東京電機大学

博 士 論 文

意図的遮断の存在下でのオフショアビジネス継続のための
シームレスな仮想ネットワーク構築方法

Seamless virtual network for international business continuity in presence of intentional blocks

平成 30 年 3 月 18 日

藤 川 洋

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In developing countries, links are poor among domestic communities or Internet Service Providers (ISP). Besides international Internet channels are suddenly blocked by such as GS (Golden Shield) in China. Offshore business communications are involved in these.

To avoid such involvement, a seamless virtual network is proposed as an international business communication bridging solution. This uses the so called Round Trip Time (RTT) based multiple thresholding differentially switched Virtual Private Network (VPN) bypass. The characteristics are

(1) the use of a multiple threshold integrated differential calculus of the RTT increase, a sign of the block is recognized as the steep staircase increase of RTT,
(2) followed by the immediate automatic switch to VPN having an RTT below 200ms and
(3) its asymmetry, i.e. only the absolute threshold value and continuation time are used to determine when to switch back.

This method is analytically and statistically evaluated as being successful (below 3% errors), using around 200 cases of data on GS blocks. Furthermore, it has been validated by the real seamless usage in more than 20 offshore companies for three years.

Besides response time in offshore applications, this method can also alleviate problems such as voice echoes and video jitters which irritate business users. These effects were validated analytically and by questionnaires to scores of business customers.

Chapter 1 motivates the topic, briefly discusses potential solution approaches, and sketches basic ideas of the developed solution to the problem.

Chapter 2 describes the communication problems such as governmental restrictions or problems in developing countries such as China, which is the reason for the inconveniences. Further, it describes a reference model for dependable network services especially for latency sensitive offshore business application.

Chapter 3 introduces our solution method to guarantee dependable offshore application services. In particular, the VPN bypass link is introduced along with its characteristic

compared to the domestic Internet is introduces in the first part and an intelligent timing policy for switching it on and off in its second part.

Chapter 4 evaluates the effects, using typical borderline examples and statistical analysis. In particular, the behavior of the proposed method on non-blocked and blocked Internet service is analyzed. Furthermore, the results are discussed and improvements are derived accordingly.

Chapter 5 analyses the effects on the technical quality of latency-sensitive key applications such as audio-conferencing. Then, effects to the end users are validated using this analysis for latency-sensitive applications and questionnaires about the quality perceived by the final/application user.

Chapter 6 outlines related work, providing the detailed comparison with existing solutions. Since the related work assumes a knowledge on the proposed approach to be correctly understood, this chapter is arranged at this place instead of a place in front of the proposed solution. Also, the paper would benefit from a more detailed comparison between existing solutions and the proposed approach. It also describes some backgrounds on the negative effects of latency turbulence on applications like cloud/fog computing and audio/web conferencing services.

Chapter 7 summarizes the thesis by reviewing the problem, the developed solution and the evaluation results and concludes the Thesis.

1. INTRODUCTION

Enabling international business communication via the Internet has become an important factor for the growth of business activities in developing countries. For example, it has become common for offshore business in emerging countries to utilize motherland cloud computers as data centers for efficiency, safety and such. Smooth and efficient Web conferences among offshore offices and headquarters or offices in other countries are also important for enterprise activities. Because of the cost, they are usually accessed via the Internet.

However, sometimes international bridging channels for developing countries are suddenly blocked. This is done by intentional actions of the local government, called GS (Golden Shield) in China. It is also known as “the Great Firewall” [52]. This causes business discontinuity resulting from sudden serious degradation of network response. Such restriction not only targets each single IP address by TCP Reset [13]. But also it cuts the route to an IP address prefix that includes the target IP address. In the latter, all business sites located near the (usually political) target become involved in the block.

VPN (Virtual Private Network) has been already used to avoid such governmental censorship. However, it has problems in persistent governmental censorship or blocking as well as its cost. Still more, manual switch to VPN takes time and is troublesome. Thus users often lose offshore business opportunities because of a lack of smooth international communications. Further, some VPNs may already be censored when they are used. Nobori et al. [39] try to solve this by costless volunteer VPN gateway servers and their collaborative detection using spy lists against governmental attack. However, despite their free cost, using volunteer gateway servers is not stable especially for business use. On the other hand, dedicated lines are expensive.

To cope with these problems, a seamless virtual network system is proposed for international business continuity in the presence of intentional blocks. This system is based on our previous network-intensive method [24], using a differential VPN bypass tool. This method exploits the staircase waveform of network delay of intentional blocking such as GS. Thus, the proposed intelligent method automatically recognizes intentional blocking of international communication. Then, this immediately activates a VPN bypass before

significant response degradation is experienced by users. The intelligent routers switch the route to foreign addresses from the open Internet to a VPN bypass, in order to limit network latency increase. Routers are placed at user's offices. However, VPN utilization is limited to the block duration to avoid the VPN gateway becoming also a target of blocking. This method applies asymmetric criteria to decide when to activate the bypass and when to return to open Internet connection. Differential values of RTT (Round Trip Time) or network latency are used for detecting the start of a GS block (bypassing). Meanwhile, to determine both the start and the end of a GS block, absolute threshold values are used. In particular, this Thesis concretely and formally shows the followings:

(1) differential values of network latency can easily detect an abrupt change of RTT and

(2) therefore, are also useful to alleviate Voice echo and jitters caused by abrupt change of RTT.

This Thesis includes newly extended parts of our network-intensive base system. The extension (the novel parts) are its conceptual features and/or methods focused on business continuity. These include multiple differential thresholds, evaluation by questionnaires and borderline cases, as well as statistical analysis. Here the types of business carried out across international borders include metal material export, import of finely processed steel, manufacturing and sales of apparel, etc. The needed type of continuity is the seamless transmission of voice, image, video data as well as text. These are necessary for animation pictures, multimedia catalogue, or high precision design documents accompanied with high quality vocal explanation in Web or video conferences. Applications such as AutoCAD, Polycom RealPresence, and various cloud services were needed for the business types mentioned above. These applications usually access cross-border service interfaces such as those of video conference whose servers are in the motherlands.

The proposed method provides an application-intensive seamless communication bridge to developing countries or communities. It is thoroughly evaluated. Its capability of providing continuity is improved at the business application level. This improvement focuses on latency-sensitive services such as audio /Web conferencing. Especially, the proposed method newly improved by integration of multiple differential thresholds. This alleviates not only response time in Web conferences but also throughput in business file

transfer, voice echo problems, and jitters in voice and video. Voice echo and jitters often and significantly irritate business users. Further, this paper newly validates our method's effects to such application level international communications. This is realized by analytical evaluations as well as questionnaires to our customers of 24 companies in their offshore business application usage.

2. COMMUNICATION GAPS WITHIN AND WITH DEVELOPING COMMUNITIES

Business continuity was often hindered in operating IT systems especially in accessing cloud computers. This chapter describes China's communication problems.

2.1 Communication problems in Operating Distributed Systems in China

Although over 500 million Internet users exist in China, its Internet suffers from the peering problem. This problem is sometimes referred as "North-South problem" or "North-South Divide" [12]. Internet exchange between China Telecom and China Unicom is very narrow, though both are ones of the world largest carriers. The quality, speed, and stability of communication over such poor link are often deteriorate sharply. If congested, more than 1000ms latency happens even in the same city [40]. The connection between an ISP in China and one in Japan is often faster than that between nodes both in China. The former is much more stable. This problem is serious for a company that runs a distributed system. It is because clients in multiple offices are linked to servers at data centers. For example, in southern China, there are many clients of branch offices. Clients of such offices are often connected to multiple ISPs. Some of them are connected to China Telecom and others are connected to China Unicom even though residing the same city. They access through the servers or data center at their headquarters connected to China Telecom. More than 1sec. latency mentioned above causes even malfunctions of the distributed systems built using application servers such as MetaFrame [35].

Regulations imposed by the Chinese government are also problematic. This is a political rather than technological issue. Because of the regulation by China State Council Di-

rective No. 273 [11], de facto global standard products for data security cannot be used in China. Thus, data centers need to be in mother countries for security reasons. Client computers in China need to communicate with each other via servers in Japan.

Furthermore, the Ministry of Public Security division of the Chinese government operates a censorship and surveillance project. This is called GS (Golden Shield) whose firewall is known as "the Great Firewall" [52]. It is known that the censor system blocks services such as Twitter, Facebook and YouTube regarded as harmful by the government. Web sites carrying political messages against the country are also blocked. It is considered to be for the purpose of thought control. However, this regulation or network restriction causes bad influence or collateral effects to business traffic as well as to daily life. For example, international communication links for business are often blocked as described later. Such incidents become frequent around the time of large political ceremonies like National People's Congress.

Below are some of the techniques used by GS [13]:

- DNS Poisoning: GS intentionally poisons its DNS caches with wrong addresses.
- Blocking Access to IPs: GS can block access to certain IP addresses. This prevents people from accessing a certain forbidden IP address directly. This technique also blocks other services located at the same address as the target (shared hosting).
- Analyzing URLs: GS scans URLs and block connections if they contain sensitive keywords.
- Inspecting and Filtering Packets: GS uses "Deep Packet Inspection (DPI)" to examine unencrypted packets, looking for sensitive content.
- Resetting Connections: When GS blocks access, it will block communication between both computers by sending a "reset packet." GS essentially lies/tells to both computers that the connection was reset. Thus, they can't talk to each other.
- Blocking VPNs: In late 2012, GS started trying to block VPNs. GS identifies encrypted traffic and kills VPN connections.

These blocks can be identified, using a tool such as "Great Firewall of China" or the Website Pulse test as Fig. 1 [53]. Below are the results of the analysis for the human rights

site. The site www.hrw.org is not accessible from mainland China but easily reachable from the US (Fig. 1). The US site's short response time of the Chinese DNS suggests DNS poisoning. The IP address resolves to an address in Europe. This address in turn is shared by the Chinese domain www.haosf.com.cn.

Due to such blocking caused by governmental restriction, multiple paths to reach Japan are prepared. Clients can choose the best path according to the situation. However, some are still problematic for business. For example, manual bypassing on GS blockage causes discontinuity in business communication. Others such as dedicated lines are expensive. VPN bypasses can also be used to avoid this. However, always using VPN services has problems with a risk of governmental restriction as well as with its cost. Though Nobori et al. [39] try to solve these through volunteer VPN services equipped with the detection of governmental censoring. However, using volunteer gateway servers is too unstable for offshore business.

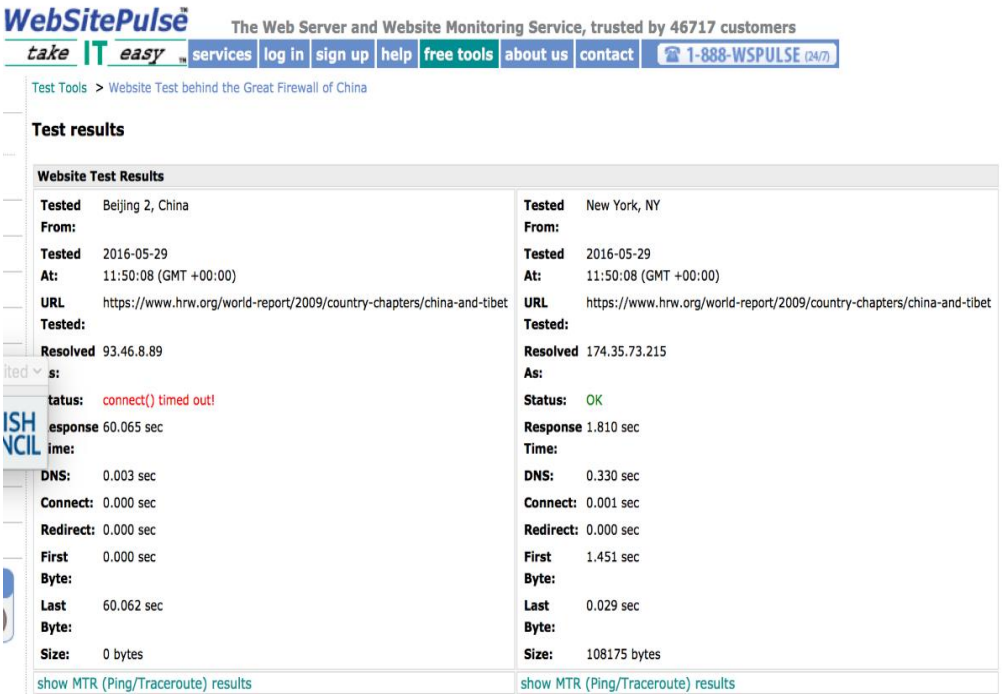

Fig. 1: Website Pulse: Censored Website Monitoring (status: connect() timed out!) Service

2.2 Alternative Connection Path for offshore business System in Developing Communities

The types of offshore business carried out in China or across the border include

(1) metal material export and finely processed steel import,

(2) the design and production of automobile parts,

(3) food manufacturing and sales,

(4) manufacturing and sales of apparel, etc.

The needed continuity type is the seamless transmission of texts, voice, image, and video data. These are indispensable for animated videos, multimedia catalogue, or high precision design documents accompanied with high quality vocal explanation in Web or Video conferences. Applications such as AutoCAD, Polycom RealPresence, and various cloud service are needed for the above mentioned types of business. They access service interfaces such as video conference.

Such interfaces should be cross-border, that is, their servers should be deployed in the motherlands as shown in Fig. 2. It is because accessing large-volume data as well as data security in real time is needed. This cannot be satisfied without exploiting cloud services across the border. This is because of communication problems such as North-South Problem and governmental restrictions discussed in the previous section.

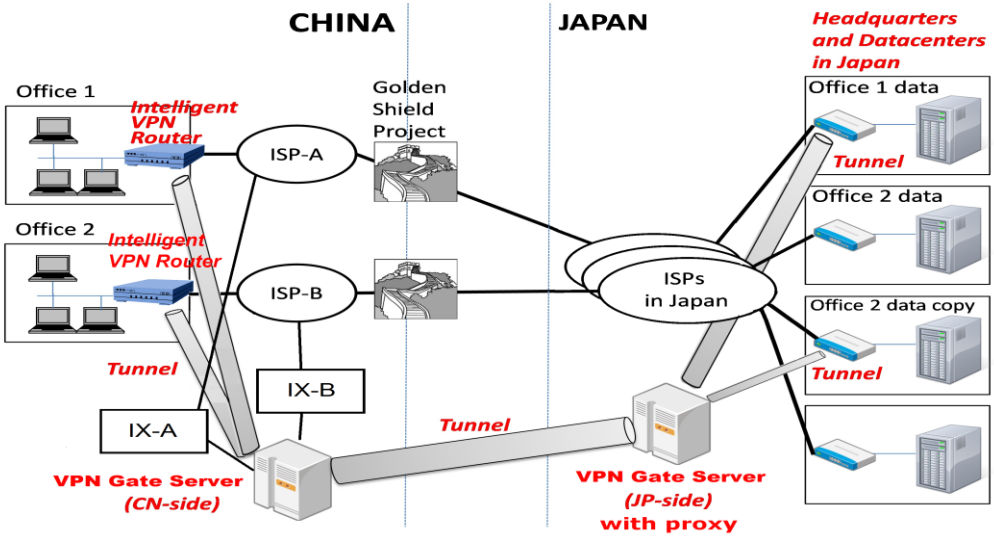

Fig. 2: Our cloud-based system provided in China

Fig. 2 illustrates the architecture or framework of such a business system. It uses cloud computers or data centers in the motherland. For the sake of simplicity, our framework only assumes two offices in China. In real cases, there are much more offices involved. Further in China, even each office (Office 1, Office 2) of the same company is often connected to different ISP, (ISP-A, ISP-B, respectively). The exchange of data among these ISPs is poor. Thus, offshore offices of various Japanese companies in China are connected through data centers in Japan. This makes our system an offshore cloud system shared by multiple companies.

Under this system model for offshore business, a lot of important data are stored in the mother country or Japan. Headquarters of companies and data centers are connected to the Internet in Japan. Application software also runs in those unrestricted places. Conversely, virtual terminal environments such as MetaFrame require data and programs to be placed inside a single server or a data center. Our framework allows these to be distributed among different places. They are connected via seamless, stable and dependable communication infrastructure in Japan. This feature provides flexibility in system deployment. This is often required in dynamically-changing situations and evolving economies of developing countries. Each database of each office or company can be deployed in each different server in Japan. Some database copies of such a distributed data center for heterogeneous company offices can be deployed in different servers. Such a remote distributed data center shared by multiple companies provides a more stable and dependable storage infrastructure. This is taken as a kind of cloud systems.

However, the serious issue in this architecture is the GS mentioned before. This causes the instability of the international Internet connection. It is not foreseeable when such connections become blocked. Furthermore, the restriction is done not only to each single IP address but also to the group of IP addresses. The former blocks by issuing TCP Reset to the IP address [13]. Meanwhile, the latter shutdowns /blocks the colleagues near the target or some groups of IP addresses such as subnets or international channels. Business sites (especially cloud computers) nearby or surrounding the (usually more political) target site are involved in this GS blocking. Such GS blocks cause a serious risk of business interruption [2]. However, this is owing to the involvement in sudden restriction of international

channels for accessing offshore cloud systems mentioned above. Such business continuity disruption is a collateral effect of an action having different objectives. Namely, objectives are those to block people's accessing politically inconvenient data or sites. The proposed method provides seamless dependable communication bridges for offshore business systems as modelled in Fig. 2.

3. DEPENDABLE COMMUNICATION BRIDGE FOR OFFSHORE BUSINESS SYSTEM

To solve the problem mentioned above, an intelligent bypass method using VPN is proposed. The aim is the dependable communication bridges whose configuration is also illustrated in Fig. 2. This automatically switches between the ordinary Internet and VPN contracted considering bandwidth and reasonable cost. This is done seamlessly without users' consciousness even on sudden GS restriction to international communication. A proxy server or VPN Gate server as shown in the bottom of Fig. 2 accepts connections from office's intelligent VPN routers and automatically controls the IP packet flow. The server relays them to its counterpart connected to the Internet in Japan or offshore cloud computers. This achieves both the effectiveness of communication and the immunity (or avoidance) from GS blocks. The proposed intelligent bypass method dynamically changes the path to send IP packets. An intelligent VPN router in Fig. 2 uses this method. It ordinarily sends them to a regional ISP (i.e. ISP-A for Office 1). No sooner it recognizes any sign of governmental network blockage, it changes the path to the VPN Gateway Server. This is done characteristically using differential calculus. On recognizing the end of GS blocks, it switches the path back to the ordinary internet (i.e. ISP-A) again.

This chapter concretely explains the proposed method and its rationale. Further, in the next chapter, the effect is estimated more quantitatively as well as validated statistically.

3.1 VPN Bypass Link for Stable Offshore Communication

Internet routing protocols such as OSPF and BGP select routings. These are based on some criteria such as minimizing the number of hops considering static band-width. However, his does not work on intentional disconnections by attackers such as those of GS. This type of countermeasure cannot form reasonable alternative routes and packets will be significantly delayed. Users facing such network system disruption have to prepare com-

munication bypass links to avoid deteriorated networks. This reasonable bypass for keeping the QoS or network response, is achieved through switching to VPN by considering its bandwidth, cost, etc. The routes through the routers/IXs at or close to the restricted international communication sites (Golden Shield Project in Fig. 2) will be very congested especially in case of GS attacks. However, China side bypass links from user's offices to VPN gateway are connected through routers/IXs such as IX-A (for ISP-A) or IX-B (for ISP-A). These routers are far from the restricted sites. Further, North-South problems do not happen since IX-A and ISP-A (also IX-B and ISP-B) belong to the same AS. Contracted VPN providers assure the performance between VPN gateway and Japan. Thus, independently of GS attacks, the bypass link is stable and has better RTT than Internet. This is shown by lower lines (bypass link) in エラー! 参照元が見つかりません。 and エラー! 参照元が見つかりません。 or RTT in the third column of Table II.

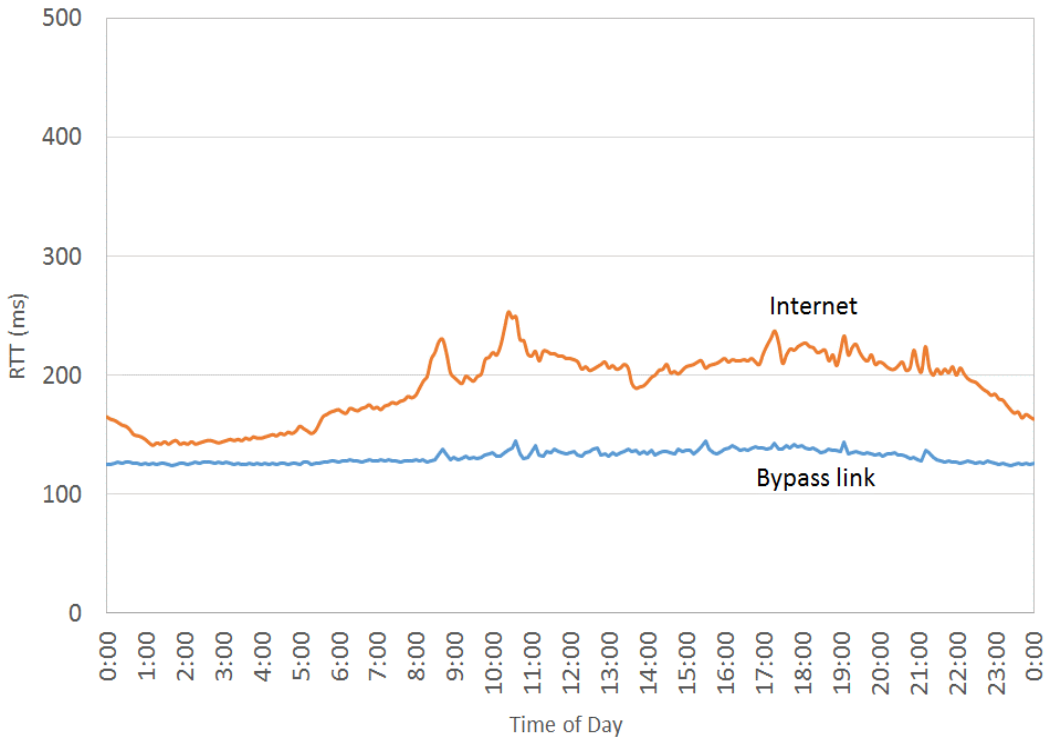

Fig. 3: RTT(Round trip time) on an ordinary day

Table I: Increase ratio (RTT IR) on non-GS in Fig. 3

Time (hour)	RTT (ms)	RTT increase ratio (%)
10:06:00	217	-0.91
10:12:00	**225**	3.69
10:18:00	239	6.22
10:24:00	**253 (Maximum)**	5.86
10:30:00	248	-1.98
⋮	⋮	⋮
21:12:00	**224**	10.3

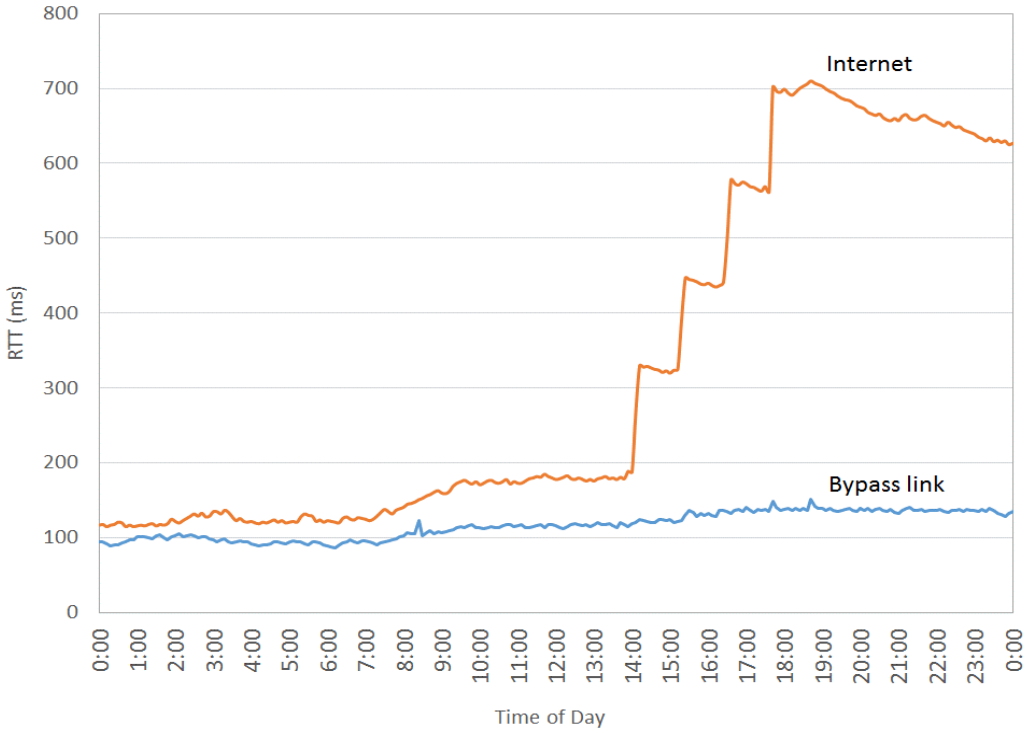

Fig. 4: RTT on typical multiple step GS

Table II: RTT increase ratio (RTT IR) on GS of エラー! 参照元が見つかりません。

TIME (hh:mm:ss)	RTT (ms)	RTT bypass	RTT IR (%)
14:00:00	188	119	-0.53
14:06:00	269	121	**43.1**
14:12:00	**330**	125	22.7
⋮	⋮	⋮	⋮
15:18:00	390	123	20.0
15:24:00	447	130	14.6
⋮	⋮	⋮	⋮
16:30:00	499	135	13.2
16:36:00	578	133	15.8
⋮	⋮	⋮	⋮
17:42:00	702	149	24.9
⋮	⋮	⋮	⋮

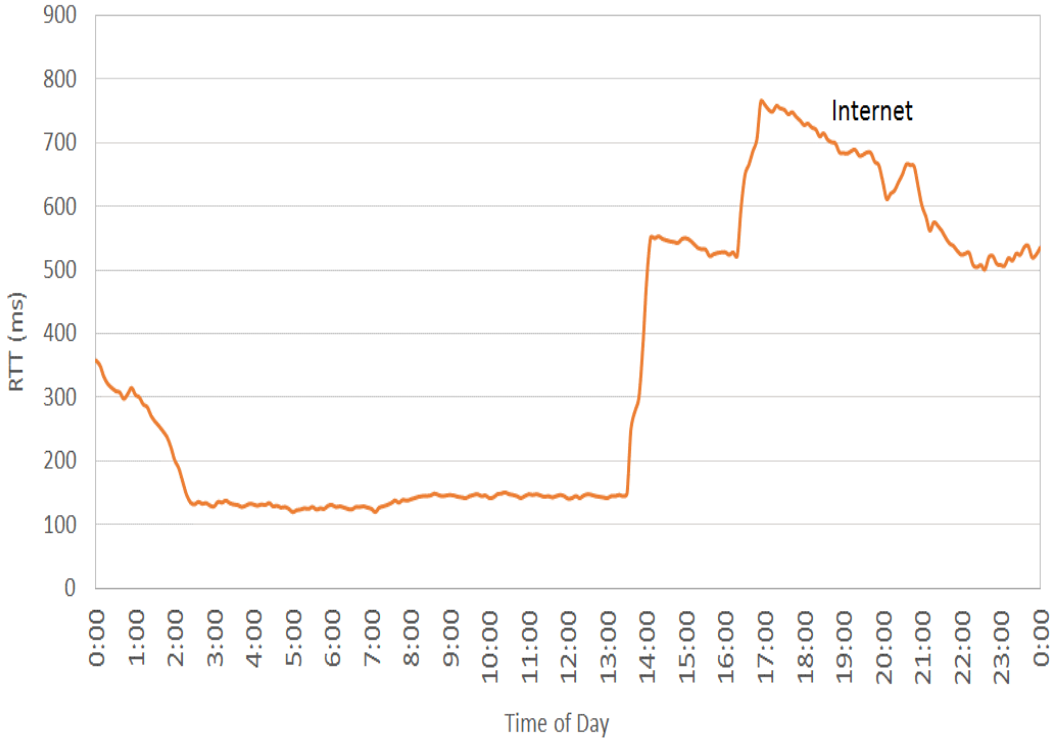

Fig. 5: RTT on typical single step GS

Table III: mmm RTT increase ratio (RTT IR) on GS in エラー! 参照元が見つかりません。

hh:mm:ss	RTT (ms)	RTT IR (%)
0:06:00	350	-2.2
⋮	⋮ (over 200ms)	⋮
2:00:00	201	-9.5
2:06:00	189	-6.0
⋮	⋮	⋮ (30minutes)
2:36:00	136	-3.1
⋮	⋮	⋮
13:30:00	149	2.8
13:36:00	250	**67.8**
13:42:00	**278**	11.2
13:48:00	299	7.6
13:54:00	378	26.4
14:00:00	485	28.3
⋮	⋮	⋮

Without attacks or intentional disconnections, users would be better served using Internet connection rather than VPN, because of cost or stability. As shown in Fig. 2, intelligent VPN routers continuously monitor the behavior of network services. Then it selects the path through which to forward the packets for stability and efficiency in running application programs. The routers placed at user's offices switch routes to/from VPN contracted by each company to ensure QoS or network response and only during regulation not to be censored. By the way, the primary motivation for the proposed method as opposed to existing tunneling methods is to improve the performance (response time) of data transfers through clouds in mother countries, with low cost, especially during the GS blocks. Therefore, the anonymity of users is not necessarily guaranteed except between VPN gates (in China and mother countries) default supported by VPN providers.

3.2 Intelligent Switch for seamless virtual network

The timing of the switch to VPN is very important for stable communication within distributed offshore information systems. Intelligent VPN routers have to recognize the

onset of a GS block before users are aware of network deterioration. GS blocks happen abruptly and cause a business activity stop. According to our experience, the behavior of the Internet services is very different between unintentional malfunctioning and intentional attack. Disruptions caused by the former primarily affect the dropped packet ratio, while the latter gives away some telling signs of the onset in terms of latency (the turn-around time: RTT). In the case of GS, network latency increases following a staircase pattern. Such latency causes throughput degradations resulting from "ack" of TCP and jitters (fluctuations) because of abrupt/sharp increasing waveform. They also hinder our distributed information systems.

Taking these considerations into account, switching to/from VPN bypass is performed by our proposed intelligent VPN routers as follows.

(Step 1) Every 15 seconds, the router sends ICMP Echo Request to the offshore servers used by applications in the office via the open Internet and VPNs. And, it records the turn-around time (RTT) for the corresponding ICMP Echo Reply to return (ICMP is forwarded by the proxy in Fig. 2).

(Step 2) The router calculates the RTT increase ratio (first derivative) by the expression as shown below. Rule1: if it is higher than a preset value *of differential threshold tdf %* per difference width *tw* seconds and the RTT absolute value is longer than starting threshold *ts* milliseconds, GS mode (initially reset) is set. Then at once, the communication path of offshore computers is switched from the Internet to a VPN bypass (which is active namely, whose RTT is less than 200 ms). Denoting by RTTC: the current RTT and by RTTB: the RTT of a ping measured a tick before, we have $RTT\ \ increase\ \ ratio = 100 * \frac{(RTTC - RTTB)}{RTTB}$

(Step 3)The router continues to record RTT of the Internet. Rule2: when RTT being below a preset threshold called *ending threshold te* (milliseconds) *continues over continuation time tc* (minutes) during GS mode on, GS mode is reset and the router changes the communication path back to the Internet.

Threshold values are selected, used, and adjusted as follows.

In (Step 2) generally as a range, *differential threshold tdf= 20~40%* per *difference width tw=15~360* sec coupled with *starting threshold ts= 120~200*ms. Specifically, *tw* is set empirically first (e.g. 360 sec in the year 2015). Then, *tdf* is selected as "the minimum value of RTT increase ratio per *tw* at GS onset (e.g. 43% in エラー! 参照元が見つかりません。 in the year 2015) - margin (usually 10 %)". Thus *tdf was* 30% in 2015. Meanwhile, *ts* is selected as "the minimum value of RTT at GS onset (e.g. 150ms in 2015) - margin (usually 10ms)". Thus, RTT absolute value threshold at GS start, namely, the *starting threshold ts* was 140ms in 2015. They are used in Rule1. Using real data, such parameters are checked every season (every 3 months) to be adjusted for the real use.

In (Step 2) *ending threshold te=200*ms and *continuation time tc=30*min are selected by the maximum RTT and its duration on non-GS days and adjusted every season for real use in Rule2.

We remark that practically speaking, this control is enabled only when the network is being used. Furthermore, when little or no traffic is observed, e.g. during late nights, they can disable switching. The aim is to limit pointless use of bypass routes. A major feature of our method is the asymmetric control of path selection between (Step 2) and (Step 2). Namely, differential values and absolute values of RTT are used for switching to bypass. Meanwhile, only absolute values combined with the elapsed /continuation time are used for switching back to the Internet. This is obtained from our experience with the systems operated in China for several years. Below, we provide the rationale of our method.

It is straight and usual to switch paths once the RTT increases over an absolute threshold. Practically, however, it does not work. It is because Internet traffic in peak hours slow-downs physiologically or comparatively gradually. In China, for example, the Internet becomes congested in the evening almost every day. Thus, a simple rule specifying an absolute threshold has the following problems. For the rule, "if RTT is more than *X* msec., it is a GS block":

(RTT on non-GS) explains it. The table explains how false positive errors occur, if threshold X is comparatively low (e.g. below **250**ms). For instance, if threshold *X* is 220/250ms, this rule takes ordinary congestions for a GS block when RTT is **225/253**ms at 10:12:00 (10:24:00).

and エラー! 参照元が見つかりません。 show these mistakes can continue almost all the day (from **10:12:00 or 10:24:00** till **21:12:00**). Meanwhile, Table III (RTT on GS) explains false negatives: noticing the block when too late if threshold *X* is slightly high (e.g. over 250ms). Namely, if threshold *X* is 270ms, this rule cannot find a GS block until RTT is **330**ms. Table II shows this. If threshold *X* is 255ms, the rule cannot find a GS block until RTT is **278**ms. Table III shows it. These RTTs make business users easily experience network latency. Such experience causes a business activity stop.

To distinguish daily congestion from GS blocks, we rather look at the first derivative of RTT. GS blocks introduce steep staircase increases of network latency. Meanwhile daily congestion causes a lower rate of RTT changes. The Internet slowdown caused by a natural disaster remains local. It does not show the sharp and rather long and/or multiple staircase RTT increase for international communications. This is typical of the onset (start) of intentional blocks such as GS. Based on this insight, the proposed method uses a first derivative threshold. This is coupled with an absolute (or fixed/static) value threshold, rather than thresholding absolute value only. The method can be expected to predict such GS blocks more effectively.

On the contrary, GS block end does not show such tendency. From our practical experience, RTT does not decrease so abruptly at the end of GS as it increases at the onset. This happens because a large amount of traffic flows in each Internet route when it reopen at the end of GS block. This results in the Internet congestion and the RTT does not decrease so rapidly. In practice, switching back is not as urgent as avoiding the onset of blockage, which halts business operations. Thus, we use simply RTT itself to switch back, instead of its differential value.

The proposed method uses Round Trip Time of ICMP Echo (RTT) rather than other parameters such as packet-loss rate. The rationale behind it is as follows. At the beginning of an intentional network block by GS, some routes are shut down. However, packets can be re-routed to the ones still open. In reality, pings namely ICMP Echo packets from our intelligent routers to the open Internet are not dropped. They come back without disappearing. Thus, the onset of the GS block can be easily missed if packet-loss is used. Eventually, packet-loss ratio cannot show the onset of (GS) blocks. Meanwhile RTT increase ratio reflects it much better because the RTT increase at the onset of GS blocks is abrupt.

エラー! 参照元が見つかりません。 shows the RTT of an ordinary day when no block was observed. Neither staircase nor abrupt RTT increase was detected. Even the maximum RTT was around 250ms. Open (public) Internet could be used all the day without significant delay or without business stop. However, this is one of confusing or borderline cases. Indeed, the RTT increased as the time of day passed. It continued to be mostly more than 200ms during 8:30-22:30 as shown in エラー! 参照元が見つかりません。. Rule 1 without RTT differential calculus would have taken this as GS blocks continuing 14 hours, even if the absolute *starting threshold ts* is set as 200ms. However, the switch to VPN bypass did not occur owing to differential calculus of RTT. The differential value of RTT did not increase so much. Even the maximum one was 10.3 % at 21:12:00 in

. This is much less than 30% of *tdf*.

Some readers may wonder why automatic switching based on RTT outperforms using the VPN link all the time. There are two reasons for this: first, permanently using VPN is costly. Our VPN bypass can partly use a leased line when the Internet is congested. Second, identifying and attacking the VPN gateway address should be avoided. Reducing the probability of successful sampling alleviates the chance of automatic entropy-based identification of VPN traffic. Thus, we need to use the VPN only for emergencies.

Each red line in エラー! 参照元が見つかりません。 and エラー! 参照元が見つかりません。 shows the RTT of the Internet on various real GS blocks. On GS blocks, the bypass was switched and the resulting RTT of the bypass remained stable below 150ms. This is shown by blue lined Bypass Link of エラー! 参照元が見つかりません。 and エラー! 参照元が見つかりません。 (the third column digits of Table II).

As a result of differential calculation of the RTT increase (Step 2), our intelligent router recognized the onset of GS. It was done at the early part of the staircase. Immediately and automatically, it switched to the stable bypass before offshore users notice the network latency. Once GS block was removed it smoothly switched back to the Internet (Step 2).

In order to analyze the behavior of RTT of ICMP Echo packets in the Internet depicted in Fig. 6 when GS occurred, a simulation model was developed on ns-3 [37][57]. The ns-

3 is a discrete-event network simulator for Internet systems. Though the mechanism is not disclosed the case of each international communication channel being step-wisely blocked (through almost perfect shaping etc.) by the governmental authority is simulated. Here, speculating from the phenomenon of RTT increasing in staircase form shown in Figure 9, the followings are assumed in the simulator. 1) Each channel is blocked to check the suspected sites step by step. 2) Some international communication channels are blocked and totally international communication is limited by authorities. 3) The latency or speed of each international communication channel is assumed to be different. 4) Each channel is blocked by the communication equipment (hardware) or the routing table.

As shown by figure 7, the simulation results showed (1) the abrupt stepwise increase on GS due to net detour and (2) it seems effectively detected by RTT first derivatives, which is a long sequence of numbers close to zero immediately followed by a short period of number close to one, which immediately decreases to almost zero again.

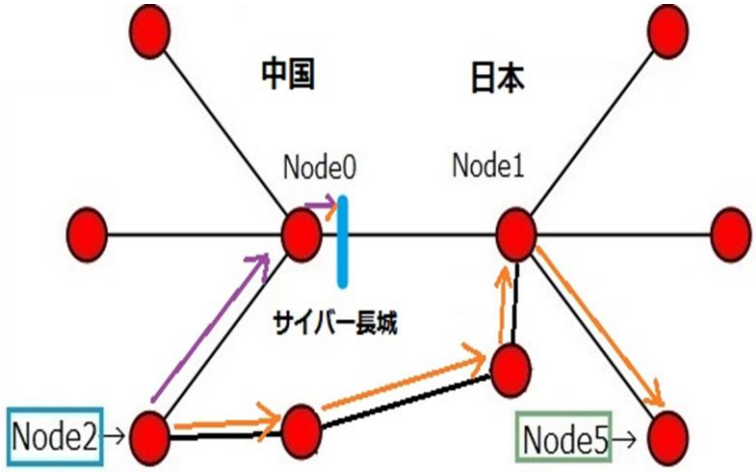

Fig. 6: Analysis of the behavior of RTT of ICMP Echo packets

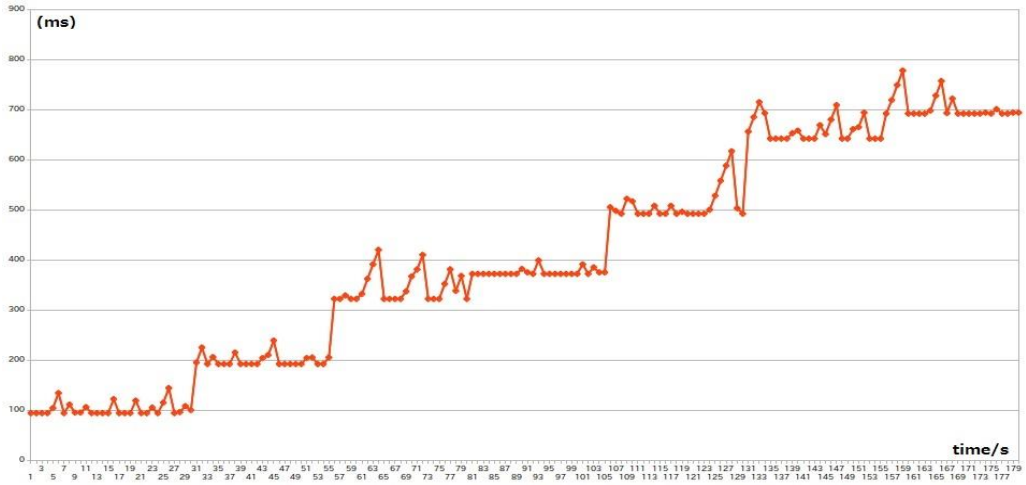

Fig. 7: Simulation results

4. EVALUATION

4.1 Evaluation on real GS block and non-GS data

This chapter evaluates (Step 1) through (Step 2) especially Rule1 and 2 of the method proposed in the previous chapter. Section 4.1 individually but concretely evaluates the effect of differential calculus. Only typical but somewhat borderline cases are used though selected out of more than 100 datasets on real GS block, business continuity as well as cost/safety (due to less bypassing time) are evaluated. As to the threshold values, the actual ones during the year 2015 are used as follows. Namely, *differential threshold: tdf=30%* per *difference width: tw=360* sec, and *starting threshold: ts=140*ms, *ending threshold: te=200*ms, *continuation time: tc=30*min. GS blocking usually happens every two or three days. GS blockings happened more than 150 times in the year 2015. Generally, the RTT increases sharply and/or abruptly at the onset of GS blocks. The increase curve is shaping steep staircases of 1-7 steps.

As for business continuity effects, エラー! 参照元が見つかりません。 shows the RTT graph on a typical GS attack. This graph has four steps of staircases observed at 14:06:00, 15:18:00, 16:36:00 and 17:42:00. Table II quantitatively shows four tuples of RTT and RTT increases. They are (269ms, 43.1%), (390ms, 20.0%), (578ms, 15.8%), and (702ms, 24.9%), respectively at each of those four steps. Utilizing Rule1 in (Step 2) with *ts*, *tdf*, and *tw mentioned above*, the proposed system successfully detected the GS attack. It was at 14:06:00 having the tuple (269ms, 43.1%). This is because 269ms is longer than *starting threshold ts =140*ms and 43.1% is higher than *differential threshold tdf= 30%* per *difference width tw=360*sec. Then, it automatically and immediately switched from international channels of the open Internet to VPN bypass. It was in time for avoiding heavy response delay such as 330ms at 14:12:00. The RTT was kept below 150ms of bypass link RTT. The RTT is shown in the lower parts of エラー! 参照元が見つかりません。 and the third column of Table II.

However, this case namely GS detection at 269ms of RTT is somewhat borderline. The RTT increases close to 300ms, clients sometimes notice the access deterioration. Though a very little, clients may notice what happened in the Internet communications.

Anyway, this resulted in an almost seamless communication bridge. Users could continue their business operations.

As to another business continuity effect, エラー! 参照元が見つかりません。 shows several sudden RTT changes especially due to GS attacks. However, as shown above, the network was successfully virtualized in case the proposed differential method is used. Meanwhile, if systems wait for RTT exceeding the absolute threshold (e.g. 270ms with *tw* kept and no *tdf* considered), users would experience deterioration. That is, RTT abruptly increased from 269ms at 14:06:00 to 330ms at 14:12:00. This is shown in Table II. Thus, judging only based on the absolute threshold is unstable. Using the first derivative, systems could predict GS effectively before users are aware of significant latency.

エラー! 参照元が見つかりません。 shows the RTT graph of another typical borderline case having just one-step (type of) GS attack. This explains a business continuity effect furthermore. Table III indicates the abrupt RTT increase at the attack (GS block) time. Again using Rule1, at 13:36:00 our system recognized the GS block. Namely it detected the abrupt RTT increase (RTT increase ratio **67.8**%). This is higher than *differential threshold tdf* =30%. At this time, RTT was 250ms, which is more than *starting threshold ts* (= 140ms). Then it immediately switched to the VPN bypass. The RTT became around 150ms of Bypass Link RTT as mentioned above. Again this is a borderline case. When RTT becomes 250ms, users may experience the network latency. However, only a little if such a case happens. Thus users could continue business.

As to VPN bypass link duration, the time to return to the open Internet was at 2:36:00 in Table III for エラー! 参照元が見つかりません。. At that time, VPN bypass ended according to Rule2. This is because RTT between *189ms-136ms* which is less than the *ending threshold te= 200*ms, continued from 2:06:00 *to* 2:36:00 which is more than the *continuation time tc=30*min. This switched back to VPN bypass again at 13:36:00 on detecting GS block. The day had two GS blocks shown in エラー! 参照元が見つかりません。 (digital data in Table III). The VPN bypass link duration was confined within 11 (= 24-13) hours (ignoring the next day).

Again concerning VPN bypass link duration,

shows the RTT data of a non-GS day. However, this is also a borderline (confusing) case. RTT reached a maximum value of 253ms at 10:24:00. Tuples of RTT and its in-

crease ratio on each of large ones were as follows. Namely, (217ms, 3.69 %) at 10:12:00, (239ms, 6.22 %) at 10:18:00, (253ms, 5.86 %) at 10:24:00, and (224ms, 10.3 %) at 10:30:00 as shown in

. None of these was more than 30 % in RTT increase ratio. Thus, even on such a congested day or a borderline case, VPN bypassing did not occur owing to our method exploiting differential calculus of RTT. Indeed, RTT exceeded 250ms. But users' experiencing of network latency and business discontinuation due to GS block did not happen.

4.2 Discussion

As another borderline or confusing case, the RTT increase ratio sometimes decreases at the onset of GS blocks. This is due to the bandwidth (namely, speed) increase of international channels. Decrease of the temporal or periodic (e.g. decrease every early morning) traffic volume also has influence. Anyway, there often occurs around a half of an ordinary step rise (usually 100ms or more).

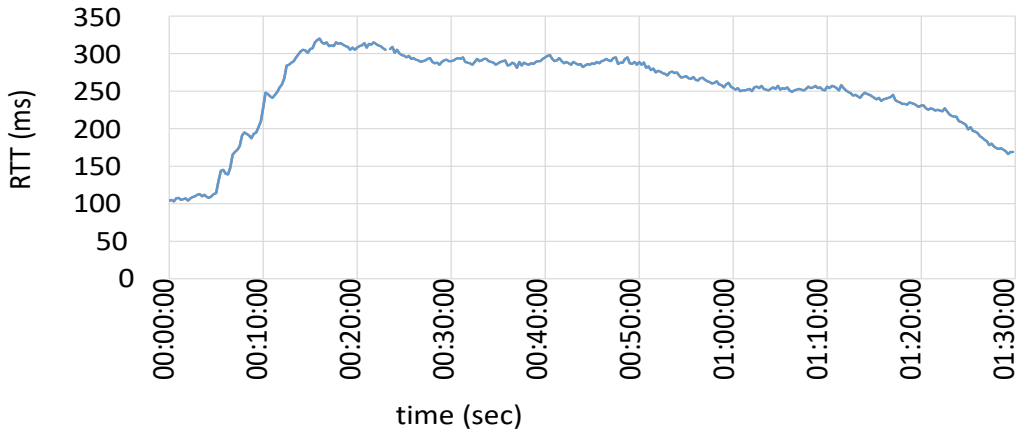

Fig. 8: RTT on GS (false-negative error if measured per 30ms)

Table IV: RTT increase ratio on GS of Fig. 8 (false-negative error if measured per 30ms)

RTT (ms)	Increase ratio (%) per 30ms	Increase ratio (%) per 90ms
177	4.7	26.4
191	11.1	37.4

195	10.2	31.8
⋮	⋮	⋮
320	1.6	5.3

If such a small step rise of RTT as continues successively, our method may not be able to detect the onset of GS. For example, if RTT increases as follows: 135ms -> 175ms -> 220ms -> 280ms, *differential threshold tdf* does not exceed 30 % and the switch to VPN cannot occur. Such cases can happen when the neighbor international channels are successively blocked and the international channel currently being used is abruptly but shortly or half-way delayed by packets from the neighbors. However, such (false negative) errors occurred only four times at most out of 159 GS blocks in the year 2015. The error rate was 2.5%.

A histogram when the proposed method detected the onset of GS blocks was made for the purpose of statistical and more formal analysis. Around forty examples were used. The average: m was 222ms. The standard deviation: *s* was 27ms. The histogram was approximately Gaussian. The average is almost equal to the median 220ms, the average standard deviation is about 25 ms. The graph of RTT at the y-axis and time at the x-axis is almost symmetric and follows the Gaussian distribution

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$$

with μ being the expectancy value and σ^2 being the variance. The probability over $m + 2*s$ is less than 2.5% in statistical estimation theory. Thus (m=222, s=27) means less than 2.5% of GS blocks is estimated to be detected at longer than 276ms (=222+27*2) of RTT when users sometimes feel GS. Namely, the statistically estimated error rate is less than 2.5%. This is almost coincident with the error results in 2015 since the number of false negative errors was 4 among 159 times of GS blocks. Therefore, the probability of GS block detection at more than 303ms (m + 3*s =222+27*3) of RTT when business users usually feel GS is estimated less than 0.15%, almost 0. Thus, the proposed method can keep business continuity.

Meanwhile, assuming the absolute threshold 250ms only was used for GS block detection, a histogram was made too. This histogram was also approximately Gaussian (symmetric and average: 304ms (303.5ms) almost equal to median: 304.3ms). The standard

deviation was 23ms. Since the probability over m + s is more than 15% in statistical estimation, more than 15% (24 errors among 159 times of GS blocks) is estimated to be detected at longer than 327ms (*m*+*s*=304+23) of RTT. Since RTT becomes longer than 300ms business users can be easily aware of GS and business discontinuities happen. Using only the threshold: *ts*=200ms, the average was 245ms (median = 246ms) and the standard deviation was 14ms. Therefore, more than 15% (24 times among 159 times of GS blocks) was estimated to be detected at longer than 259ms (m+s=245+14) of RTT.

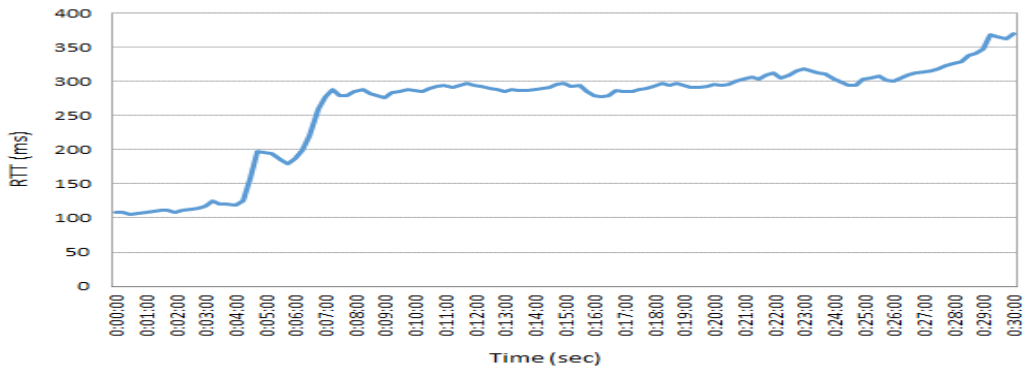

Fig. 9: RTT on GS (false-negative error if measured per 15ms)

Table V: RTT increase ratio on GS of Fig. 8 (false-negative error if measured per 15ms)

RTT (ms)	Increase ratio (%) per 15 ms	Increase ratio (%) per 30 ms
159	27.2	33.6
198	24.5	58.4
⋮	⋮	⋮
220	10.6	17.6
259	17.7	30.2
278	7.3	26.4

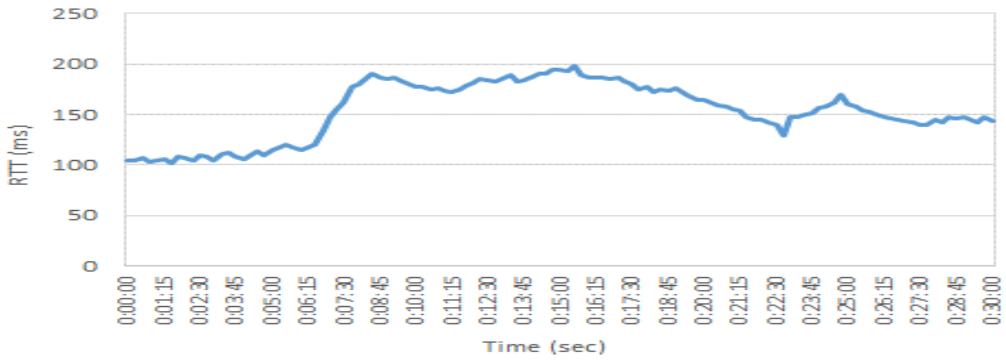

Fig. 10: RTT on an ordinary day (false-positive error)

Table VI: RTT increase on non-GS of Fig. 10 (false-positive error)

RTT (ms)	Increase ratio (%) per 30ms	Increase ratio (%) per 90ms
148	23.3	28.7
155	14.8	32.5
162	9.5	35.0
178	14.8	50.8
⋮	⋮	⋮
190	5.6	58.3
187	1.1	38.5
185	-2.6	25.0

Since RTT becomes so longer than 259ms, business users can become aware of GS and business discontinuities happen. Especially, in this case of using only ts (=200ms) for GS block detection, bypass is switched almost all day. This can be readily known from エラー! 参照元が見つかりません。 (quantitatively

) on a non-GS but congested day. There are many such days (e.g. every three days) as shown in both Fig. 1 and エラー! 参照元が見つかりません。 in China.

These results show our system can virtualize offshore information access routes or seamlessly connect international channels. Clients do not experience significant latency hindering their business. GS occurs around three times per week. エラー! 参照元が見つかりません。 and エラー! 参照元が見つかりません。 are similar in their steep staircase shapes, though the number of the step is different. Our approach focuses on

steep or sharp staircase increase in RTT. It is effective to quickly predict GS blocks, as shown by the data of

trough Table III and the statistical analysis mentioned above. Indeed, the proposed method well predicted the onset (start) of GS blocks at the sufficiently early timing of the RTT stepwise increase. This was shown by the following two facts: 1) RTT increase ratio becomes more than 30% on a day having GS blocks as in Table II and Table III) RTT increase ratio is less than 30% on a day having no GS as in

. Such prediction was useful to keep business communications stable.

4.3 Improvement by multiple threshold values integration

Recently, the interval between each staircase step has become shorter. It changed from several hours to tens of minutes. As well, each step's height has become smaller (e.g. less than 30% of RTT increase ratio) as in Table IV (corresponding to Fig. 8).

In reality, RTT increase ratio per (tw=) 30ms in Table IV is much less than (tdf=) 30% (even the maximum value is 11.1%). Never the less, RTT in Table IV becomes 320ms. This makes it difficult to predict the onset of blocks before 300ms of RTT more than which users experience delay. We can simply lessen the threshold of the first derivative. However, it causes false positives too often, misjudging as blocks despite the absence of GS.

To avoid this false-positive error, we propose the integration method of multiple thresholds of derivatives per various intervals. This is such as OR combination of 25 % per 15 seconds, 30% per 30 seconds, and 35% per 90 seconds. Due to such threshold integration (a sort of simple sensor fusion), our system can detect GS blocks before users notice intolerable network latency such as more than 300ms of RTT. For example, the RTT is 191ms (37.4% per 90ms: over 35% in Table IV for Fig. 8) and 159ms, perfectly 198ms (58.4% per 30ms: over 30% in Table V for Fig. 9).

Meanwhile, even on non-GS (Fig. 10), our system switches when RTT is 178ms (in Table VI). However, 30 minutes later it switches back. In case of non-GS shown in Fig. 10 (エラー! 参照元が見つかりません。 also), RTT is usually below 200-300ms all day. Thus, it switches back by the rule of Step 3 "switch back if RTT is below *ending threshold*: *te* for longer than *continuation time*: *tc* (=30 minutes)".

Even if no GS sign, it is useful to detect abrupt /sharp RTT increases and switch to bypass. Such sharp RTT increases often cause jitters (fluctuations). Only jitters can irritate business users in Web conferences (voice, video) and such. Thus, these false-positive errors become fortunate errors. Of course, it is a little harmful to shorten the VPN bypassing period against censoring. But it is useful to cope with sharp increase of network latency annoying business users in their usage of latency-sensitive applications. Still more, such miss-switched (false-positive error) duration or occurrence can be easily adjusted. For example, *ending threshold te* (maximum RTT on non-GS days) can be adjusted between 200-300ms. Further, the *continuation time (*elapsed time threshold*)*: *tc* can be relaxed a little more between 15-90 minutes.

Our evaluation showed that differentially switched VPN enables dependable offshore information systems. In these systems, clients of offshore offices in China can stably access servers in Japan even on GS. Thus, offshore users can continue business without experiencing quality deterioration of access to motherland servers. Successful usages of more than fifty offices over 3 years also validated such effects. Our intelligent router's differential prediction was combined with the immediate automatic switch to VPN bypass. Users are not hindered with their business even on real blocks by the Golden Shield (GS).

5. EVALUATION OF OFFSHORE APPLICATION SUPPORT QUALITY

5.1 Application Quality Evaluation by Analysis

Web/audio conferences are important for offshore business information systems. For example, VoIP communication in audio conferences is increasingly widespread on the global Net. However, VoIP voice quality suffers in critically non-isochronous environments showing high RTT variance. Intentional governmental restrictions such as GS can cause such a quality loss by sharp /steep staircase RTT increase.

In order to alleviate this quality loss, many algorithms have been proposed to recognize and eliminate acoustic echo and noise. The performance of some echo cancellation algorithms is analyzed in critically non-isochronous environments. Such analysis shows PBEC is effective if the size of the packets taken into account remains above a threshold [5]. PBEC is Packet-based Echo Canceller approach. The joint adoption of PBEC and of an advanced Jitter Buffer is also useful.

Indeed, GS blocks cause abrupt increase of the RTT. But, our intelligent VPN router for our bypassing system can recognize GS at the early stage before GS blocks increase RTT drastically. Namely, the network is switched to VPN bypass so that the RTT can remain around that of VPN (150ms). The WeChat system [54] is permitted and usually used in China where GS blocks occur. Such systems or gateways have Echo Canceller and sufficient buffer for strengthening the Echo Canceller. This kind of Echo Canceller perfectly guarantees the successful echo-cancelation if RTT is below 200ms. Further, it mostly guarantees if RTT is below 300ms.

The proposed VPN bypassing method guarantees below 270ms of RTT or so. Therefore, neither delay nor echoes /jitters can almost be expected in audio /Web conference. Thus, the proposed method can realize seamless virtual network for international business continuity.

5.2 Application Quality Evaluation by Questionnaires

A negative impact on their business from Internet censorship is reported by 4 out of 5 of member companies. It is a statement by The American Chamber of Commerce in China [2]. Thus, the ultimate user effects of our seamless virtual network exploiting differentially switched VPN were evaluated on GS attack. Thus, the following user level (i.e. application level) questions were posed to 24 offshore companies of our clients in China:

(1) Did you feel image/voice data delay (on such as during the onset of a GS block) in Web conferences?

(2) Did you have stressful experiences of heavy response on connecting with offshore clouds?

(3) Did you irritate in transferring large amounts of files such as CAD and Video data on GS?

(4) Did you feel general inconvenience (causing business discontinuity) or incur high expense?

Each item has the following selections: A. problems, B. small problems, C. no problem

Results were as follows:

(1) All but three companies answered as C (no problem). To the item 3, three companies answered as B and to the other items, they answered as C (no problem).

(2) One of these three companies has its headquarters in Singapore, where the communication channel itself is relatively poor.

(3) Others have the contract with a service estimated or noted as minor clouds even on domestic usage in Japan.

Thus, we had the 24 companies evaluate the suitability of the proposed method. Mainly seamless response was asked in multimedia communication necessary for Web conferences among headquarters, branch offices, and offshore offices across the border. These results validated that our proposed method and system work well in offshore business

applications. With reasonable cost, the seamless international communication was realized under some intentional restrictions.

Generally, each country has multiple international channels for the Internet. Each channel has different speed depending on its route length as well as performance. If the national government finds inconvenient sites outside the country, some of international channels may be blocked step by step. Therefore, abrupt steep staircase increase of RTT occurs and business continuity is disrupted. Since this is a fairly general scenario, the proposed method using differential calculus with the threshold adjusted can be adaptively applied for other than China.

Though other type of shape may appear, a staircase shape RTT is seemingly the most difficult case to keep business continuity. Further, governments dare not to create more difficult shapes since their firewalling (GS block) is not targeting business continuity disruption. Thus we can expect RTT increases gradually in other shapes. Suppose RTT gradually and linearly increases always (e.g. 10ms per 360sec) to more than 300ms. It can be detected by the absolute threshold only before users notice heavy response. However, the proposed method has the absolute threshold also and differential thresholds can be invalid by relaxing it to 0. Thus, it can be expected to easily handle such somewhat gradual slopes of RTT increase and to keep the business continuity.

6. RELATED WORK AND BACKGROUND

Our method transfer data through bypass routes provided by the underlying IP network layer. Thus, it is taken as an overlay network. In other words, the bypass is managed not by network carriers (who may set up the blocks) but by users. Namely, the bypass is managed by users' intelligent routers who automatically switch to alternatives from blocked paths.

A typical overlay network is a peer-to-peer (P2P) system. A peer can have a stable identity and neighbors in the overlay layer while changing continuously its IP address [16].

There are various P2Ps such as Bittorrent [14], Tor Project [18], and content delivery/distribution network (CDN [23]). Overlay networks such as CDN have many mirror sites to copy the redundant files. CDN distributes them from the optimal site, usually from the neighbor site. It is very efficient. However, it is expensive to maintain many mirror sites especially with the real-time synchronized update.

VPN is also an overlay network. Various VPNs are available: IPSec [31] on Layer 3 and L2TP [33] on Layer 2; PPTP [27] often used as a de-facto standard; SSL-VPN (VPN via SSL). Our system automatically switches to VPN to avoid blocks of public (open) Internet links and keep network response for offshore services.

STT [17] is also an overlay network technology. STT is used in SDN (Software Defined Network) for network virtualization [32]. Network virtualization creates multiple virtual networks shared among multiple-tenants in a data center. Such virtualization by overlay networks is promising. Some overlay type network virtualization methods such as STT have dynamic switching functions. However, they are usually limited within data centers of homogeneous (same provider's) AS. They do not easily work among heterogeneous (different provider's /policy's /goal's) ASs across the border.

Indeed, overlay network technologies are useful in alleviating the partitioning of the underlying IP networks. They can force more optimal routes or bypasses than optimal routes of public internet calculated by BGP etc. Recently, software-defined overlay by-

pass methods using VPN have been proposed for Inter- and Intra-cloud Virtual Networking [29]. They can avoid structural problems such as trombone routes [51][44].

Our method also uses VPN bypass. However, GS blocks let RTT extremely sharply increase in a steep staircase shape. Offshore business continuity needs not only automatically detecting the onset of GS but also bypassing before users become aware of GS blocks. Our method exploits multiple threshold integrated differential calculus. This can recognize the steep staircase waveform of network delay by GS in the early stage before business users are aware of deterioration. Overlay network or VPN itself does not have such function. They can scarcely cope with predicting abrupt or steep staircase RTT increases caused by intentional blocks such as GS.

MON [25] is a multilayer overlay network against Denial-of-Service (DoS). In MON, DDME [28] monitors the packet rate of all the incoming flows. If the rate exceeds the threshold, packets of the flow are “punished” (i.e. dropped). However, this is not applicable if attacks are performed to networks under no control of users as in GS.

A stateless spread-spectrum paradigm [45] encodes data into hashes sent safely via multiple paths on overlay networks. Responsive multiple paths with hash coding are costly, while even one dedicated line to data centers in Japan [49] is costly. Our method uses just one VPN path, easily or alternately operated on censoring or deterioration.

There is also a product, made by Yamaha NetVolante [57] which automatically diverts to the ISDN line prepared beforehand when the Internet is completely shut down due to malfunction of equipment etc. However, even while GS is in operation, the Internet is not shut down completely. Thus, it automatically diverts and it will not lead to stress reduction of Internet users.

Recently, for traffic differentiation detection, NetPolice [56] or NVLens [55] compares the aggregate loss rates of each flow. It infers “network neutrality violations” in backbone ISPs.

NANO [47] uses causal inference. DiffProbe [30] uses active queue management (AQM) such as random early detection (RED) and weighted fair queue. AQM complements Glasnost [20].

Monkey [10] takes a packet-level trace. It generates a trace of network-level properties such as latency and bandwidth. More recent work [15] infers higher-level protocols from

low-level packet traces. PlanetLab [43], RON [3], and NIMI [42] are measurement systems for researchers.

Netalyzr [50] is a web-based tool to detect traffic blocking or content manipulation by a HTTP proxy. “Glasnost”, “Test Your ISP” Project [21], DIMES Project [48] and the Measurement Lab [36] help detect Internet blocks or differentiation by an easy-to-use interface. Network Diagnostic Test (NDT) [8] captures detailed connection statistics. To detect differentiation between applications, Glasnost collects RTT (round trip time), TCP throughput, UDP jitter and datagram loss, etc. Glasnost compares the throughput of a pair of flows to check differentiation. However, to overcome the noise interference, flows are running many times. This is expensive and subject to censoring.

Measurement software [7] collects data by iPerf [38] and a ping tool. The iPerf measures TCP throughput/bandwidth and UDP data-loss/jitter. These many works focus on packet loss to detect traffic differentiation or blocks. Even the ping tool provides the minimum, maximum, and average of RTT (absolute value) to indicate packet loss. Meanwhile, our unique method uses first derivative on RTT to detect the abrupt/steep staircase latency increase that is typical of GS.

In the past few years, cloud computing has provided many opportunities for enterprises. It offers their customers a range of computing and networking services. Cloud computing frees enterprises and end users from specification details such as storage resources, computation limitation and networking cost. However, this becomes a problem for latency-sensitive (RTT dependent) applications. Such applications require nodes in the vicinity to meet strict delay thresholds. This also applies to situations like the China Golden Shield. Namely, the Internet latency seen by network nodes is controlled by an adversary, potentially disrupting the functionalities of applications.

An emergent paradigm SDN separates control from data communication layers. SDN solves the problem of latency control inside the cloud. This is because it can control latency between virtual addresses in the cloud by remapping such addresses to meet the latency thresholds. SDN latency control can be exploited for attacks [4]. Meanwhile, it can also be used to enforce uniform latency. [34] discuss how to provide open APIs to SDN routers for network-as-a-service application development. Their proposal does not

explicitly mention latency control. Nevertheless, it would allow writing applications to manage latency according to requirements.

SDN may control distance and therefore latency between two virtual network interfaces in the cloud. Unfortunately, it cannot control latency on an external network interface between public internet and the cloud accessing IP addresses. A way to address this latency problem is fog computing [46].

In vehicular networks, fog computing is already used together with a (centralized or distributed) server capable of reconfiguring the mobile node addresses. Different from our RTT's first derivatives are not used. But, "neighborhood" between addresses is managed by the server on the basis of the nodes relative position and speed. Therefore, the server can keep latency (RTT) between any two nodes as uniform as possible. In principle, the same concept can be used to keep uniform latency on an overlay network even when latency in the underlying IP layer is controlled by an attacker.

A remapping and migration method for Cloud and Fog resource providers was proposed by [41]. Their technique enforces application-defined end-to-end latency restrictions and reduces the network utilization by planning the remapping/migration ahead of time. Network intensive operators are placed on distributed fog devices while computationally intensive operators are in the cloud.

At the moment there is little industrial support for this approach. Cisco has recently delivered their vision of fog computing. Devices already connected in the Internet of Things (IoT), run directly at the network's edge. Customers can develop, manage and run software applications on the Cisco IOx framework of networked devices. Networked devices include hardened routers, switches and IP video cameras. Cisco IOx brings the open source Linux and Cisco IOS network operating system together in a single networked device. They are brought together initially in routers. Latency control has not yet emerged as a goal in Cisco open application environment. However, it encourages more developers to bring their own applications and connectivity interfaces at the edge of the network especially for latency-sensitive applications [22].

Latency-sensitive applications require meeting strict delay thresholds. As for such applications, VoIP communication is increasingly widespread on the global Net. However, VoIP voice quality suffers in highly non-isochronous environments. Such environments

exhibit high RTT variance. However, putting address remapping functionalities on the edge also raises some specific security concerns. This makes it easier to spoof IP addresses and to perform Man-in-the-middle attacks. These have the potential to become a typical attack in Fog computing. Support for strong authentication must be provided.

To alleviate this quality loss, many algorithms have been proposed to recognize and eliminate acoustic echo and noise.

In [5], the performance of echo cancellation algorithms is analyzed in critically non-isochronous environments. As a result, a PBEC (Packet-based Echo Canceller) approach has proved effective if the packet size satisfies a threshold. Their work also discusses the joint adoption of PBEC and an advanced Jitter Buffer. As mentioned in the section 5.1, such a work is useful for business continuity to cancel echoes resulting from bypassing.

7. CONCLUSION

Seamless virtual network technology was proposed as business solution towards economic prosperity of developing countries. Differentially switched VPN bypass was utilized. It avoided blocks of international bridging channels and continues business communications. The seamless features were as follows:

(1) the onset of GS blockage is recognized, exploiting the multiple threshold integration types of differential calculus combined with absolute (*starting*) threshold,

(2) immediately followed by switching to the VPN bypass before serious network latency starts.

(3) Asymmetrically, the absolute (*ending*) threshold and *continuation time* (elapsed time) was used to determine the end of bypassing.

This method was evaluated to be successful using around 200 cases of GS data (4 errors out of 159 cases, around 2.5% false negative errors in 2015).

In offshore applications, our method alleviated response time in Web conferences and throughput in business file transfer. As well, it solved the voice echo problems and jitters in Voice and Video that irritate business users. All of them were validated by questionnaires to our customers of 24 companies in their offshore business application usage.

In many situations, governmental blocks on Internet links conflict with normal business activity. In this paper, we argue that this situation is not exceptional, and has become part of regular (every 2-3 days) activity. Therefore, a way of coping with it must be found. We disclosed and improved the RTT-based method to detect the onset of blocks introduced by the Chinese GS system.

Then, we presented and, more thoroughly, validated such an improved version of our most recent solution [24]: Network Virtualization Using VPN for Stable Communication with Offshore Cloud. This system is a concrete contribution towards preserving the functionality of international business communication and economic activity under an intermittent governmental block. This method has been applied to international communication channel in more than 20 offshore companies for three years. Also, this paper validated the effect of our solution over the operation of the set of application-level protocols

that can guarantee business continuity. The solution is believed to mitigate the negative impact of governmental interference in the operation of their communities' links to the global Internet. This preserves the minimum continuity needed for economic activities.

REFERENCES

[1] N. Abramson. 1970. The Aloha System: another alternative for computer communications. In: AFIPS 1970: Proceedings of the fall Joint Computer Conference, November 17-19, pp. 281–285. ACM.

[2] Amcham China: American Chamber of Commerce in China. 2016 Business Climate Survey, retrieved on May 29, 2016 from http://www.amchamchina.org/policy-advocacy/business-climate-survey/

[3] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris. 2001. Resilient Overlay Networks. Proc. of SOSP.

[4] C. A. Ardagna and Ernesto Damiani. 2014. Network and Storage Latency Attacks to Online Trading Protocols in the Cloud. On the Move to Meaningful Internet Systems: OTM 2014 Workshops. Vol. 8842. 192-201. DOI:10.1007/978-3-662-45550-0_20

[5] D. Benetti, E. Damiani and P. Houngue. 2008. VoIP echo suppression in critical environments. 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, Phitsanulok, 558-562

[6] R. Beverly, S. Bauer, and A. Berger. 2007. The Internet's Not a Big Truck: Toward Quantifying Network Neutrality. Proc. of the Passive and Active Measurement Conference (PAM).

[7] Y. Byun, S. Narayanan, S. Mottand K. Biba. 2013. Wireless Broadband Measurement in California, 10th International Conference on Information Technology: New Generations (ITNG2013), pp. 505 - 509, DOI: 10.1109/ITNG.2013.85.

[8] R. Carlson. 2003. Developing the Web100 Based Network Diagnostic Tool (NDT). Proc. Passive and Active Measurement.

[9] K. Chen and C. Hu. 2011. Border gateway protocol monitoring system can be cost effective. Communications, IET Journals & Magazines, vol. 5, issue 15, pp. 2231-2249.

[10] Y.-C. Cheng, U. Hoelzle, N. Cardwell, S. Savage, and G. M. Voelker. 2004. Monkey See, Monkey Do: A Tool for TCP Tracing and Replaying. Proc. of the USENIX Technical Conference.

[11] China State Council. 2003. Regulation of Commercial Encryption Codes. China State Council Directive No. 273, 2000.

[12] China's North-South Divide. 2016. IIJ GIO CHINA Service: Overview. retrieved on Jan. 21, 2017 from http://www.iij.ad.jp/en/svcsol/service/gio/china/

[13] R. Clayton, S. J. Murdoch, and R. NM Watson. 2006. Ignoring the great firewall of china. Privacy Enhancing Technologies. Berlin, Heidelberg: Springer.

[14] B. Cohen. The BitTorrent protocol specification BitTorrent.org. retrieved on March 24, 2016 from http://www.bittorrent.org/beps/bep_0003.html

[15] W. Cui, M. Peinado, K. Chen, H. J. Wang, and L. Irun-Briz. Tupni. 2008. Automatic reverse engineering of input formats. Proc. of CCS.

[16] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, F. Violante. 2002. A reputation-based approach for choosing reliable resources in peer-to-peer networks. ACM Conference on Computer and Communications Security 2002: 207-216

[17] B. Davie and J. Gross. A stateless Transport Tunneling Protocol for Network Virtualization (STT). Internet Draft. Draft-davie-stt-03.txt, IETF. March 2013.

[18] R. Dingledine, N. Mathewson, and P. Syverson. 2004. Tor: The second-generation onion router. Naval Research Lab.

[19] M. Dischinger, A. Mislove, A. Haeberlen, and K. P. Gummadi. 2008. Detecting BitTorrent Blocking. Proc. of IMC.

[20] M. Dischinger, M. Marcon, S. Guha, K. P. Gummadi, R. Mahajan, and S.Saroiu. 2010. Glasnost: Enabling End Users to Detect Traffic Differentiation. Proc. USENIX Symposium on Networked System Design and Implementation (NSDI), San Jose.

[21] EFF. “Test Your ISP” Project. retrieved on March 24, 2016 from http://www.eff.org/testyourisp

[22] C. Fraleigh; F. Tobagi; C. Diot. INFOCOM 2003. Provisioning IP Backbone Networks to Support Latency Sensitive Traffic. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies Year: 2003, Volume: 1 pp. 375 – 385 vol.1, DOI: 10.1109/INFCOM.2003.1208689

[23] M. J. Freedman, E. Freudenthal, and D. Mazières: Democratizing content publication with Coral, Proceedings of NSDI '04, San Francisco, CA, March 2004.

[24] H. Fujikawa, H. Yamaki, Y. Yamamoto, S. Tsuruta. 2015. Network Virtualization Using VPN for Stable Communication with Offshore Cloud. 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp. 200 – 207

[25] D. Geneiatakis, G. Portokalidis, and A. D. Keromytis. 2011. A Multilayer Overlay Network Architecture for Enhancing IP Services Availability against DoS. Springer ICISS 2011, pp. 322-336.

[26] greatfirewallofchina.org retrieved on May 29, 2016

[27] K. Hamzeh, et al. 1999. RFC 2637 - Point-to-Point Tunneling Protocol (PPTP). Network Working Group.

[28] J. Ioannidis and S. M. Bellovin.2002. Implementing Pushback: Router-based defense against DDoS attacks. Proc. of the Network and Distributed System Security Symposium (NDSS), pp. 1-8.

[29] K. Jeong and R. Figueiredo. 2016. Self-configuring Software-defined Overlay Bypass for Seamless Inter- and Intra-cloud Virtual Networking, Proceedings of the 25th ACM International Symposium on High-Performance Parallel and Distributed Computing, May 2016 HPDC '16, pp. 153-164.

[30] P. Kanuparthy and C. Dovrolis. 2010. DiffProbe: Detecting ISP Service Discrimination. Proc. of INFOCOM.

[31] S. Kent and K. Seo. 2005. RFC 4301 -- Security Architecture for the Internet Protocol. Network Working Group.

[32] T. Koponen, et.al. Network Virtualization in Multi-tenant Datacenters, Technical Report, TR2013-001E International Computer Science Institute UC Berkeley

[33] J. Lau, M. Townsley, and I. Goyret. 2005. RFC 3931 -- Layer Two Tunneling Protocol - Version 3 (L2TPv3). Network Working Group.

[34] S. Luo, K. Ota, M. Dong, J. Wu, J. Li, and B. Pei Toward High Available SDN/NFV-based Virtual Network Service in Multi-Provider Scenario, Proceedings of 2016 World Automation Congress (WAC), July 31-August 4, 2016

[35] B. S. Madden. 2003. Citrix Metaframe Xp: Advanced Technical Design Guide. Brianmadden.Com Publishing Group.

[36] Measurement Lab (M-Lab) retrieved on March 24, 2016 from http://www.measurementlab.net/

[37] National Science Foundation and the Planète group. retrieved on March 24, 2016 from https://www.nsnam.org/

[38] NLANR/DAST, iPerf, retrieved on March 24, 2016 from http://sourceforge.net/projects/iperf/

[39] D. Nobori, Y. Shinjo. 2014. VPN Gate: A Volunteer-Organized Public VPN Relay System with Blocking Resistance for Bypassing Government Censorship Firewalls. USENIX NSDI '14.

[40] A. Ootsuka, 2014. retrieved on January 20, 2017 from http://ascii.jp/elem/000/000/933/933306/ (in Japanese)

[41] B. Ottenwalder, B. Koldehofe, K. Rothermel, and U. Ramachandran, 2013. "Migcep: Operator migration for mobility driven distributed complex event processing," in Proceedings of the 7th ACM International Conference on Distributed Event-based Systems, ser. DEBS'13. ACM, pp. 183–194

[42] V. Paxson, A. K. Adams, and M. Mathis. 2002. Experiences with NIMI. Proc. of the SAINT Workshop.

[43] PlanetLab. retrieved on March 24, 2016 from http://www.planet-lab.org/.

[44] Run Skype for Business. 2016. Retrieved on Jan. 14, 2017 from https://www.citrix.com/content/dam/citrix/en_us /documents/products-solutions/run-skype-for-business-as-a-secure-virtual-app-with-a-great-user-experience.pdf

[45] A. Stavrou and A. D. Keromytis. 2005. Countering DoS Attacks With Stateless Multipath Overlays. Proc. of the 12th ACM conference on Computer and communications security (CCS'05), pp. 249-259.

[46] I. Stojmenovic and S. Wen. 2014. The Fog Computing Paradigm: Scenarios and Security Issues. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems ACSIS, Vol. 2 pp. 1–8 DOI: 10.15439/2014F503

[47] M. B. Tariq, M. Motiwala, N. Feamster, and M. Ammar. 2009. Detecting Network Neutrality Violations with Causal Inference. Proc. of the CoNEXT Conference, 2009.

[48] The DIMES Project. retrieved on March 25, 2016 from http://www.netdimes.org/

[49] The Global Broadband Speed Test. retrieved on March 25, 2016 from http://www.speedtest.net

[50] The ICSI Netalyzr. retrieved on March 25, 2016 from http://netalyzr.icsi.berkeley.edu.

[51] Viptela 2015. Retrieved on Jan. 22, 2017 from http://network-insight.net/2015/05/viptela-software-defined-wan-sd-wan/

[52] The Washington Post. 2016. China's scary lesson to the world: Censoring the Internet works. retrieved on March 25, 2016 from https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html

[53] WebSitePulse.com retrieved on May 29, 2016

[54] www.wechat.com retrieved on May 29, 2016

[55] Y. Zhang, Z. M. Mao, and M. Zhang. 2008. Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs. Proc. of ACM HotNets-VII Workshop.

[56] Y. Zhang, Z. M. Mao, and M. Zhang. 2009. Detecting Traffic Differentiation in Backbone ISPs with NetPolice. In Proc. of the Internet Measurement Conference (IMC).

[57] Yamaha co,ltd https://network.yamaha.com/products/routers/rt57i/index on dec.2017