Adaptation method for video streaming over HTTP/2

Duc V. Nguyen\textsuperscript{1a)}, Hung T. Le\textsuperscript{1}, Pham Ngoc Nam\textsuperscript{2}, Anh T. Pham\textsuperscript{1}, and Truong Cong Thang\textsuperscript{1}

\textsuperscript{1} Computer Engineering Division, The University of Aizu, Tsuruga, Ik kimachi, Aizuwakamatsu 965–8580, Japan
\textsuperscript{2} School of Electronics and Telecom., Hanoi University of Science and Technology, 1 Dai Co Viet, Hanoi, Vietnam
\textsuperscript{a)} m5182102@u-aizu.ac.jp

Abstract: HTTP streaming, which is currently based on the pull-based HTTP/1.1 protocol, has a tradeoff problem between overhead and adaptivity. We propose an adaptation method for adaptive streaming over the new HTTP/2 protocol, leveraging its server push feature. The method is based on a cost function that takes into account the number of pushed segments and the client buffer level. Experiment results show that the proposed method can improve the balance between the number of requests and buffer stability compared to existing methods.

Keywords: adaptive streaming, adaptation, HTTP/2, server push

Classification: Multimedia Systems for Communications

References


1 Introduction

Dynamic and Adaptive Streaming Over HTTP (DASH) standard has emerged as a dominant standard for video streaming over the Internet, especially for mobile devices [1, 2]. For adaptivity to network fluctuations, a video is encoded in different quality versions, each is further divided into short segments. Currently, the target delivery protocol in DASH is HTTP/1.1, so each segment is delivered by a pair of request-response [2]. Usually, video segments have a fixed duration, typically from 2 s to 10 s [3]. Obviously, using a long segment duration would benefit from fewer requests, and so less overhead for client/server and networks. However, a long segment duration results in buffer instability [3] and large delay [4]. For adaptivity and low delay, one can use short segment durations; yet, this requires more requests. The overheads caused by using many requests are presented in [4, 5]. Specifically, the more frequently the requests are sent, the more the energy is consumed in mobile devices. Moreover, though having a small data size, each request should be processed by network nodes (e.g. proxies and servers) on the content delivery path. So, a huge number of requests will significantly increase the processing complexity of network nodes [5].

The recently ratified HTTP version 2 (HTTP/2) provides a new feature called server push [6], which is expected to reduce the request-related overheads [4, 5]. This feature, which allows the server to respond a request with multiple consecutive segments of the same version, enables the use of a short segment duration without having to use too many requests. In this trend, the ISO/IEC MPEG group is working on an extension of DASH, where an HTTP/2-based request can specify the number of requested segments [7]. Recently, the server push feature has been employed for low latency streaming [5] and low request-related overheads [6]. However, in the existing studies, the number of pushed segments per request is fixed and the considered network throughput is simply constant.

To the best of our knowledge, no previous work has adaptively decided the number of pushed/requested segments for a request. In this study, we propose a novel adaptation method for adaptive streaming over HTTP/2, under time-varying bandwidth. To find the optimal number of pushed segments for a given request, we define a cost function depending on two factors, which are request cost and buffer cost.

2 Proposed method

In general, a streaming client should 1) estimate the throughput and 2) decide the video bitrate for a request [2, 3]. In this work, we adopt the method presented in [3] to estimate the throughput. For streaming over HTTP/2, our goal is to decide the video bitrate and the number of pushed segments for a given request, so as to have a small number of requests and a good buffer stability.

Suppose that, after sending request $i-1$ (called the last request) asking for $N_{i-1}$ segments, the client has just received all $N_{i-1}$ requested segments, each has a duration of $\tau$ seconds. The current buffer level is $B_{i-1}$. Now, for the next request $i$, the client will decide the bitrate $R_{ij}$ and the number of pushed segments $N_i$. Here
$R_{ij}$ means the bitrate version $j$ ($1 \leq j \leq M$, where $M$ is the number of versions) decided for request $i$.

Denote $T_i$ the estimated throughput for response $i$, which is obtained by the method of [3], and $C$ the cost caused by a decision with $R_{ij}$ and $N_i$. Given the estimated throughput $T_i$, the current buffer level $B_{i-1}$, and the low buffer constraint $B_{low}$, the adaptation problem can be formulated as follows.

For the next request $i$, decide $R_{ij}$ and $N_i$ to minimize the cost $C$ which is a function of $N_i$ and $R_{ij}$

\[
C = f(N_i; R_{ij})
\]

subject to

\[
B_i \geq B_{low}.
\]

In this study, bitrate $R_{ij}$ is decided as the highest bitrate that is lower than $T_i$.

\[
R_{ij} = \max \{ R_{il} \mid R_{il} \leq (1 - \mu)T_i, \ 1 \leq l \leq M \},
\]

where $\mu$ is the safety margin ($0 < \mu < 1$) [1, 2]. After receiving $N_i$ requested segments, the buffer will have additionally $\tau \times N_i$ seconds of media. However, the transport time of those segments takes $(\tau \times N_i \times R_{ij})/T_i$ seconds. So $B_i$ can be estimated as follows.

\[
B_i = B_{i-1} + \tau \times N_i - \tau \times N_i \times \frac{R_{ij}}{T_i}.
\]

For the above goal, we define the cost function $C$ as a weighted sum of request cost $C_{rq}$ and buffer cost $C_{bf}$.

\[
C = \alpha \times C_{rq} + (1 - \alpha) \times C_{bf},
\]

where $\alpha$ is a weighting parameter. The request cost $C_{rq}$ is computed as a linearly decreasing function of $N_i$ as follows.

\[
C_{rq} = \frac{1}{N_i}.
\]

The buffer cost $C_{bf}$ is computed based on the following observations. First, a high value of $N_i$ would increase the chance that the buffer level reduces significantly when the throughput drops, so $C_{bf}$ should be proportional to $N_i$. Second, a higher buffer level helps the client tolerate throughput drops, and thus reduce $C_{bf}$. Consequently, $C_{bf}$ is computed by

\[
C_{bf} = \frac{N_i \times \tau}{B_{i-1} - B_{low}}.
\]

In our method, the decision based on (5)(6)(7) is applied when $B_{i-1} \geq B_{low}$. When $B_{i-1} < B_{low}$, the client switches to the so-called conservative mode. In this mode, if the throughput decreases, $N_i$ is set to 1; and if the throughput increases, $N_i$ is simply increased by 1 every two requests until $B_{i-1} \geq B_{low}$. As seen in the next section, our method rarely goes into the conservative mode.

As the problem space of this decision process is small, we apply a full search to find the best decision. Specifically, cost $C$ corresponding to each of the available values of $N_i$ is first computed using (5)(6)(7). Then, the one having the minimum value of $C$ and satisfying condition (2) is selected as the number of pushed segments for the next request. In our method, the first request asks for one segment (i.e. $N_0 = 1$) of the lowest bitrate version.
3 Experiment results

Our experiment test-bed is based on that of [1], with protocol updates to support HTTP/2. The client running the proposed method above is implemented in Java. The number of pushed segments is included in the query string of the HTTP/2 request. At the server, a video, consisting of 1000 segments with duration $\tau = 1$ s, is provided at 15 bitrate versions, from 200 kbps to 3000 kbps with a step of 200 kbps. The network is emulated using a real mobile bandwidth trace (Fig. 1) [8]. The maximum number of pushed segments is set to 4, $\mu$ to 0.1 and round-trip time to 100 ms. The proposed method is compared to push-$N$ method of [4, 5], in which $N$ ($1 \leq N \leq 4$) segments is pushed per request. The client buffer size is set to 16 s and $B_{low}$ to 12 s.

![Fig. 1. Mobile bandwidth trace](image1)

![Fig. 2. Resulting video bitrate and buffer level](image2)

For clarity, an excerpt of adaptation results from $t = 80$ s to $t = 110$ s is provided in Fig. 2, showing the resulting video bitrate and buffer level. The bitrate curve of our method with $\alpha = 0.6$, additionally attributed by $N_i$, shows that the
optimal value of $N_i$ is 2 before $t = 85$ s. As the throughput decreases, $N_i$ is reduced to 1 at $t = 91$ s. After that, $N_i$ is increased to 2 and then 3. Also, the decided bitrate closely follows the throughput. Thanks to this adaptivity, our method can help prevent buffer level drops as the throughput continues to decrease.

Meanwhile, with the push-$N$ method, only push-1 policy can provide a more stable buffer than our method; however, the number of requests almost doubles that of our method. All the other push policies are less responsive and result in less stable buffers. Our method with $\alpha = 0.6$ results in much fewer requests and a higher buffer level curve compared to the push-2, push-3, and push-4 policies.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Push-N method</th>
<th>Proposed method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of requests</td>
<td>Push-1 Push-2</td>
<td>Push-3 Push-4</td>
</tr>
<tr>
<td></td>
<td>1000 500</td>
<td>334 250</td>
</tr>
<tr>
<td>$p(B &lt; B_{low})$ (%)</td>
<td>0 0.4</td>
<td>2.1 6.4</td>
</tr>
<tr>
<td>Min. buffer level (s)</td>
<td>12.91 10.93</td>
<td>8.72 5.64</td>
</tr>
<tr>
<td>Avg. bitrate (kbps)</td>
<td>1529.8 1648.4</td>
<td>1674 1704.8</td>
</tr>
</tbody>
</table>

For overall statistics, Table I shows the number of requests, $p(B < B_{low})$ the probability that buffer level $B < B_{low}$, the minimum buffer level $B_{min}$, and the average video bitrate. Note that the first two parameters are the lower the better and the last two are the higher the better. It can be seen that push-$N$ method results in a poor tradeoff between requests and buffer stability. When $N = 1$, it is possible to achieve a stable buffer with $B_{min} = 12.91$ s and $p(B < B_{low}) = 0$. However, the client/server and networks must handle 1000 requests in this case. The number of requests can be as low as 250 (when $N = 4$) but the resulting buffer is very unstable, with $B_{min} = 5.64$ s and $p(B < B_{low}) = 6.4\%$. Meanwhile, our proposed method can provide much better performance. Specifically, with $\alpha = 0.6$, the buffer of our method is as stable as that of the push-1 policy while the number of requests is almost halved (i.e. 523). With $\alpha = 0.3$, in comparison to push-3 policy, the proposed method have higher $B_{min}$ and lower $p(B < B_{low})$ while the number of requests is just a little higher (348 versus 334). It should be noted that the average bitrate of our method is always comparable to or higher than those of the push-$N$ method.

The above results imply that our method can smartly change the number of pushed segments according to network fluctuations. Also, by adjusting the value of the weight $\alpha$, the tradeoff between the number of requests and buffer stability can be controlled.

4 Conclusions

In this study, an adaptation method for adaptive streaming over HTTP/2 has been proposed. This method employed a cost function of both the number of pushed segments and the client buffer level. The experiment results showed that our method improved the tradeoff between the number of requests and buffer stability by smartly changing the number of pushed segments.
Analysis of via-resolver DNS TXT queries and detection possibility of botnet communications*

Hikaru Ichise\(^1\)a), Yong Jin\(^2\), and Katsuyoshi Iida\(^2\)
\(^1\) Technical Department, Tokyo Institute of Technology, Japan
\(^2\) Global Scientific Information and Computing Center, Tokyo Institute of Technology, Japan
\(a)\) hichise@nap.gsic.titech.ac.jp

Abstract:Botnet involves various communication protocols and according to recent reports DNS TXT record has been used for botnet communications. However, we have never statistically analyzed the usage of DNS TXT record and the signatures of its malicious usage, thus, it is difficult to block out the malicious usage only. In this paper, we analyze the usage of the DNS TXT record and present statistical results obtained from more than 5 million real DNS TXT record queries with responses captured in our campus network for over 3 months. As a result, we filtered out 2,293 “Unconfirmed” usages of DNS TXT record queries and checked the queried domain name and the destination IP address in detail. Finally, we confirmed that it is effective to check the unknown usage of DNS TXT queries for detecting botnet communication.

Keywords:botnet communication, C&C, DNS, TXT record

Classification: Internet

References


*The paper has been presented in part at IEEE PACRIM 2015.
1 Introduction

Botnet, a logical network consists of many computers has become one of the most significant threats in the Internet. In botnets, attackers operate computers called Command and Control (C&C) servers to control a huge number of bot-infected PCs1 performing attacks such as SPAM e-mail distribution, malware distribution and Distributed Denial of Service (DDoS) attacks, etc.

In general, bot-infected PCs periodically communicate with their C&C servers for malware update and obtaining further instructions for successive attacks and we call this as botnet communication. So far there have several communication protocols such as IRC, P2P and HTTP used in botnet communication. From 2011, the usage of the Domain Name System (DNS) protocol had been detected in botnet communication is reported in some researches [1]. Since the DNS protocol is a fundamental communication protocol, therefore it is difficult to simply block out all DNS traffic.

Moreover, ref. [1] reported that some botnets use DNS TXT record in their botnet communications. Since there are also legitimate usages of DNS TXT record, we need to distinguish them from the usages in botnet communications. In order to distinguish the legitimate usages of DNS TXT record, it is necessary to be aware of the details of legitimate usages as well as those in botnet communications. We captured and analyzed the DNS traffics in our campus network which contains about 5.53 million query-response pairs during three months2. The analytical results confirmed that it is respectful to detect DNS based botnet communication by monitoring DNS TXT query and response in the DNS full resolvers of an organization.

2 Analysis of DNS TXT record usage

Although the major objective of the DNS system is to provide name resolution between hostname and IP address, it also provides some other supplementary functions using such as MX, TXT, SRV and other resource record types. As one of the unique resource record types, the TXT record provides a way to store some short text descriptions about corresponding machines and with the extension of DNS protocol standard the DNS response packet also can possibly includes longer message up to 4,096 bytes. Under this circumstance, it becomes possible that the DNS TXT record can be used in botnet communication. Therefore, it is necessary to establish a method to differentiate legitimate usages from malicious usages of DNS TXT record.

---

1We refer to a PC infected by some kind of bot program and controlled by a C&C server as a bot-infected PC.
2Note that we only captured DNS traffic from DNS full resolvers provided by our university. This means the DNS traffic from independent DNS full resolvers are not included.
2.1 DNS traffic capturing and analytical methodology

In most organizations, several DNS full resolvers are setup for performing name resolutions on behalf of individual internal computers. Therefore, in this research, we captured DNS traffics from all of the DNS full resolvers in our campus network and analyzed the usages of DNS TXT records. Fig. 1 depicts the brief network topology of DNS full resolver configuration and how we obtained the DNS traffic. We captured the DNS traffics in the traffic log server using port mirroring and anonymized the source IP addresses considering the privacy of individual users.

Fig. 1 shows a simple procedures of name resolution launched by a personal computer via a DNS full resolver. We captured all the DNS traffics from the DNS full resolvers in our campus network for 99 days (from March 24, 2014 to June 30, 2014) and analyzed them through a two-step process as described in the following:

1. Differentiate legitimate Usage of DNS TXT records and filter out unconformed usages (Sect. 2.2)
2. Investigate the unconformed DNS TXT usage in more detail to detect botnet communications (Sect. 3)

2.2 Usage of DNS TXT record

We analyzed the actual DNS traffics achieved from our campus network which is described in Sect. 2.1 and confirmed clarified usages of the DNS TXT record. The following procedures present the details about how we categorized the usages of the DNS TXT record using the real DNS traffic logs.

- SPF (RFC4408) and Domainkeys (RFC4870): To count the number for this category, we identified “v=spf” and “domainkey” in the responses.
- DNS-Based Service Discovery (RFC6763): To count the number for this category, we identified “_dns-sd” in the queries.
- NFSv4 (RFC3530): We identified and filtered out the DNS queries including strings “_nfsv4idmapdomain”.
- Anti-Virus: This category represents the software update process for anti-virus software. We identified the following domains: “.sophos.” [2], “immunet” [3], and AVG corporation’s domain [4].
• SPAM Check and DNS Blacklist: This category includes specific domain names for SPAM check and DNS blacklists. We identified the following domains “spamcop.net” [5], “spamhaus.org” [6], “rbl.maps.vix.com”, and “sa-accredit.habeas.com”.

• P2P tracker: This category represents P2P trackers used by BitTorrent. We identified the “Bittorent” and “tracker” strings in the queries.

• NTP (RFC1305): Some corporations use DNS TXT records to obtain the IP addresses of NTP servers. We identified “ntp minpool” strings in the queries and the “time.FQDN” domain name.

• Misc: This category includes miscellaneous applications and campus internal communications. For miscellaneous applications, we identified the following domain names: “time.asia.apple.com”, “apple.com” (push notifications for mail deliveries by Apple), “planex.co.jp” (software updates for network devices manufactured by Planex Corporation), “gateway.com”, and “xmpp.org” [7]. For internal communications, we identified the “titech.ac.jp” domain name.

• Unconfirmed: This is a group of usages of the DNS TXT record which are not included in any of the above categories.

The last category, “Unconfirmed”, contains the instances that cannot be added into any of the other categories. Those usages of the DNS TXT record are neither announced officially in specific application vendors nor based on any standard protocols based on DNS. Therefore, these “Unconfirmed” usages possibly include suspicious information exchange such as DNS-based botnet communications. The statistical results are shown in Table I. Note that we only counted the DNS queries have responses since the bot-infected PCs need to exchange information with the C&C servers. Consequently, in the above statistics we had 2,293 “unconfirmed” DNS TXT queries which need further investigation.

3 Further investigation of unconfirmed usages of DNS TXT record

We checked the destination IP addresses of “Unconfirmed” 2,293 queries in the “Virustotal.com”, a free third-party security check web site. “Virustotal.com” provides brief check of the target IP addresses if they are involved in downloading suspicious files and hosting URLs to identify malware, infected files and malicious web sites, etc. In our further investigation, we filtered out 330 unique destination IP addresses of the “Unconfirmed” queries and checked them in “Virustotal.com”. The results are shown in Table II.

“Virustotal.com” provides two checking methods based on either the URL or the IP address with corresponding results. Among the 330 IP addresses, 72 and 6 IP addresses are detected based on URL and IP address checking, respectively and five IP addresses were detected by both methods, consequently 73 unique IP addresses were detected in total. It means that about 22.1% (= 73/330) of the unique IP addresses obtained from “Unconfirmed” category were detected as suspicious.

Above all, we extracted 330 unique destination IP addresses of DNS TXT record queries that might have been involved in malicious communications during
99 days which means an average of 3.3 addresses per day. Considering there are four DNS full resolvers set in our campus network and based on the network traffic condition of our university, three or four times as many as unique destination IP addresses will be detected as suspicious per day (about 10 IP addresses) from an organization with the same scale of our university. We consider this is a reasonable number for handling by human operators.

### 4 Conclusion

In this paper, we analyzed DNS traffic obtained from our campus network and categorized the usages of the DNS TXT record to detect DNS-based botnet communications. As a result, we filtered out 5.53 million DNS TXT record queries from the obtained DNS traffic and confirmed that the usages for 99.95% of DNS TXT record queries were legitimate. We found the rest 2,293 “Unconfirmed” DNS TXT record queries and performed further investigation on the 330 unique destination IP addresses of the queries using “Virustotal.com” and confirmed that 22.1% of them were identified as suspicious. Accordingly, the network administrator needs to perform further investigation for about 10 IP addresses per day and we consider this number is acceptable.

<table>
<thead>
<tr>
<th>Category</th>
<th># of queries</th>
<th>Ratio [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF and domainkey</td>
<td>12,223</td>
<td>0.24</td>
</tr>
<tr>
<td>DNS-based service discovery</td>
<td>213,978</td>
<td>4.30</td>
</tr>
<tr>
<td>NFSv4</td>
<td>3,596,481</td>
<td>72.14</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>597,901</td>
<td>12.00</td>
</tr>
<tr>
<td>SPAM Check and DNS Blacklist</td>
<td>180,600</td>
<td>3.63</td>
</tr>
<tr>
<td>P2P Tracker</td>
<td>446</td>
<td>0.01</td>
</tr>
<tr>
<td>NTP</td>
<td>632</td>
<td>0.01</td>
</tr>
<tr>
<td>Misc</td>
<td>380,723</td>
<td>7.63</td>
</tr>
<tr>
<td>Unconfirmed</td>
<td>2,293</td>
<td>0.04</td>
</tr>
<tr>
<td>Total</td>
<td>4,985,277</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th># of suspicious IP addresses</th>
<th>URL detection</th>
<th>IP address detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratio to 330 IP addresses</td>
<td>72</td>
<td>6</td>
</tr>
<tr>
<td>21.8%</td>
<td>1.8%</td>
<td></td>
</tr>
</tbody>
</table>
Time estimation of logical optical line terminal migration for Elastic Lambda Aggregation Network

Yoshihiro Isaji\(^a\), Takehiro Sato, Hidetoshi Takeshita, Satoru Okamoto, and Naoaki Yamanaka

Graduate School of Science and Technology, Keio University,
3–14–1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223–8522, Japan
\(^a\) isaji@yamanaka.ics.keio.ac.jp

Abstract: Elastic Lambda Aggregation Network (E\(\lambda\)AN), the next-generation access and aggregation integrated network, has been proposed. In E\(\lambda\)AN, Optical Line Terminals (OLTs) are programmable, and Logical-OLTs (L-OLTs) can be migrated between different P-OLTs. L-OLT migration leads to enhance failure resistance and improve power saving. We have experimented L-OLT migration between P-OLTs in our laboratory. However it is necessary to evaluate how L-OLT migration time changes according to physical distance. Therefore we made an experiment of L-OLT migration in wide area network on JGN-X. This paper proposes estimation equation of L-OLT migration time. The equation leads to determine L-OLT arrangements considering time of L-OLT migration for physical distance.

Keywords: optical access network, optical aggregation, SDN, OpenFlow, E\(\lambda\)AN, JGN-X

Classification: Network System

References

1 Introduction

By the spread of Fiber To The Home (FTTH) which is high-speed Internet access and the advent of video applications that require large bandwidth, Internet traffic has been rapidly increased. In addition, the traffic of the mobile network is also increasing rapidly due to the spread of smartphones and high-speed wireless communication systems. Moreover, an expansion of network transmission capacity leads to an increase in power consumption of network components.

In access network and metro network, each service including Internet, leased line, and mobile backhaul, has its own network. Therefore, capital investment cost and operating cost increase. This is because each service network has its own requirement conditions such as protocol and Quality of Service (QoS).

From this background, a next-generation access and aggregation integrated network, named Elastic Lambda Aggregation Network (EλAN), has been proposed [1, 2, 3]. In EλAN, a programmable optical line terminal (P-OLT) provides logical OLTs (L-OLTs) and a programmable optical network unit (P-ONU) provides logical ONUs (L-ONUs). Each L-OLT is dynamically reconfigurable and supports a variety of services. In order to maximize the programmability and reconfigurability, L-OLT migration among P-OLTs [4, 5, 6] for network energy consumption reduction and virtual OLT based disaster recovery method [7, 8] has been proposed. However, L-OLT migration causes service intermittent time. Therefore, we are able to determine the distance between L-OLTs for acceptable intermittent time by understanding the interruption time for L-OLT migration time in this paper.

How long time is required for the migration is an important issue to apply the L-OLT migration to the actual service environment. Therefore, we make an experiment of L-OLT migration on the wide area network conditions and propose the estimation equation of L-OLT migration time in this paper.
2 Architecture of EλAN

Fig. 1 shows the architecture of the EλAN [1, 3]. In EλAN, L-OLTs, L-ONUs, and an active optical distribution network (ODN) using optical switches have flexibility to realize a variety of services and network configurations. By providing flexible access paths in response to service requests using the active ODN, EλAN increases the accommodation efficiency of the entire network.

EλAN integrates the current access network and metro/aggregation network into a single network. The active ODN connects L-OLTs and L-ONUs. Transmission distance between the L-OLT and the L-ONU is designed more than 40 km and a single L-OLT accommodates more than 256 L-ONUs. P-OLTs are located in central offices (COs) and connected to core network via virtual layer2 switch (VL2SW), which is constructed with distributed real L2SWs. VL2SW transmits traffic between the core network and P-OLTs and traffic between P-OLTs.

The VL2SW, P-OLTs, and the active ODN are controlled through control plane by an EλAN network management system (NMS). The L-OLT migration is initiated by NMS. Fig. 1 shows the L-OLT migration example. When traffic between the L-OLT and L-ONUs is small, L-OLTs can be aggregated into small number of P-OLTs. Therefore, it is possible to sleep the unused P-OLTs in CO and reduce power consumption of CO. In Fig. 1, NMS gives trigger message to L-OLT#22 operating in the P-OLT#2 to migrate to P-OLT#1 in order to reduce power consumption of CO.

At the same time, NMS sends messages to the VL2SW and the active ODN to set switches to configure the access path between L-OLTs and L-ONUs. In the actual environment, NMS, P-OLT, VL2SW, and the active ODN switches are physically separated in few m to few 10s km distance range. We make the estimation equation of L-OLT migration time from L-OLT migration experiments under long distance transmission conditions.

3 L-OLT migration experiment

We performed L-OLT migration experiment between P-OLTs with different physical distances to measure the required time. Fig. 2(a) shows the EλAN experimental network which is a part of the Interop Showcase network in iPOP2015 [9].
P-OLT consisted of L-OLTs and software L2SW which was a part of VL2SW and implemented using Open vSwitch (OVS). In this experiment, L-OLTs and L2SW were made as software in Virtual Machine (VM).

In Fig. 2(a), Domain#1 was located in Koganei, and Domain#2 was located in Koganei, Yokohama and also Naha in order. The distance between Domain#1 and Domain#2 was defined as $X$. L-OLT migration was performed between P-OLT#1 (Domain#1) and P-OLT#2 (Domain#2) by changing the distance $X$. $X$ between P-OLT#1 and P-OLT#2 set up in three patterns. In the first pattern, both P-OLT#1 and P-OLT#2 were located in Koganei. The distance between P-OLT#1 and P-OLT#2 was 0 km (less than 20 m). In the second pattern, P-OLT#1 was located in Koganei and P-OLT#2 was located in Yokohama. The distance between P-OLT#1 and P-OLT#2 was 22.9 km. In the third pattern, P-OLT#1 was located in Koganei and P-OLT#2 was located in Naha. The distance between P-OLT#1 and P-OLT#2 was 1543.3 km. Fig. 2(b) shows geographic locations of Koganei, Yokohama, and Naha. Domain#1 was composed of P-OLT#1, L2SW, L2SW adapter for controlling L2SW via NMS using the OpenFlow protocol, traffic generator, and video server. Domain#2 was composed of P-OLT#2, an layer-1 switch (L1SW) which emulates the active ODN, an L1SW adapter for controlling an L1SW via NMS using the OpenFlow protocol, P-ONUs, and NMS. Fig. 2(c) shows domain#2 in the Naha site. Two domains are connected by Ethernet virtual local area networks (VLANs) provided on JGN-X [10]. But in the first pattern (Koganei – Koganei), two domains were not connected on JGN-X.

It is necessary to evaluate how L-OLT migration time changes according to physical distance. Therefore we set the distance between L-OLTs 1500 km.
(Koganei – Naha). In EiAN, the actual target of L-OLT migration distance is up to 40 km.

4 Experimentation results

As a first measurement, round trip times (RTTs) from NMS in domain#2 to OVSs in each P-OLT and adapters are measured using the ping command. The RTTs from the NMS to each device (OVS#1, OVS#2, L2SW adaptor, L1SW adaptor) were 0.313 ms, 0.421 ms, 0.248 ms, 0.190 ms in the first pattern, and 5.545 ms, 0.421 ms, 5.517 ms, 0.190 ms in the second pattern, and 42.111 ms, 0.225 ms, 41.944 ms, 0.256 ms in the third pattern. These times are RTTs average of 10 pings. This result shows that the time to send a message from the NMS to each device is increased in relation to physical distance.

Next, L-OLT migration time was measured. The start of the measurement was defined as the time that NMS sent message of L-OLT migration direction to P-OLT. The end of the measurement is defined when a new path is configured and end-to-end data transmission is resumed.

L-OLT migration time is determined as an average of the three measured L-OLT migration times. As a result, the L-OLT migration time between Koganei – Yokohama is 77.035 s, and between Koganei – Naha is 79.118 s. The process that spent much of the L-OLT migration time is VLAN configuration at the L2SW. This configuration time is device-dependent and nearly 70 s is required for VLAN setting and ports setting in this experiment. This time can be reduced to 30 s [5] and 4.5 s [11].

L-OLT migration time is divided into two parts. One is a distance-dependent part such as message transmission from NMS to each device. Another is a distance-independent part such as device configuration time. Therefore, L-OLT migration time is estimated using Eq. (1).

\[ t = \alpha \times X + t_{init} \]  

In Eq. (1), \( t \) [s] is L-OLT migration time, \( \alpha \) [s/km] is the proportionality constant, \( X \) is a distance of L-OLT migration, and \( t_{init} \) is a distance-independent device configuration time. Experimental results are plotted in Fig. 3. As a result, \( \alpha \) is estimated at 0.0014 [s/km] using Eq. (2).
This value is varied according to the information amount of L-OLT and transmission rate at control plane. However, from the experimental results, since the information amount of L-OLT was relatively small, \( \alpha \) can be treated as a constant value. If the information amount of L-OLT is huge, \( \alpha \) is bigger than 0.0014 [s/km].

\[
\frac{79.11768 \text{s} - 77.0347402 \text{s}}{1543.3 \text{[km]} - 22.9 \text{[km]}} = 0.0014 \text{[s/km]}
\]  \hspace{1cm} (2)

The migration time between the same P-OLT (Koganei - Koganei) is 7.099 s. The VLAN configuration of L2SW is not changed in this migration. Therefore, \( t_{\text{init}} \) can be described in Eq. (3).

\[
t_{\text{init}} = t_{\text{VLAN}} + 7.099
\]  \hspace{1cm} (3)

In Eq. (3), \( t_{\text{VLAN}} \) [s] is device-dependent VLAN configuration time. Eq. (1)–(3) achieve to determine L-OLT arrangements considering of physical distance between L-OLTs.

5 Conclusion

We evaluated L-OLT migration time for physical distance between L-OLTs, and made L-OLT time estimation equation. As a result, estimation equation of L-OLT migration time for any physical distance was provided.

Acknowledgments

This work is partly supported by “Research and Development of Elastic Optical Aggregation Network Project” funded by NICT, Japan and also supported by JGN-X (JGNX-A14022).
Experimental evaluation on outdoor to indoor propagation characteristics for multiple microwave bands

Hayate Kimoto\(^{1a)}\), Kentaro Nishimori\(^1\), Nobutaka Omaki\(^2\), Koshiro Kitao\(^2\), and Tetsuro Imai\(^2\)

\(^1\) Graduate School of Science and Technology, Niigata University, 8050 2-no-cho Ikarashi, Nishi-ku, Niigata 950–2181, Japan
\(^2\) NTT DOCOMO INC. Research Laboratories, 3–5 Hikari-no-oka, Yokosuka-shi, Kanagawa 239–8536, Japan
\(^a\) kimoto@gis.ie.niigata-u.ac.jp

Abstract: Recently, the next generation (5-th generation: 5G) mobile communication systems have been actively investigated all over the world, in order to satisfy the strong demand for the faster and larger data communication. In 5G systems, not only UHF band but also SHF/EHF bands have been attracted much attention. Hence, frequency characteristics of radio propagation path loss have been studied. We have previously investigated outdoor to indoor (O2I) propagation characteristics in the 2.2 GHz band, and a modified path loss model instead of 3GPP model has been proposed. In this paper, in order to investigate frequency characteristics in terms of O2I propagation, the received power is measured for O2I propagation when considering 0.8, 2.2 and 4.7 GHz bands. Moreover, we investigate O2I propagation characteristics for different frequency bands by using O2I factor which denotes co-efficient versus transmit distance with logarithm expression when considering O2I propagation. Moreover, we consider O2I factor which is calculated by the least square approximation.

Keywords: 5G systems, O2I propagation, indoor penetration, path loss

Classification: Antennas and Propagation

References

1 Introduction

The 5th generation (5G) mobile communication systems are required for 1000 times system capacity and 100 times higher data rates beyond 2020. Accordingly, utilization of super high frequency (SHF: 3~30 GHz) and/or extremely high frequency (EHF: mainly 30~60 GHz) have been considered all over the world [1], as well as the frequency bands (0.7~2 GHz) which are used for the conventional cellular systems, because wider frequency bandwidth is required in 5G systems. However, there is a trade-off between low and high frequency bands from the point of view of path loss and bandwidth.

Measurement and analysis results for the path loss characteristics in the line of sight (LoS) area of an urban street microcell environment are shown when considering frequency bands from 800 MHz to 37 GHz [2]. Although various applications and services can be provided in indoor scenario thanks to smartphones, it has not been studied over a plurality of frequencies in the outdoor to indoor (O2I) propagation which is one of typical scenarios in 5G systems.

The authors have measured the O2I propagation path loss in 2.2 GHz band, and have proposed a modified path loss for O2I propagation for the 3GPP model [3, 4]. In this paper, in order to investigate frequency characteristics in terms of O2I propagation, the received power is measured for O2I propagation when considering not only 2.2 GHz but also 0.8 and 4.7 GHz bands. Moreover, we investigate O2I propagation characteristics for different frequency bands by using O2I factor which denotes co-efficient versus transmit distance with logarithm expression when considering O2I propagation.

2 Measurement environment

Fig. 1 shows the measurement environment for O2I propagation characteristics. The measurement is employed at the building at Niigata University, Japan. The height of building is 25 m. There is a window on each side of the building, it is defined as #1 to #4 in Fig. 1. The measured frequency bands are 0.8, 2.2 and 4.7 GHz. The continuous waves (CWs) with 0.8, 2.2 and 4.7 GHz are simultaneously transmitted from the base station (BS) in outdoor to the user equipment (UE) in indoor. The BS is located at Area A in Fig. 1. The transmit (Tx) antenna height of the BS is 2.5 m from the ground. The distance between A-1 to A-5 in Fig. 1 and the window #1 is from 31.5 to 72.4 m. For course 1, the incident angle for the window (Δθ) are 0 (A-1), 30 (A-2), 60 (A-3), 70 (A-4), 55 (A-5), and 32 (A-6) degree, respectively. Similarly, for course 3, the incident angle for the window (Δθ) are 11 (A-1), 18 (A-2), 54 (A-3), 72 (A-4), 60 (A-5), and 43 (A-6) degree, respectively. In addition, A-3 is regarded as NLoS environment. The UE walked across corridor in Fig. 1 while receiving the CWs. The receive (Rx)
points are 1F, 2F, 4F, 6F, and 8F (Rx height is $3 \cdot (\text{floor} - 1) + 1.5\, \text{m}$) at the building in Fig. 1, in order to evaluate the height pattern characteristics for O2I propagation.

### 3 O2I propagation characteristics

The path loss for O2I propagation is defined by calculating the power ratio between the received power at the window in Fig. 1 when assuming the free space path loss and the measured received power in indoor. In this letter, we define O2I factor which denotes co-efficient versus transmit distance with logarithm expression. O2I factor is approximated by using the least squares method. The function is defined as

$$a \log_{10}(d) + b \quad (0.5 \, \text{m} \leq d \, \text{m} \leq 20 \, \text{m}, \, a, b: \text{real number})$$

where $a$ is O2I factor for each incident angle and each floor in Fig. 2. In this case, $a$ is increased when $\Delta \theta$ is from 0 to 30 degree for course 1. On the other hand, $a$ is decreased when $\Delta \theta$ is greater than 30 degree for course 1. For example, as can be seen in Fig. 2(c), O2I factors are 5.7 and 12.9, respectively, when incident angles ($\Delta \theta$) are 0 and 30 degrees. However, in the case of $\Delta \theta$ is 70 degree, O2I factor as low as 6.4. Also, course 3 shows the same tendency as the course 1. On the other hand, when $\Delta \theta = 70$ degree, O2I factor is 6.4 and its value is smaller than that when $\Delta \theta$ is less than 30 degree.

In order to examine the reason why the results in Fig. 2 are obtained, we compare O2I factors between measured results (0.8/2.2/4.7 GHz) and modified 3GPP model [3] and these results are shown in Fig. 3. O2I factors by 1F, 2F, 4F, 6F and 8F are averaged for each frequency bands. As can be seen in Fig. 3, the characteristics by the measured results are similar among three frequency bands. Moreover, when $\Delta \theta$ is less than 30 degree, tendency regarding O2I factor versus incident angle by measured results is similar with that by the modified 3GPP model in [3]. On the other hand, when $\Delta \theta$ is greater than 30 degree, it is shown that the tendency
between measured results and modified 3GPP model does not agree with each other. Although the penetration by #1 Fig. 1 is dominant when $\Delta \theta$ is less than 45 degree, the dominant window is changed to be #2 when $\Delta \theta$ is greater than 45 deg, as shown in Fig. 1. From the above observation, we propose the modification of the modified 3GPP model in [3]. Instead of $\alpha = \frac{11.93 \cdot (1 + \sin \Delta \theta)}{C_1}$ in modified 3GPP model [3], we adopt $\alpha = \frac{11.93 \cdot (1 + \cos \Delta \theta)}{C_1}$ when $\Delta \theta$ is greater than 45 degree. By utilizing this modification, the tendency of O2I factor is similar with the measured results. We found that the dominant window should be considered when considering O2I propagation characteristics. On the other hand, because the absolute values of O2I factors between measured results and modified 3GPP model are different with each other, the further measurement and investigation should be evaluated.
In this paper, we conducted O2I propagation measurement for 0.8, 2.2 and 4.7 GHz bands. We define O2I factor which denotes co-efficient for transmit distance with logarithm expression in indoor O2I factors are obtained by the least square approximation for each measured result. From the measured results, O2I factor is increased and decreased from a certain angle according to the incident angle regardless of frequency bands. It is shown that the dominant window should be considered when considering O2I propagation characteristics.

**Acknowledgments**

We would like to thank the members of Nishimori Laboratories for the help on O2I measurement.

---

![Fig. 3. Comparison of O2I factor between measured results and modified 3GPP model [3].](image)
HPBW control of dipole antenna with frequency selective reflector using different size elements

Keizo Cho\textsuperscript{1a)}, Hideya So\textsuperscript{2}, and Atsuya Ando\textsuperscript{2}
\textsuperscript{1} Department of Electrical, Electronics and Computer Engineering, Chiba Institute of Technology, 2–17–1 Tsudanuma, Narashino, Chiba 275–0016, Japan
\textsuperscript{2} NTT Network Innovation Laboratories, NTT Corporation, 1–1 Hikarino-oka, Yokosuka, Kanagawa 239–0847, Japan
\textsuperscript{a)} cho@m.ieice.org

Abstract: This paper proposes a reflector backed dipole antenna whose reflector is composed of frequency selective reflector (FSR) and the size of the FSR elements aligned in the both side columns is changed. Since the width of the frequency selective reflector, which is composed of an array of the frequency selective elements, is chosen discretely, it is difficult to design an arbitrary beamwidth of the reflector backed antenna because the beamwidth of the reflector backed dipole antenna can be adjusted by the size of the reflector. The proposed antenna configuration can achieve arbitrary beamwidth by using different size of the FSR elements aligned in the both side columns. This paper also shows the condition of the FSR element size aligned in the both side columns to obtain sector radiation pattern.

Keywords: base station antenna, mobile communication, frequency selective reflector, reflector backed dipole antenna

Classification: Antennas and Propagation

References

1 Introduction

Multi-band base station antennas are widely used for mobile communication systems since current systems operate at multiple frequency bands from 700 MHz to 2 GHz bands to cover recent large traffics [1, 2]. Ministry of Internal Affairs and Communications in Japan announced that 3.5 GHz bands were assigned to the fourth generation mobile communication systems [3]. In this situation, multi-band base station antenna that operates from 700 MHz to 3.5 GHz bands should be useful for the next mobile communication systems.

Reflector backed dipole (RBD) antenna configuration is popularly used for mobile base station antennas because of its broadband characteristics and ease to form sector radiation pattern with dual-polarized configuration. In the RBD antenna configuration, the spacing between the dipole element and reflector should be less than about quarter wavelength to obtain sector radiation pattern. Therefore, when configuring the multi-band antenna sharing the reflector, dipole elements of the RBD antenna for high frequency bands should be closely placed to the reflector than those for lower frequency bands. In this case, the waves radiated from high frequency band dipole elements induce the currents on the low frequency band dipole elements and the induced currents distort the radiation pattern in the high frequency band [4].

It has been reported that using frequency selective reflector (FSR) as the reflector of the RBD antenna is effective to configure the multiband mobile base station antennas [5, 6, 7]. In the base station antennas, the beamwidth in the horizontal plane is important to cover sector service area and to suppress the interference toward the adjacent sectors [1, 2]. Generally, the beamwidth of the RBD antenna can be adjusted by the width of the reflector. However, the width of the FSR depends on the number of the FSR elements, therefore the width of the reflector cannot be configured arbitrarily when using the FSR as the reflector, this means that it is difficult to obtain an arbitrary beamwidth of the RBD antenna using FSR as the reflector.

This paper proposes the configuration using different size of the FSR elements aligned in the both side columns of the FSR in the FSR backed dipole antenna.
Square loops are considered as the FSR elements in this study [8]. It is shown by the numerical analysis using the moment method that the proposed antenna enables to adjust the half-power-beam-width (HPBW) of the RBD antenna arbitrarily under the limited range.

2 Proposed FSR configuration

It has been reported that the phase of the current flowing on each FSR element can be controlled by changing the size of the FSR element [9]. When the size of the loop FSR is increased, the phase of the wave radiated from the enlarged loop element is delayed, and when the size is decreased, the phase is advanced. By using this property, we propose the beamwidth control of the FSR backed dipole antenna (FBD). We change the size of the FSS elements in the both side columns to adjust the beamwidth. Using enlarged elements aligned in the both side columns can increase the beamwidth while using reduced elements should decrease the beamwidth as shown in Fig. 1. In this letter, the effectiveness of the proposed configuration is evaluated by the moment method analysis.

3 Analysis model

The proposed configuration is shown in Fig. 2(a). The dipole antenna is composed of strip conductors. Each strip conductor of the dipole antenna is modeled by wire grid divided into 4 and 5 in width and length directions as shown in Fig. 2(a), and the width \( w_d \) and length \( l_d \) are 10 mm and 32.6 mm, respectively. The dipole element is fed at the wire connected between both the strip elements. The diameter of the wire used in the wire grid model is 0.2 mm. The square loop elements configuring the FSR are configured by the wires whose diameter is 0.2 mm, and are placed in the yz plane. These are separated by 17.1 mm from the dipole element as shown in Fig. 1(a). The number of the loop elements in the y and z directions are both threes in this study. The side lengths of the square loops in the left and right

![Fig. 1. Concept of the proposed FSR backed dipole antenna.](image)
columns, and in the center column are represented by \( l_s \) and \( l_m \), respectively. The side length \( l_m \) is 23 mm, and the side length \( l_s \) is determined by \( l_m \times TF \). \( TF \) is called ‘taper factor’ here defined by the ratio of the side length \( l_s/l_m \). The distance \( s_l \) between the centers of the adjacent loop elements is 26 mm. The investigated frequency is 3.5 GHz. 4NEC2 [10] is used for this analysis. In this letter, the dependency of HPBW and the front to back power ratio (FB) on the taper factor \( TF \) is investigated. The FB is defined by the ratio of the forward radiation power (at 0 degrees) to the maximum backward radiation power in the range from 135 to 215 degrees.

4 Analysis result

Fig. 2(b) shows the relationship between the taper factor \( TF \) and HPBW. The relationship between \( TF \) and FB is also plotted in Fig. 2(b). As can be seen in Fig. 2(b), arbitrary HPBW from 70 degrees to 145 degrees can be obtained by adjusting the side length of the square loops aligned in the both side columns when changing \( TF \) from 0.7 to 1.1. HPBW is minimum when \( TF \) is 0.92. The reason for increasing the beamwidth as decreasing the loop size is considered as that the reflected wave with advanced phase from the reduced loop elements is largely tilted, this causes to increase the beamwidth as shown in Fig. 3(a). Therefore, the same HPBW can be obtained when \( TF \) is less than 0.92 and \( TF \) is more than 0.92.

As for the FB characteristics, FB is minimum when \( TF \) is 0.88. Fig. 3(b) shows the radiation pattern comparison of proposed antennas obtaining the same HPBW of 85 degrees using different \( TF \)s of 0.885 and 1.003. As can be confirmed from Fig. 3(b), the back lobe with the \( TF \) of 1.003 (large loop case) can be reduced than that of 0.885 (small loop case). Thus the large loop case is suitable for the base station antenna from the view of obtaining sector radiation pattern. In addition, the HPBW suddenly changes according to the change of \( TF \) when \( TF \) is less than 0.92. From that point, the large loop case is also suitable for the base station antenna to obtain frequency stable radiation pattern.

![Fig. 2. Proposed antenna configuration and HPBW characteristics.](image-url)
5 Conclusion

In this letter, we proposed a frequency selective reflector backed dipole antenna whose element sizes aligned in the both side columns are changed. It is shown that the proposed antenna can control the beamwidth of the antenna by adjusting the size of the frequency selective surface elements in both side columns. There are two cases to obtain the same HPBW sector pattern using the different taper factor $T_F$s; the $T_F$s are less than 0.92 case (small loop case) and more than 0.92 case (large loop case) in this antenna configuration. However, considering the FB characteristics and stability of the radiation pattern, large loop case is suitable to obtain sector radiation pattern.

Acknowledgments

This work was partially supported by JSPS KAKENHI Grant Number 25420381.