Efficient DoS-limiting Support by Indirect Mapping in Networks with Locator/Identifier Separation

Daochao Huang, Dong Yang, Hongke Zhang
School of Electronic and Engineering, Beijing Jiaotong University, Beijing, China
Email: {08111043, dyang, hkzhang}@bjtu.edu.cn

Fuhong Lin
School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China
Email: dr.lin.bjtu@139.com

Abstract—Recent research in the designing of an elegant mapping service to map identifiers onto locators in networks with locator/identifier separation, focuses on solving practical issues related to mapping system. However, how to provide entire secure support in separation networks is still an open issue. In this paper, we present the design and evaluation of a hierarchical indirect mapping system (HIMS). It provides indirect mapping from connection identifier (CID), a novel flat identifier space introduced to stamp packets, to endpoint identifier (EID), can limit the impact of full range of destination attacks such as Denial of Service (DoS) floods from the outset by EID hidden, and fulfills the requirements such as low latency, efficient network utilization and scalability. Based on an efficient merging rule, HIMS build a hierarchical Chord architecture which can scale to Internet level by preserving the locality and convergence of the inter-domain path. We present scalability assessment and numerical results to demonstrate the performance gains of the proposed approach.

Index Terms—Locator/identifier separation, connection identifier mapping, indirect mapping, Denial-of-Service, hierarchical DHT

I. INTRODUCTION

It has been widely recognized that today’s Internet architecture is facing serious security problems. Two reasons lead to these security problems. First, the original Internet protocol stack design deliberately did not include solutions for security [1][2]. The original Internet architecture was designed to provide unicast point-to-point communication between fixed locations. This makes traditional Internet vulnerable to destination attacks, such as denial of service (DoS) and distributed denial of service (DDoS) [6][7]. Because packets transferring across the Internet encapsulate the source and destination IP addresses in their headers, the malicious nodes can easily capture data packets and launch attacks. Second, the trend toward network-based Cloud computing is driving security concern more seriously [3][4][5]. With the success of cloud computing, the Internet is increasingly a platform for online services—such as Web search, social networks, and video streaming—this makes people fetch services more convenient while leading to more security issues.

During the last few years, there has been a considerable number of proposals to address security issues, for a partial list of proposals, consider [8][9][10]. However, most existing security approaches rely on adding overlays to current Internet architecture, while these proposals achieve the desired functionality; they do so in a very disjointed fashion in that solutions for one service are not solutions for other services. So far, none of the proposals are centered on the idea of providing a novel entire secure Internet architecture which includes inherent security mechanism.

In this paper, we base on two recent proposals, the locator/identifier (Loc/ID) split routing architecture and identifier mapping system. The Loc/ID split, by [11], provides a clean-slate redesign of Internet architecture which is introduced to resolve traditional Internet architecture design problems, such as semantic overloading of IP address, lack of mobility support and poor robustness etc. The most related representative approach is LISP [12]. Both of these studies provide a Loc/ID split mechanism to solve the scalability issue of current Internet routing and addressing system.

The service identifier mapping system, SIDMAP [13], is a proposal to effectively resolve a service identifier (SID) to end-point identifier (EID) in Loc/ID separation networks when users want to apply to services identified by the SIDs. The SIDMAP consists of resolvers and a Chord-based mapping system. The Chord-based mapping system is an overlay network and comprises a collection of mapping servers that are used to store and retrieve SID-to-resolver mapping entries. A resolver stores and retrieves SID-to-EID mappings for end hosts and servers in its corresponding zone. With SIDMAP, both mapping resolution delay and maintain overhead are significantly reduced by multilayer cache mechanism and local entries update. Unfortunately, the basic SIDMAP is only designed to directly resolve a SID to one or more EIDs and unable to deal with the type of flooding denial-of-service attacks.
In order to fully support security isolation through mapping system, we introduce a new identifier space, connection identifier (CID), into Loc/ID separation networks and design a hierarchical Distributed hash table (DHT)-based CID-to-EID pair indirect mapping system (HIMS). We argue that HIMS, with some modifications to SIDMAP, could provide a DoS-limiting infrastructure for Loc/ID separation networks. To be effective, the HIMS system must satisfy several important goals for its users. It must be:

Secure: The HIMS should address destination attacks such as DoS, DDoS, making service providing and communication among users more secure.

Effective: The HIMS should enable a receiver to detect attack traffic without inflicting damage to other legitimate hosts and with litter overhead burden to receiver or routers.

Scalable: Based on Chord or any other DHT algorithms, HIMS should resolve mapping requests quickly without introducing unacceptable resolution delay even widely deployed in large-scale Internet.

Reliable: If one indirect mapping server fails to work, the HIMS should limit the impact of the failure, and provide stable mapping service to relevant legitimate communications.

The rest of the paper is organized as follows. Section II describes the relevant background and related work; While Section III presents a concrete design and implementation of an indirect mapping system. Section IV analyzes the scalability and performance of HIMS. Section V evaluates our approach through numerical results and Section VI concludes the paper.

II. BACKGROUND AND RELATED WORK

Our work encompasses Loc/ID separation architecture and many aspects of DoS limiting mechanisms. In what follows we first present the main ideas of Loc/ID split architecture, then summary some representative pieces of research closely related to our work.

A. The Main Ideas of Loc/ID Split

The namespace of current Internet, IP address, is used for two separate functions: 1) as an end-point identifier to uniquely identify "who" a device is; 2) as a locator for routing purposes, which describes "where" a device is attached to the network. This "overloading" of functions makes it virtually impossible to build an efficient routing system without forcing unacceptable constraints on end-system use of addresses. The Loc/ID split is introduced to split these functions apart by using different numbering spaces for EIDs and route locators (RLOCs). This decoupling yields several advantages, including improved scalability of the routing system through greater aggregation of RLOCs, persistent identity in the EID space and, in some cases, the efficiency of network mobility support. But while its benefits have been widely discussed, there has been less attention paid to the entire security approach that is key to Loc/ID split networks.

In the Locator/Identifier Separation mechanism Internet end-hosts depend on the network elements (routers) to look up the mapping between EID and RLOC. Typically, the mappings are stored in a distributed database called the mapping system, which responds to the lookup queries. Some prototype implementations such as, LISP-DHT [14] and DHT-MAP[15] have already been implemented.

B. Existing DoS Defence Mechanisms

In the area of DoS, many approaches have been proposed in the past, such as Ingress filtering[16], Overlay based filtering (SOS)[17], network filtering[18], Capability based approach[19], SIFF (Stateless Internet Flow Filter)[20]. Some of the proposals mainly focus on making all sources identifiable. For examples, Ingress filtering [16] discards packets with widely spoofed addresses at the edge of the network, and traceback uses routers to create state so that receivers can reconstruct the path of unwanted traffic. However, attackers may still launch packet floods with unspoofed packets under these solutions.

By giving legitimate hosts an authenticator off-line that permits them to send to specific destinations, SOS can block the attacking traffic from malicious attacker effectively. Besides, typically filtering mechanism is the most commonly used method. Unfortunately, these filters will block some legitimate traffic from the receiver because there is no clean way to discriminate attack traffic from other traffic, for example, ingress filtering suffered from the shortcoming that a single unprotected ingress allows remote spoofing. In summary, these approaches only address an aspect of the problem but not the entire problem, and they do not provide a complete solution by themselves. A robust and efficient systematic approach that overcomes the shortcomings of current packet filtering techniques by allowing destination to control what it receives and automatically validating senders without prior arrangement is needed.

Packet filtering is a traditional tool for migrating DoS flooding attacks: when a receiver does not want to receive traffic from a sender, it can request to install filters to block the traffic. However, existing packet filtering systems are rendered ineffective by source address spoofing because it is easy for attackers to spoof source IP addresses to evade attack detection and packet filtering in the current Internet. Source address spoofing also enables attackers to launch reflector attacks, in which the attackers can hide behind innocent sources and the attack traffic can be significantly magnified. Our solution to authenticate source addresses is using self-certified flat CIDs instead of IP addresses during communication process.

In [20], by enabling routers stamp packets with a key that reaches the receiver and is returned to authorize the sender, SIFF built a stateless Internet flow filter that can eliminate the separate overlay channel for request packets and per-flow state. However, the SIFF proposal suffered from the following weaknesses: 1) for efficiency, only short stamps (2 bits) embedded in normal IP packets were adopted, and thus potentially discoverable by brute-force attack. 2) Initial request packets are forwarded with low
priority. This allows malicious hosts to take over the connected links.

Capabilities are short-term authorizations that senders obtain from receivers and stamp on their packets. This provides the permission in the form of capabilities to those senders whose traffic it agrees to accept. Both capability-based and filter-based approaches are promising building blocks for DoS flooding defense systems. They both enable a receiver to control the traffic it receives, but differ dramatically in methodology. Under the DoS-limiting traffic validation architecture (TVA)[21], it is required that each packet carries unique capacities that are not easily forgeable or usable if stolen by other party. Routers on the path validate these "stamps" but are not required to trust the hosts. Through this way, capacities expire to control the flow to destination while causing little overhead both in computation and bandwidth. When the attack power is very low, filters are more effective than capacities, while combining with per-source-AS fairness, capacities might be more cost-effective than filters. However, traditional capability-based approaches leave many questions unanswered, such as how capabilities are granted without being vulnerable to attack.

III. DESIGN OVERVIEW

In this section, we present the main ideas of our design. The overall goal is to strictly hide endpoint identifiers so that two hosts can communicate despite attacks by other hosts using an indirect mapping. To this end, we start with the definition of connection identifier. We then introduce standard packets forwarding and routing with CIDs in Loc/ID separation network. Details of indirect mapping scheme are described finally.

A. The Definition of CID

We design connection identifier mapping servers as entities that offer CID-to-EID pair resolution services to Internet end-hosts. The corresponding identifier space needs to uniquely identify connection between the two sides of communication by using a unique, temporary, and global scope CID. The lifetime of a CID depends on the session length, that is, it starts when a connection is established and ends when the session finished.

CIDs have significant potential benefits compared to other schemes such as filters and capabilities. They do not require routers to participate in filtering unwanted packets using implicit features. However, to be viable as a DoS-limiting solution, CIDs must meet several implied requirements. First, they must be generated by destination and authenticated by indirect mapping system, so that they can be distributed to the sender and stamped on packets. Second, routers in Loc/ID separation networks must be able to verify CIDs through communicating with indirect mapping servers. Third, CIDs must expire so that a destination can cut off a sender from whom it no longer wants to receive packets, in other words, the lifetime of a CID is strictly limited in the session period. Fourth, CIDs is designed as flat, self-certifying identifier excluding any semantic information of the session. Finally, CIDs must add little overhead in the common case. The following CIDs’ format design is geared towards meeting these requirements.

CIDs is the cryptographic hash of the information such as sender’s EID, destination’s EID, timestamp and a small random number. We can summarize the format as follows:

| CID | hashid of EID, dest EID, timestamp, random number (160 bits) |

Figure 1. Format of CIDs

B. Packets with CIDs

With CID indirect mapping system, a typical session between a sender $H_s$ with $EID_s$ and a receiver $H_d$ with $EID_d$ is:

- $H_s$ sends a service request to Internet, asking for service from $H_d$. The Loc/ID split based network with CID indirect mapping system answers with a CID.
- $H_d$ sends traffic to $H_s$, with CID embedded in each packet.

All CID-stamped packets are piggy-backed into normal traffic between senders and receivers. We illustrate this through an example shown in Fig. 2, assuming that each AS has one or several HIMS servers that handle CID requests from its ITR/ETR and other ASes.

- Step1 A source host $H_s$ that wishes to require a service from a destination host $H_d$ sends a service request to its tunnel router $ITR$. This request includes the communication’s source and destination endpoint identifiers: $(EID_s, EID_d)$, the connection identifier CID and the payload data.
- Step2 The tunnel router $ITR$ resolves the identifiers $EID_s$ and $EID_d$ to corresponding locator $Loc_s$ and $Loc_d$. Then forwards the request including source and destination locators: $(Loc_s, Loc_d)$, the connection identifier CID and the payload data to the destination tunnel router $ETR$.
- Step3 The CID indirect mapping server in the destination $H_d$’s AS forwards an inter-domain HIMS request to the destination indirect mapping server of CID to resolve CID to corresponding
Finally, ETR forwards the request to the destination host.

The impact of destination attacks should be limited. In such attack, attackers send mass attack traffic to the target, congest the link to the target, and exhaust the target’s resources. We use CIDs instead of EIDs in core network to achieve EIDs hidden and limit the impact of destination attacks.

C. Basic Design of Indirect Mapping

There are several challenges in designing this indirect mapping system:

There must be a way for senders and receiver to request CID from mapping system, and such mapping system should ensures that the increased communication delays after CID notification are not significantly higher than the delays prior to existing approaches without mapping system. In our design, mapping system servers are organized as distributed system based on hierarchical DHT algorithm.

CIDs should be unforgeable, and ITR/ETR should be able to efficiently verify CIDs. We use consistent hashing function to generate a unique, temporary, and global scope Connection Identifier to ensure Unforgeability of CIDs as well as efficiency in CID generation and verification. The temporary characteristic indicates that the lifecycle of each CID is limited and only be used to identify one connection within a limited time period. Even if an attacker can obtain CIDs by pretending to be a good sender, it cannot abuse it later.

The CIDs generation and distribution should be bound in order to make mapping system scalable. In our design, each mapping server does not have to keep the global knowledge to locate the sender/receiver. We also designed an algorithm that uses distributed hash table to forward the request/response between multiple mapping servers to obtain the destination server of a CID.

Since CIDs have to be embedded into each packet, the header overhead should be minimized. We allow CIDs caching on mapping servers to significantly reduce the header overhead and mapping resolution delay.

To meet the requirements described above, we propose to use a hierarchical Chord ring in which CIDs are used as ChordIDs, and have domains create a local Chord ring for each of ASes (see Fig.3). As shown in Fig.3, The proposed two levels hierarchical indirect mapping system (HIMS) consists of low level components, local indirect mapping server (lIMS), and top level components, global indirect mapping server (gIMS). Such a deterministic approach allows the HIMS to benefit from following advantages: 1) Typically, inter-domain traffic accounts for a large proportion; hierarchical design enables mapping resolution delay decreases significantly with efficient caching and bandwidth usage. 2) The proposed approach can achieve good performance with limited costs. Due to large quantity of CIDs will exist simultaneously; the tradeoff between performance (e.g. resolution delay) and cost (maintenance overhead) needs to be considered. By reasonable design of merging multiple Chord rings, HIMS can use less resource usage to achieve the same performance. 3) The HIMS supports adaptation to the underlying physical network. One of the main challenges in Chord is that end-hosts have little control over the location of their connection identifiers. This is because mapping server identifiers are randomly chosen, and, therefore, mapping servers close together in the identifier space can be far apart in the underlying network. To solve this problem, locality and convergence of inter-domain paths are considered to adapt to underlying physical networks in HIMS. When the sender which starts the CID lookup and the destination indirect mapping server is in the same domain, then the lookup never leaves this domain. This is called locality of inter-domain paths. When different nodes from one domain A route to the same node in another domain, all the different routes exit the domain A through the same node. This node is the closest successor of the target node’s identifier in the domain A. This is called convergence of inter-domain paths. In view of above considerations, in HIMS, each lIMS x in one sub-Chord ring creates a link to a lIMS y in another sub-Chord ring if and only if:

- y is the closest IIMS that is at least distance $2^k$ away for some $0 \leq k < m$, where $m$ is the length of a CID.
- y is closer to x than any node in x’s sub-Chord ring.

Fig.4 depicts the merging process for lIMS 0 (in sub-Chord ring A) and lIMS 7 (in sub-Chord ring B). In view of merging rule described above, IIMS 0 links to IIMS 2 and 4, IIMS 7 links to IIMS 9 and 11.
Compared with two Chord rings, one local and one global, the proposed HIMS only needs 14 extra links while two Chord rings 32 extra links.

C. Registration of CID-to-EID pair Mappings

Whenever an end host wants to communicate with other hosts, it should obtain a CID from the proposed indirect mapping system. We take a classical client-server process for example to illustrate the steps of registration process of a CID in HIMS. Assuming that every service is accompanied by a metadata file that includes the server’s public key and as well as its digital signature over the publication data.

In HIMS, a registration process comprises the following steps.

- Step 1. When a sender (or client) wants to obtain a service, it first depends on third trusted parties such as Domain Name System (DNS) or SIDMAP for service retrieval and revocation, then resolves this service’s name to its EID using external, reliable mapping mechanisms (e.g. SIDMAP) in Loc/ID split based network (see Fig.5 (1)).

- Step 2. Instead of returning the resolution results to the client, the third trusted parties create a CID for the request which is used to stamp on subsequent packets of this session later and forward the CID with relevant information including source EID, destination EID etc. to the nearest lIMS server through the tunnel router (TR) which further resolves the endpoint identifier to its corresponding locators using mapping system such as LISP-DHT. The details of this process can be illustrated in Fig.5 (2).

- Step 3. When the lIMS server receives the message from the third trusted parties, it first check whether or not the CID belongs to its range according to Chord protocol. If it is the case, the lIMS is the destination IIMS of the CID which is responsible for creating a new CID-to-< EID_a, EID_d > and then storing in its local mapping table. After that, the lIMS needs to forward the mapping to the gIMS in the same AS. If not, the lIMS forwards the CID registration message to the CID’s destination IIMS and gIMS (see Fig.5 (3)). Both the destination IIMS and gIMS add a new CID-to-< EID_a, EID_d > mapping entry in their local database. Then, the CID is registered at top and low levels of HIMS simultaneously.

- Step4 The destination IIMS needs to answer the sender with the CID by distributing the CID to the sender and the required server simultaneously. After receiving the CID, the sender sends service request with the CID to tunnel router which is responsible for verifying and forwarding the packets to the server.

D. Resolving EID Pair for a CID

The steps of resolution process of a CID in HIMS are as follows:

- Step 1. The end host sends a message which includes the CID and payload data to its ITR to indicate that it will communicate with the destination network through that TR (see Fig.6 (1)).

- Step 2. When the ITR receives the message, it sends a mapping request to the lIMS in its domain. The mapping request should contain the CID information and some signature used for security (see Fig.6 (2)).

- Step 3. When the lIMS receives such a mapping request, it first finds in its local CID-to-EID pair mapping table whether there is a CID-to-EID pair for the required CID or not. If so, then directly return back resolution results to the ITR. Otherwise, the IIMS should forward the mapping request to its nearest gIMS that is closest to the destination gIMS (see Fig.6 (3)).

- Step 4. When the gIMS receives the mapping request, it first finds whether the requested CID is in its local domain. If so, returns the CID-to-EID pair mapping to the ITR. If not, the gIMS should forward the mapping request to its nearest gIMS that is closest to the destination gIMS (see Fig.6 (4)).

- Step 5. When the destination gIMS receives the mapping request, it sends the resolution result back to the ITR. Then, the ITR further resolves the EIDs to their locator and forwards the packet to...
the destination. In this transforming process, EIDs are replaced by the CID (see Fig.6 (5)).

- Step 6. When the packet is arriving at ETR, the ETR first sends a request to resolve the CID. HIMS resolves the CID, then forwards the packets to the destination (see Fig.6 (6)).

E. Security Primitive Provided by HIMS

DoS attack occurs when an attacker uses a thousand systems to simultaneously launch attacks against a remote host, and then floods the bandwidth or resources of a targeted host. The major advantages of an attacker of using a DoS attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. These attacker advantages cause challenges for defense mechanisms in traditional Internet.

The root cause of the problem lies in the IP address leakage. The original Internet architecture was designed to provide unicast point-to-point communication between fixed locations. In this basic service, the sending host knows the IP address of the receiver and the malicious node can easily obtain the IP addresses of sender and receiver, and then attaches a destination attack to the sender or the receiver. With HIMS, communication partners, neither clients nor servers, never know the exact access identifiers of each other, in other words, HIMS hides the identifiers of communication hosts. At the client, when a packet is sent out to local ITR, the source EID and the destination EID are \( \text{EID}_s \) and \( \text{EID}_d \) respectively. After local ITR receives the packet, it first extracts the CID and matches it with its cache entries of CID mappings, then forwards the packet to the destination indirect mapping server of the CID. The same process proceeds at the server. By EID hidden, communication security is provided as built-in function of HIMS in universal network. Instead of explicitly sending a packet to a destination using IP addresses or EID pairs, each packet is associated with a connection identifier; this identifier is then used by the sender and the receiver to obtain delivery of the packet. As a result, HIMS provides an efficient method to alleviate or, to some extent, eliminate DoS attack.

IV. SCALABILITY AND PERFORMANCE ANALYSIS

We give a preliminary and simplified assessment of the system scalability in terms of required number of world-wide HIMS servers. For this assessment, we assume a world-wide HIMS with two levels (gIMS, IMS). In order to store a binding record in a valid CID mapping table, it details a storage space of 4KB (\( >160 \) bits EIDsrc + 160 bits EIDdst + 8 bits CID +8 bits timestamp+ 16 bits random number etc.). Solid State Disk (SSD) memory instead of traditional hard drive is used to store these binding records to offer sufficiently fast access (15 \( \mu \)s, let \( \bar{W} \) denote the average sojourn time that equals to waiting time plus service time, then \( \bar{W} = 15 \mu \)s). Current state-of-the-art SSD storage servers have 4TB of memory [22]. Assuming that \( 10^{15} \) (=8.4 \( \times \) 109 indexed Web pages [23], about 109 connections per page) CIDs globally with mapping records of 4KB coexist simultaneously, and each gIMS can store 109 mapping records. Therefore, 109 indirect mapping servers are required for a world-wide HIMS with 1015 CIDs.

Typically, regular Chord is not equal to the number of routers since each hop on the logical, overlaying network connecting the Chord nodes may comprise of a number of physical communication links and their routers. HIMS efficiently solve this problem by implementing intra-domain paths locality and inter-domain paths convergence. To illustrate the efficiency of HIMS and analyze the performance, we present a modeling as follows: Given a random graph, the average number of routers between two peers in the network is given by [23]

\[
\langle d \rangle = \frac{\ln \left[ N_k - 1 \right] (\bar{z}_i + z_i) - \ln (z_i)}{\ln (\bar{z}_i / z_i)}
\]

where \( \bar{z}_i \) is the average number of hop neighbors and \( N_k \) is the total number of nodes in the router graph. Since the HIMS is implemented as a hierarchical Chord ring, the expected average number of routing hops between two nodes is \( \frac{1}{2} \log_2 (N - 1) + \frac{1}{2} \) with \( N > 1 \), where \( N = 2^n \) is the total number of HIMS servers. Therefore, each query is forwarded for \( \frac{1}{2} \log_2 (N - 1) + \frac{1}{2} \) hops with an average of \( \langle d \rangle \) routers per hop and assuming that the return path has an equal number of routers. The expected network delay of the resolution process is then

\[
E[T_{gs}] = \left( \log_2 (N - 1) + \frac{1}{2} \langle d \rangle \sum_{i=1}^{N_k} \left[ E[W_{t}] + \tau_i \right] \right) / N_k
\]

where \( \sum_{i=1}^{N_k} \left[ E[W_{t}] + \tau_i \right] / N_k \) is the average queuing delay at a router, and \( E[W_{t}] \) is the expected waiting time in the \( t \) th router which is given by [23] as follows:

\[
E[W_{t}] = \tau_i \rho_i (c_{w} + c_{z}^2) g_i / (2 - \rho)
\]

In which \( g_i = g_i(\rho_i, c_{w}, c_{z}) \) is defined as

\[
g_i(\rho_i, c_{w}, c_{z}) = \begin{cases} \exp \left( \frac{2(1 - \rho_i)(1 - c_{w}^2)}{3 \rho_i (c_{w}^2 + c_{z}^2)} \right), & c_{w} < 1 \\ 1, & c_{z}^2 \geq 1 \end{cases}
\]

The total average lookup latency of a request being resolved by HIMS is denoted as \( \bar{T} \), which is the sum of the average sojourn time and network delay. Thus,

\[
\bar{T} = \bar{W} \left( \frac{1}{2} \log_2 (N - 1) + \frac{1}{2} \right) + E[T_{gs}]
\]
V. Simulation Results

We evaluate the efficacy and scalability of the HIMS using numerical simulations. These simulations are based on the Chord protocol [25] and uses recursive style routing. We consider the following two network topologies in our simulations:

**Topology 1:** A real network topology generated with the kingdata [26] with 2501 nodes. In this topology, the distance between two DNS servers is used to simulate the distance of two indirect mapping servers. Therefore, the simulation results greatly reduce the deviation between simulation and real network because it includes a connection of real network RTT (Round-trip Time) values.

**Topology 2:** A power-law random graph topology generated with INET topology generator [27] with 16,384 nodes, where the delay of each link is uniformly distributed in the interval (1, 80) ms. The HIMS servers are randomly assigned to the network nodes.

Consider a sender $EID_s$ communicates with a receiver $EID_d$ via $CID_{sd}$. As discussed in Section 3.3, packets are routed in locator/identifier separation network with CID instead of EIDs, and then EID hidden is achieved to limit destination attacks such as DoS. During the communication process, mapping requests are sent to HIMS to resolve CID to its corresponding EID pairs. We use the ratio of the inter-node latency on the HIMS network to the inter-node latency on the underlying network to evaluate the routing efficiency of HIMS.

As shown in Fig.6, both in Topology 1 and Topology 2, the 90th percentile latency stretch can be reduced up to 1.5-3 times as compared to the default Chord protocol since intra-domain paths locality and inter-domain paths convergence are considered in HIMS.

To evaluate how efficiently our design choices use HIMS for better lookup performance, we introduce the average number of bytes sent per node per unit time as the cost metric. This cost accounts for all messages sent by a node, including periodic routing table refresh traffic, lookup traffic, and join traffic. The performance vs. cost simulation results are as follows:

VI. Conclusions

With the disadvantages of traditional Internet architecture becoming more and more obvious, a number of novel identifier split mechanisms are proposed so as to solve the issues mentioned above. However, most of these proposals cannot provide entire security support. In light of this issue, a novel secure hierarchical DHT-based connection identifier mapping system called HIMS is proposed in this paper, the basic idea of which is to set a connection of mapping servers that store CID-to-EID pair mapping entries for the corresponding CIDs. Using HIMS, terminals communicate with each other without knowledge of the correspondence node’s EID, so as to limit destination attacks such as DoS attack, providing security support in locator/identifier separation Network.

To demonstrate the feasibility of our approach, we have built a connection identifier indirect mapping system based on the hierarchical Chord lookup system. Preliminary experience with suggests that the system is highly flexible and provides secure, scalable and good worst-case lookup performance.

ACKNOWLEDGMENT

This work was supported in part by a grant from the National 863 Key Project (2011AA010701), and Basic Research Supporting of Beijing Jiaotong University (2009JBZ004-2).

---

Figure 6. The 90th percentile latency stretch in the case of (a) A real network topology generated with the kingdata with 2501 nodes, and (b) a power-law random network topology with 16384 nodes.

Figure 7. Performance vs. cost tradeoff in HIMS with 1024 servers.
REFERENCES


[27] http://topology.eecs.umich.edu/inet/

Dochoao Huang received the M.S. degree in communication systems from the Beijing Jiaotong University of electronic and engineering of China, Beijing, China, in 2007. Now he is a Ph.D. candidate of Beijing Jiaotong University. His research interests are in the areas of communication networks including cloud computing, data center and Next Generation Internet technologies.

Dong Yang received the M.S. and Ph.D. degrees in communication and information systems from the Beijing Jiaotong University of electronic and engineering of China, Beijing, China, in 2003 and 2008, respectively. His research interests are in the areas of communication networks including cloud computing, data center and Next Generation Internet technologies.

Fuhong Lin received the M.S. and Ph.D. degrees in communication and information systems from the Beijing Jiaotong University of electronic and engineering of China, in 2006 and 2010, respectively. He is a post doctor at University of Science and Technology Beijing. His research interests include social network, P2P network, and Future Internet technologies.

Hongke Zhang received M.S. and Ph.D. degrees in electrical and communication systems from the University of Electronic Science and Technology of China, Chengdu, China, in 1988 and 1992, respectively.

From September 1992 to June 1994, he was a Post-Doctoral Research Associate with Beijing Jiaotong University (BJTU), Beijing, China. In July 1994, he joined BJTU, where he is currently a Professor in School of Electronic and Information Engineering. He is also the Chief Scientist of the National Basic Research Program of China.