time and also should be deal with the continuously growing n.
4.2. P2P load

Using ALTO services, P2P applications should request and make use of ALTO guidance for each peer selection. The cost is higher than random peer selection. But comparing to some unilateral traffic optimization methods, because P2P applications do not need to estimate the network traffic, its cost is lower.

5. Solution space analysis

| IP mapping | -> | cost of IP-pairs | -> | ranking | -> | peer selection |

Figure 1. Basic process of P2P guidance

The goal of P2P guidance is to provide the ranking of the destination peers. The basic process of P2P guidance can be summarized as follows: first find the groups that the requested source and destination peers belong to; then calculate or search the cost of source and destination groups, maybe with consideration of some peer attributes as the cost of source and destination peers; then sort the costs and at last select peers according to the ranked costs. Here, 'group' is a set of peers defined by ISPs for the purpose of aggregation under similar network characteristics. Most solutions use this process with different group granularities. Finer gain of group granularity, such as one peer per group, performs well but costs more whereas coarse gain may lead to less effective guide. In the second step, the cost between source and destination groups can be prepared in advance or calculated on the fly. Due to the low efficiency and poor performance of real time computation for huge requests, the popular way is to calculate the cost of each peer pair/group pair in advance and maintains a back-end database that updates at pre-determined intervals or sudden changes. Even though, for each request the server has to do lookup from group pairs to their cost.

The ALTO server and client play different roles in these steps. In different solutions, the server has different number of functions, leading to different level of ISP and P2P privacy disclosing and server load. Assuming that a function is only provided by ISP or P2P, there will be five potential/existing solutions that support ALTO service.
Figure 2. Potential/existing solutions

5.1. Solution 1

An extreme way is that the ISP server charges all the process. In this case, ISP directly forces P2P to select the peers it chooses. Undoubtedly, all the topology information can be kept in the server side, but the P2P applications lose their independence and the ISP server may be overloaded with too much work. This solution is not reasonable.

5.2. Solution 2

Similarly, if P2P applications charge all the process with the primal topology information, ISP may suffer from the risks caused by privacy exposition. It is also unreasonable.

5.3. Solution 3

The acceptable solution is to find a strategy to divide the functions to server and client. One solution is the server controls the first three steps of the process and the client controls the last one. A representative example is PROXIDOR. To use the PROXIDOR service, the client generates a standard PROXIDOR query and sends to the PROXIDOR server. The PROXIDOR server that receives a query will rank the target IP address and then send back to the client.
PROXIDOR Server               Client
|                                 |
| Retrieve candidate peer list    V
|                                 |
<---        ----Ask for ranking
Sort the list                     |
Send ranked list----    --->            |
                        V
Peer selection

Figure 3. Basic flow of PROXIDOR

The client can get the ranked destination peers directly. ISP’s privacy is kept because it is difficult to collect all costs of the N*N IP pairs for an N IP network. It therefore has the advantage that all operational information is kept in the ALTO server and is not revealed to the ALTO client. But P2P applications should provide all potential source and destination peer pairs. PROXIDOR requires the exact destination peers per each source peer for sorting. ISPs can be able to infer the communication patterns of a client from the queries. P2P may be afraid of the privacy exposition so that not so many P2P applications choose it.

In addition, similar to taking all functions in the server, this kind of 3-1 partition solutions may also have the risk of overload. When various P2P applications request ALTO services simultaneously at hot time without caching, it is hard for the server to deal with the huge requests. Even using caching, direct using IP for ranking requires the cache mechanism to be design carefully.

5.4. Solution 4

Another solution is to distribute the first two functions to the server and the others to the client, which is represented by P4P. In P4P, the server controls the first two steps of the process. The client queries the server and gets the group ID (PID) for peer, and directly requests and obtains the cost/priority between source and destination groups (pDistance).
PID may disclose some location information. This depends on the type of PID, such as ASN. Though some services obtaining which AS an IP belongs exist, they increase the possibility of privacy exposition. The other indirect type may not have this problem. Through collection all (M*M for an N IP into M groups) or most pDistance may be obtained by P2P or other parties, a network topology may be disclosed. Obviously, it is easier than PROXIDOR to infer a network topology. However, if the reconstructed information can be obtained by the other ways (e.g. traceroute), it does not need to be taken into account much.

In P4P, Clients can potentially disclose private information to the ALTO Service Portals if either PIDs are extremely fine-grained or
Network Location Identifiers are included directly in the query. One possibility is that clients only retrieve the full set of PIDs (via GetPIDMap) and pDistances (via GetpDistance). Without knowing which one the source/destination is and how they link, it is hard for P2P traffic to trace for each link. But it increases the risks of disclosing ISP privacy on the other hand. In this way, other people can easily access all pDistances to construct a topology on group level. Granularity of group decides the probability that ISP and P2P privacies expose to some extent.

Regarding the traffic load, it is obvious that clients charging ranking step disperses the ranking cost from small numbers of servers to large number of clients. Although the ranking cost is very low for each peer, cost of millions of ranking altogether can not be neglected and the delay issue should also be considered. Moreover, because using group ID to request cost directly can reduce the request time significantly, it can also reduce the server load. If there are averagely X peers in a group, then the time of request may decrease to 1/X or more. If ISP provides full network map and cost map directly, the server’s workload could be reduced more. Most time it only needs to response to some timely requests.

5.5. Solution 5

In the case that P2P and ISP can not fully trust each other, another possible way is to provide necessary ISP information for P2P guidance without requesting P2P’s operational information. Comparing with other solutions in the figure, the characteristic of the last solution is that the server controls the first step and the client gets the costs of peer pairs, sorts the cost and then does the peer selection only according to group IDs. In other solutions such as 2-2 partition, the group ID denoting Network Location Identifiers can not represent cost relationship without a cost map. Instead, in this solution the group ID for a peer could be used as the carrier which also implies the cost to the other peer indirectly.

In section Section 5.4, 2-2 partition solutions such as P4P uses two steps to guide P2P: obtaining PIDs for the source and destination peer, and getting pDistance between the source PID and destination PIDs. Incorporating the two steps in P4P, in 1-3 partition solution ISP guides P2P through PID/group ID only. First ISP uses full set of pDistance to construct the set of PIDs. These PIDs are only a set of ruleless numbers, but from simple calculation with two PIDs the pDistance between these two PID could be obtained. In this way, the same performance as P4P could be obtained and the requests of getting pDistance could also be avoided. ISP doesn’t need P2P operational details, which can reduce the risk of disclosing P2P privacy. Even in the structured P2P network, some surrogate or transfer mechanisms
can be used to avoid source peer information being disclosed. Although the ISP topology information can be inferred by the full collection of PIDs as P4P, a correct computational function or driver still need to be obtained additionally to calculate the corresponding cost value. Moreover, the load on the ALTO server can be re-balanced to ALTO server and ALTO clients together.

The methods for constructing PIDs from pDistances are various, which can be freely adopted by ISP. The most appropriate PID type needs to be further verified.

5.6. Merged solutions

The solutions discussed above are just simple classification. A function may have different criterions and implementations in different solutions. And a function may be charged not by ISP or P2P alone. A cooperative way and a reliable third party can also be a reasonable manager. A merged solution may satisfy different requirements. For different P2P applications ISP can provide different solutions according to their credits or other stipulations. But this kind of merged solutions should be designed carefully to make the protocol in phase. Furthermore, the merged solutions may have the cons of the individual solutions. Of course, good combinations can make them complementary to each other and improve the advantages of protocol. However, providing multiple solutions simultaneously will result in the increase of workload. Moreover, aggregation of multiple solutions may introduce privacy concern of these solutions which increase both ISP and P2P privacy risks in the merged protocol.

5.7. Conclusion

In most cases, the more functions the ISP controls, the more cost the ISP spends and the less privacy the ISP discloses, but more P2P information is needed. On the other hand, if P2P controls more functions, P2P information may not be open to ISP, but it means that ISP may have to provide some sensitive information to P2P. In conclusion, the protocol should provide at least the basic mechanisms to deal with the privacy issue and it should be scaleable. The requirements [I-D.ietf-alto-reqs] for supporting mutual authentication of clients and servers are declared. But it is not enough when clients prefer to avoid explicit authentication and have privacy related to a network location basis. Currently ISP and P2P can not trust each other completely for some reasons. P2P may want much guidance which is sensitive to ISP. On the other hand, the protection of ISP privacy may damage P2P privacy and lead to server overload. Such conflictions should be solved, so there are implications cannot be ignored. Such mechanisms should reach a
balance between the benefits and requirements of ISP and P2P.

6. Security Considerations

The security issues have been taken into account in design considerations. An ALTO Server may optionally use authentication and encryption to protect ALTO information. Note that it can only prevent the information being disclosed on the path, but cannot prevent the information being redistributed by P2P applications. This will be further discussed in other documents.

7. IANA Considerations

There is no IANA action required by this draft.

8. References

8.1. Normative References


8.2. Informative References

[I-D.ietf-alto-problem-statement]

[I-D.ietf-alto-reqs]

[I-D.akonjang-alto-proxidor]

[I-D.wang-alto-p4p-specification]

draft-wang-alto-p4p-specification-00 (work in progress),
March 2009.

[I-D.penno-alto-protocol]
Penno, R. and Y. Yang, "ALTO Protocol",
draft-penno-alto-protocol-03 (work in progress),
July 2009.

[I-D.song-alto-server-discovery]
Song, H., Tomsu, M., Garcia, G., Wang, Y., and V. Pascual,
"ALTO Service Discovery",
draft-song-alto-server-discovery-01 (work in progress),
July 2009.

Authors’ Addresses

Yan Wang (editor)
Huawei
KuiKe Building, No.9 Xinxi Rd. Hai-Dian District
Beijing  100085
China

Email: wyan@huawei.com

Song Haibin
Huawei
Baixia Road No. 91
Nanjing, Jiangsu Province  210001
P.R.China

Phone: +86-25-84565867
Email: melodysong@huawei.com

Mach(Guoyi) Chen
Huawei
KuiKe Building, No.9 Xinxi Rd. Hai-Dian District
Beijing  100085
China

Email: mach@huawei.com