Visibility of Scan Traffic Trends in Sparsely Populated Darknets

Kodai Mizutani, Daisuke Kotani(✉), and Yasuo Okabe

Kyoto University, Sakyo, Kyoto 606-8501, Japan
mizutani@inet.media.kyoto-u.ac.jp, kotani@media.kyoto-u.ac.jp

Abstract. The darknet is one of the main sources for obtaining knowledge of cyber-attacks. Maintaining a large-scale darknet may become difficult in the future due to the high demand for IPv4 addresses and the exhaustion of IPv4 address pool. In the case of reducing the size of the darknet for assigning more IPv4 addresses to users, it is necessary to understand how the reduction in address size will affect the visibility of the darknet, which refers to the degree of attack trends that can be understood. Darknet visibility is discussed from various perspectives, but this research focuses on visibility related to detecting signs of an attack on a specific port, especially the accuracy of change point detection based on time-series data representing the number of packet transitions on each port. We propose Sparsely Populated Darknets consisting of small address blocks as a way to reduce the size of the existing darknet, and report on the usefulness of this type of darknet. We compare Sparsely Populated Darknets with contiguous address darknet that consists of the same number of contiguous IP addresses as Sparsely Populated Darknets. Sparsely Populated Darknets showed higher visibility than contiguous address darknet in terms of trend changes in the number of TCP SYN packets on each major ports. Based on this, this paper reports the possibility of effectively utilizing a small number of IP addresses that are not assigned by an organization as Sparsely Populated Darknets.

Keywords: Darknet · Port scan · IPv4 address · Sparsely Populated Darknet

1 Introduction

A darknet is an unused IP address space, and legitimate network traffic is never destined for a darknet. However, a large amount of traffic is observed in the darknet. This traffic can be attributed to cyber-attacks targeting an unspecified number of IP addresses. Therefore, analysis of darknet traffic can contribute to gain recent trends of attacks. In fact, the darknet has been used as an information source of many researches, such as the Internet scanning [2], a measurement of the size of DDoS attacks [5], and IPv4 address utilization [1].

Currently working with NRI SecureTechnologies.

H. Duan et al. (Eds.): SecureComm 2023, LNICST 568, pp. 230–248, 2025.
https://doi.org/10.1007/978-3-031-64954-7_12

However, in recent years, IPv4 addresses have been exhausted due to high demand for IPv4 addresses. Due to the large address space of the darknet, there is a possibility that the darknet will be forced to release some of its IPv4 addresses and allocate them to users. However, without any strategy, reducing the size of the darknet may unintentionally changes the features of the darknet. Therefore, to reduce the address size of the existing darknet while maintaining its visibility as much as possible, we need to know what kind of the strategy we should follow to reduce the address size.

In this research, darknets with a contiguous address space are called "CD" (Contiguous address Darknet). And a CD before reduction is called "base darknet". A darknet with a distributed IP addresses is called "DD" (Distributed address Darknet). So Sparsely Populated Darknets mean DD.

We focus on DD as a method to reduce the address size of the darknet. In particular, we propose the type of DD that is composed of several address blocks, which is referred to as "DBD" (Distributed address Block Darknet). Each address block consists of contiguous some IP addresses.

As shown in Fig. 1, we believe that CD provides a detailed understanding of the tendencies of a small number of attacks, while DD provides a rough understanding of the tendencies of many attacks. This is because, when an attacker targets a specific address space, we can monitor the attack completely using CD if CD covers the address space being attacked, but DD usually covers a part of the address space being attacked thus can monitor only a part of the attack. Instead, DD samples address blocks from a large address space, so we will be able to see attacks to different address blocks at the same time. Therefore, when a base darknet needs to be reduced, it can be considered better to reduce from base darknet to DD than to CD.

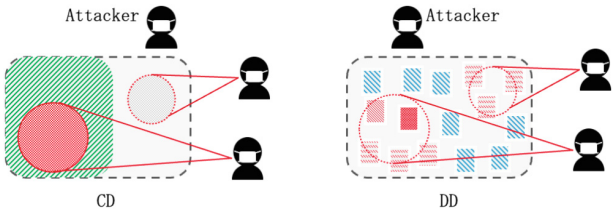

Fig. 1. Idea to have more visibility of DD than CD

"Visibility" refers to the degree of possibilities to understand attack trends, and the visibility of the darknet should be discussed from a variety of perspectives. This study focuses only on the visibility of trends in the number of packets on each port, and evaluates the visibility of DD's traffic trends by comparing to CD's traffic trends.

If the base darknet is reduced to DD and some IP addresses is released to users, the IP addresses of DD are present around active hosts. To fully evaluate the visibility of DD, it is necessary to actually release address of the base darknet to the user before evaluating DD. However, this prevents us from comparing traffic to DD with those to CD using the same address space. Therefore, in this research, as a preliminary step, we evaluate DD with no active hosts around the DD's IP address.

To evaluate the visibility of the number of packets and its trends in DD, a comparative analysis of DD and CD was conducted for TCP SYN packets, which are mainly observed in the darknet. The main findings of this study are as follows.

- In terms of visibility of trends of TCP SYN packets on each of the major ports, the results show higher visibility in DD than in CD.
- We investigated the timing of events reported in past darknet observation reports and found that DD can detect events closer to the base darknet than the CD.

2 Related Work

W. Harrop et al. [6] reported that a small number of unused IP addresses in a subnet to which active hosts also belong can be used to form a darknet as Greynet, which can detect scans at a useful level. The idea of Greynet, like the DD in this study, is to achieve visibility that is similar to that of a CD with a larger address space by a smaller number of IP addresses. The visibility of these DD has been evaluated in previous studies, which strongly suggests the usefulness of DDs. However, there is no discussion on the relationship between the number of IP addresses and visibility of the DD, and there is a lack of knowledge to provide concrete guidelines for downsizing the darknet to a DD.

While Greynet consists of a DD by sparsely allocating each IP address, our proposed method consists of a DD by sparsely allocating IP addresses in blocks, which can reduce operation and management costs compared to Greynet. Compared to Greynet, our results are the same in that it shows the superiority of DD. In this study, a large number of DD configuration are used to evaluate the superiority, which improves the credibility of the results.

Various institutes report information on targeted port or services based on traffic observed in the darknet [8, 9]. These reports activities that could be related to the attack, as well the vulnerabilities that caused it.

In this study, we use ChangeFinder [7] and Bollinger Bands [10] to detect anomalous changes. ChangeFinder is a method that scores the degree of change in time-series data through two-stage training of a time-series model. ChangeFinder outputs the large score when the change is large. Bollinger Bands is an anomaly detection method that uses moving averages and standard deviations. The speed and accuracy of change detection can be adjusted by the parameters of this method and can be changed flexibly according to the situation.

3 Dataset for Analysis

3.1 Base Darknet

The base darknet used in this study is the real /21 darknet that is operated by Kyoto University. Distributed and contiguous darknets are defined within the address space of the base darknet. Datasets from scaled-down distributed and contiguous darknets are extracted from packet data observed by the base darknet in the same period.

3.2 Distributed Darknet Composed of a Group of Small Darknets

In this study, we propose DBD consisting of several small darknets to reduce the number of IP addresses in the darknet while maintaining the same level of visibility as a darknet with a larger IP address space. Blocks of DBD are distributed in the address space of the base darknet. When the block size n is small, we can spread the blocks across the base darknet. However, when the DBD is managed by configuring routing information for each block in a router, the operation and management cost of the DBD will be increased when more blocks are configured as blocks of DBD. Therefore, we can reduce the operation and management cost when the block size n is large.

Originally, the notation /S ($0 \leq S \leq 32$) refers to a subnet with a contiguous address space with a subnet mask length of S bits. In this study, to simplify the expression of the number of IP addresses that compose a DD, the address size of a DD, CD, or each address block consisting of the same number of IP addresses with the subnet whose subnet mask length is /S is expressed as the "/S-scale".

The block sizes n used in the DD proposed in this study are 8, 16, 32, 64, and 128. Generally, the minimum route size exchanged between ASes as BGP routing information is /24 [3], so IP address space whose size is equal to or greater than /24 will be transferred to others if the whole /24 address space is not used. Thus, each block for the DD must be smaller than /24. Therefore, in this study, the maximum size of a block that composes a DBD is /25-scale (128 IP addresses). The minimum block size is 8. A block size of 8 is the same as a /29 network, and a block size of 16 is the same as a /28 network.

When a block is considered as a subset, we call the host part in the address of the subnet the block part. A block part of a block size 8 (/29) corresponds to the last 3 bits. The length of the block part is $\log_2 n$ for block size n.

The placement of the blocks is randomly determined to obtain a knowledge of the usefulness of the DBD regardless of location pattern of blocks. However, without any restriction on the placement of the blocks, the locations of the blocks in the address space of the base darknet may be extremely unbalanced. To avoid this, this study uses a simple rule for the location of blocks. Specifically, the base darknet is first divided into p subnets (hereinafter referred to as "divided darknet"). When base darknet is 10.0.0.0/21 and $p = 8$, the divided darknets are 10.0.0.0/24, …, 10.0.7.0/24. The same number of blocks are placed in each divided darknet to guarantee a minimum scattering of blocks. In this study, the size of each divided darknets is /24, considering that the maximum block size is /25.

To determine the location of a block within the divided darknet, an identification-bit-string is defined. The identification-bit-string starts after the prefix of the divided darknet, and identifies each block in the divided darknet. For example, when the size of the divided darknet is /24 and a block size is 8, the identification-bit-string in a DD is 5 bits long located at the 25th to 29th bit of a 32-bit IP address.

In this study, we configured two types of DBDs and evaluated the effects of the different configuration methods on their visibility.

The first type is a DBD with a common identification-bit-string, where the location of blocks in a divided darknet is common to all the divided darknets. Figure 2 shows an example of configuration in the /24-scale divided darknets with a block size of 8 from the

base darknet 10.0.0.0.0/21. The DD configured in this way is hereafter called “CDBD” (Common identification-bit-string DBD).

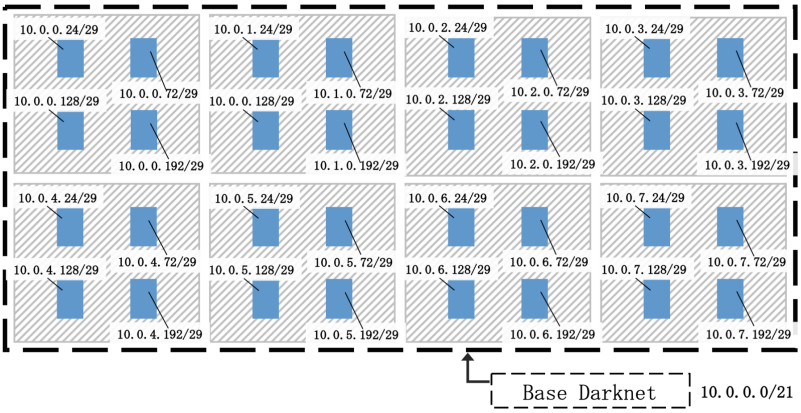

Fig. 2. Example of CDBD configuration

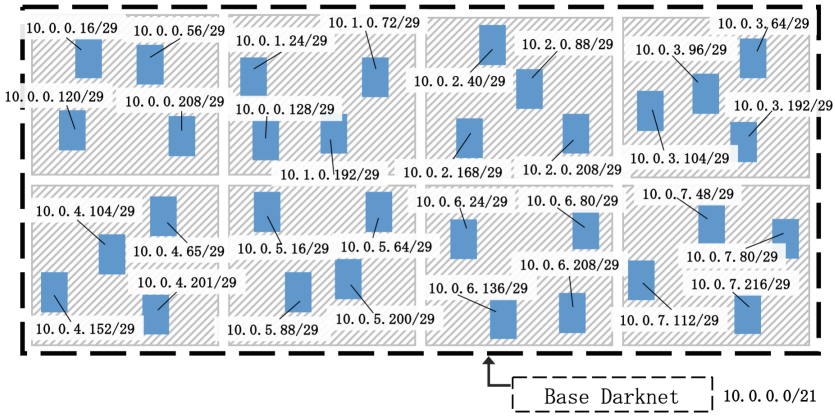

Fig. 3. Example of UDBD configuration

The second type is a DBD using a random identification-bit-string. This locates the blocks in a divided darknet randomly. The DBD constructed in this way is hereafter called a “UDBD” (Unique identification-bit-string DBD) as shown in Fig. 3.

Between each address size /23-scale to /27-scale, CDBD and UDBD are composed of 15 each. To be DBD, the number of blocks that are included in DBD should be at least two. When we select a block size of 32 and a DBD is /27-scale, for example, this DBD is essentially the same with CD. So, we carefully select a block size from {8, 16, 32, 64, 128} for each DBD so that CD is not extracted. Each DBD consists of the blocks in the same size. For each address size, the same number of DBDs is extracted per block size. For example in /26-scale DBD, 5 DBDs are extracted for each block size 8, 16 and 32.

3.3 Distributed Address Darknet by a Single IP

The simplest configuration method for DD is to randomly allocate single IP addresses in the base darknet. Although this method loses the advantage of the DBD, which can be configured with low operation and management costs, it will provide a similar IP address layout with Greynet, which consists of a small number of IP addresses scattered in a network with active hosts. The DD constructed in this way is hereafter called as "RDD" (Random deployment DD). For example, in the case of configuring a /24-scale RDD, 256 IP addresses are randomly selected from the base darknet, 4096 addresses (/21) in our data.

In this study, we configured 15 RDDs for each size of RDD from /23-scale to /27-scale, for a total of 75 RDDs. We used them for comparative analysis with DBDs of the same address size.

3.4 Contiguous Address Darknet

CD (Contiguous address Darknet) is prepared for comparison to evaluate the usefulness of DDs. Each CD is a subnet of the base darknet.

In this study from /21-scale base darknet, 4 /23-scale CDs, 8 /24-scale CDs, 16 /25-scale CDs, 32 /26-scale CDs, and 32 /27-scale CDs are extracted. Note that for the /27-scale CD, only half (32) of the 64 possible configurations from the base darknet are included in the analysis. Since the number of darknets other than the /27-scale CD is less than 32, even if the number of /27-scale CDs is increased, the reliability of the analysis results will not be improved much, but the processing time will be very long if all 64 /27-scale CDs are analyzed. Therefore, only half of them, 32, are randomly selected and analyzed.

4 Method for Evaluation

We assumed that each darknet had been deployed at that point in the past, and extracted the packet data that would be observed in each darknet from the base darknet. By calculating the similarity between the packet data in the base darknet and in the extracted darknets, we evaluated which darknet's observed data is closer to the observed data in the base darknet among the extracted darknets, i.e., which darknet has more visibility.

The visibility of attack trends based on darknet traffic should be discussed from various perspectives. When issuing a public darknet observation report to alert external organizations, it is necessary to evaluate the visibility of the darknet from a bird's-eye view of the Internet, such as the number of packets by country or a sudden increase of scans to a certain port. The visibility addressed in this study belongs to this category. Note that we deal only with visibility from the perspective of understanding changes in the number of packets on each port and in the number of source hosts.

In this study, two major types of analysis were conducted to quantitatively and qualitatively evaluate the visibility of the DBD in Sect. 4.1 and Sect. 4.2.

4.1 Visibility of Trend Changes in the Number of Packets on the Destination Port

We evaluate the visibility using time-series data representing the change in the number of packets to each port. We select the 1000 major ports with the highest number of TCP SYN packets in the base darknet for each observation period. To see the visibility of the trend in the number of packets to each major port for TCP SYN packets, we examined the number of ports that showed a superiority for the DD over the CD in the same address size from /23-scale to /27-scale.

"Superiority" in this study is defined as the statistical likelihood that one of the two darknets is able to observe traffic closer to the base darknet, i.e., has higher visibility. Conversely, the term "inferiority" is used when two darknets are compared and it is statistically determined that one darknet has lower visibility than the other.

4.1.1 Method of Calculating Similarity of Time-Series Data

To evaluate the visibility of each CD or DD (called scale-down darknet hereafter), the similarity between the base darknet and each scale-down darknet is calculated as a numerical value. We count the number of TCP SYN packets per hour for each of the top 1000 major ports, and this time-series data is used for this evaluation.

First, observed packets on the base darknet are counted per hour and this time-series data is normalized. The normalization process is performed by subtracting the mean value of the time-series data for each point and dividing it by the standard deviation.

The normalized data are then converted into time-series data of change point scores. ChangeFinder was used for the conversion. ChangeFinder uses two-stage learning of an autoregressive model and outputs a larger score when the change in the time-series data is larger. The forgetting rate $R = 0.005$, the smoothing interval $S = 3$ (hours), and the dimension of the autoregressive model is set to 1 dimension. These parameters were tuned by the author with [7] to better represent changes as scores.

The same method is used to prepare time-series data of change scores for the scale-down darknets that are compared with the base darknet. The similarity of the time-series data between the base darknet and the scale-down darknet is obtained by calculating the DTW (Dynamic Time Wrapping) distance [11] of the time-series data of each change point score converted from the time-series data of the base darknet and the scale-down darknet.

DTW is a dynamic time-wrapping algorithm that can calculate the similarity of two time-series data as a distance. DTW does not require two time-series data to have the same length so DTW can calculate a high similarity even when comparing time-series data with different periods, as long as the waveforms are similar. It works by finding the optimal alignment between the elements of the two time-series data. DTW calculates a distance matrix, considering all possible alignments, and then finds the path with the lowest cost through the matrix. The path represents the most similar alignment between the two time-series.

In this study, the similarity between the base darknet and each scale-down darknet is the DTW distance calculated by comparing the time-series data of change point scores converted from the normalized time-series data of the number of packets per hour, not the DTW distance calculated from the normalized time-series data representing the number

of packets per hour itself. This is because we want to compare the visibility necessary for detecting changes of trends. If the visibility for change point detection were to be compared, a possible method would be to detect change points using change point scores and calculate similarity by comparing the timing of detection. However, to perform the change point detection, it is necessary to set an appropriate threshold of the scores for detecting changes for each port. Since it is very difficult to set an appropriate threshold value for all 1000 ports, and it may be difficult to understand the analysis results, this study uses the DTW distance between change point scores as the similarity. The method of the change point detection is explained in Sect. 4.2.1.

4.1.2 Method of Evaluating Superiority

Using the DTW distance, which represents the similarity between the base darknet and the scale-down darknets with respect to the time-series data calculated by the method described in Sect. 4.1.1, t-test is used to statistically determine if there is a significant difference in the visibility of the trend in the number of packets between the two darknets.

In the CD, the number of darknets to be analyzed depends on their address size as described in Sect. 3.4. In the DD, 15 darknets are analyzed as described in Sect. 3.2 and Sect. 3.3, respectively.

The following is an example of the process of determining whether there is a significant difference between the /26-scale CD and the /26-scale CDBD. 32 /26-scale CDs are represented as $A_1, A_2, \cdots, A_{31}, A_{32}$, and 15 /26- scale CDBDs are represented as $B_1, B_2, \cdots, B_{14}, B_{15}$. For the time-series data representing the number of TCP SYN packets per hour to each port P_i on 1000 major ports P_i ($0 \leq i \leq 1000$), the method described in Sect. 4.1.1 is applied to the base darknet and $A_1, A_2, \cdots, A_{31}, A_{32}$ respectively, and the DTW distances $D_{a1}, D_{a2}, \cdots, D_{a31}, D_{a32}$ are calculated. Similarly, DTW distances $D_{b1}, D_{b2}, \cdots, D_{b14}, D_{b15}$ are calculated for the similarity between the base darknet and $B_1, B_2, \cdots, B_{14}, B_{15}$ respectively. In order to evaluate whether there is a statistical advantage or not, we test by Welch's t-test if there is a significant difference between $\{D_{a1}, D_{a2}, \cdots, D_{a31}, D_{a32}\}$ and $\{D_{b1}, D_{b2}, \cdots, D_{b14}, D_{b15}\}$ at 5% significance level. When there is a significant difference, we conclude that the set with the smaller average DTW distance has a higher similarity, i.e., superiority to the other. We do this for 1000 ports P_i ($0 \leq i \leq 1000$) to investigate the number of major ports that have a visibility advantage regarding the trend of the number of packets per port.

4.2 Case Study

The evaluation in Sect. 4.1 shows whether it can successfully detect changes in the number of packets per hour when viewed over the entire observation period, but it does not provide a specific evaluation of whether the detection is faster or slower when a particular event occurs. Since the scale of damage is greatly affected by how quickly a cyber-attack is detected and response to the attack is started, it is an important point of view whether the reduction of the darknet causes a delay in the detection of events. Therefore, we conducted a case study to analyze whether there is a difference in the timing of detecting changes in attack trends between the darknet before and after reduction and between DD and CD.

In this study, changes reported in the NICTER Darknet observation reports are used as a case study. The observation reports indicate when the traffic is suddenly increased and characteristics of such traffic. The case study in this section investigates whether and when the change is detected in each scale-down darknet.

4.2.1 Change Point Detection Method

The change points are detected by finding anomalies in the time-series data of the change point score obtained when calculating the similarity of the time-series data in Sect. 4.1.1.

Bollinger bands are used as the time-series data anomaly detection tool [10]. Bollinger bands define bands of standard deviations above and below the moving average of the time-series data and detect anomalies when the actual time-series data do not fall within the bands. Assuming that the data follow a normal distribution and that the band width is twice the standard deviation, there is a 95% probability that the time-series data will fall within the band.

5 Result

We select several observation periods below so that the results does not depend on a specific observation period and those of similar length. The observation period X_1 is from July 1, 2020 to December 31, 2020, the observation period X_2 is from July 1, 2020 to September 30, 2020, the observation period X_3 is from September 1, 2020 to November 30, 2020, the observation period X_4, and the observation period X_5 is from July 1, 2021 to September 30, 2021.

5.1 Result of Visibility Evaluation of Trend Change in the Number of Packets to Each Destination Port

This section shows the results of the evaluation described in Sect. 4.1. Table 1 shows the number of ports that were found to be statistically superior or inferior by comparing the three types of DDs (CDBD, UDBD, and RDD) with the CD of the same address size with respect to "visibility of the trend in the number of packets destined to each of the 1000 frequently accessed major ports" in TCP SYN packets.

As can be seen from Table 1, "number of ports showing superiority" is much larger for the DD compared to the CD in the same address size ranging from /23-scale to /27-scale, compared to the "number of ports showing inferiority". The results also show that there is no significant difference in the results depending on the difference in the observation period.

When comparing the same address size for the CDBD, the UDBD, and the RDD, there is almost no difference in the number of ports showing inferiority for five different address sizes (/23-scale to /27-scale) and five different observation periods ($X_1, X_2, \cdots, X_5$), and the number of ports that showed superiority to the RDD is the largest.

In other words, the darknets consisting of distributed single IP addresses provides the best visibility of the trend in the number of TCP SYN packets, rather than the darknets consisting of distributed address blocks. Therefore, it is desirable to keep the block size as small as possible when configuring the DBD.

Table 1. # of ports showing superiority or inferiority to the DD out of 1000 major ports for TCP SYN packet compared to the CD with the same address size.

type of DD	X_1	X_2	X_3	X_4	X_5
/23-scale CDBD	799, 1	627, 0	670, 6	686, 6	521, 5
/23-scale UDBD	805, 2	653, 2	683, 5	693, 4	538, 12
/23-scale RDD	831, 1	671, 0	702, 6	723, 5	562, 9
/24-scale CDBD	914, 0	797, 1	827, 3	833, 1	700, 4
/24-scale UDBD	924, 0	827, 0	845, 0	848, 1	726, 6
/24-scale RDD	950, 0	852, 0	868, 0	862, 0	742, 0
/25-scale CDBD	960, 2	898, 0	871, 1	887, 2	784, 2
/25-scale UDBD	940, 3	868, 4	875, 0	875, 1	778, 0
/25-scale RDD	972, 0	926, 0	908, 1	909, 1	813, 3
/26-scale CDBD	963, 2	911, 0	894, 1	907, 6	808, 6
/26-scale UDBD	958, 2	894, 2	899, 2	904, 3	815, 1
/26-scale RDD	969, 1	937, 3	905, 3	923, 5	843, 10
/27-scale CDBD	929, 1	846, 2	868, 2	863, 5	646, 6
/27-scale UDBD	937, 2	840, 2	862, 1	865, 5	759, 8
/27-scale RDD	957, 9	929, 5	899, 11	910, 10	811, 9

(left：Number of superior ports, right:Number of inferior ports)

When we focus on the address scale, there is a large difference in the number of ports that show an advantage for the DD, especially between /23-scale and the other scales. For example, in the observation period X_1 of Table 1, while the number of ports that are superior in the distributed /23-scale is around 800, the number of ports that are distributed-superior in the /24-scale to /27-scale is more than 900. Compared to the /24-scale to /27-scale, the /25-scale and /26-scales have the largest number of ports that are superior to the DD, indicating that the number of ports that are superior to the DD does not only depends on the address size when the address size is small. This suggests that only the visibility of the /23-scale CD is higher due to other factors than the number of IP addresses in the darknet. A possible case will be that the attack targets only the specific address space in the CD. In this case, the CD can observe all the traffic of the attack, while the DD can observe only a part of it. In other words, the fact that the number of ports showing higher visibility of the CD than the DD was larger on the /23-scale than on the /24-scale to /27-scale suggests that many hosts targeted only the address space in the /23-scale CD.

On the other hand, in terms of the visibility of the trend in the number of TCP SYN packets per port, the DD, especially the DD with a highly distributed IP address layout, showed higher visibility than the CD, suggesting that if a darknet with a certain number of IP addresses is to be configured, a DD is better than a CD. If the darknet is configured with a certain number of IP addresses, the number of ports with higher visibility is larger with DD than with CD.

In the observation periodX_1, we choose 1433/TCP, which showed a superiority of DD in all address sizes from /24-scale to /27-scale, and visualize where the packets on

1433/TCP comes in the 32 /26-scale CDs in time-series heatmap in Fig. 4. 1433/TCP is used by Microsoft MySQL Server. As we can see in Fig. 4, the values are large only in a very small range in the base darknet. These large values can be caused by a small number of scanners. When DD is configured to include these narrow address spaces, it is expected to observe traffic trends similar the base darknet and have superiority to CD, which has the same number of IP addresses as the DD.

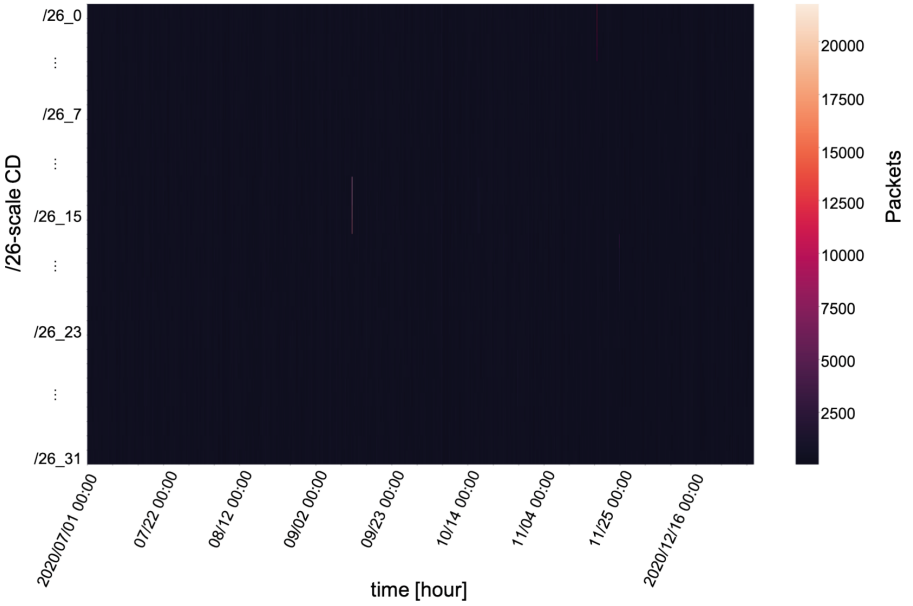

Fig. 4. Heatmap of concentration of packets on 1433/TCP of 32 /26-scale CDs (hourly data)

In the case of 51005/TCP, which showed inferiority of DD in some address sizes from /24-scale to /27-scale. Figure 5 and Fig. 6 show a visualization of where the packets on 51005/TCP comes in the 32 /26-scale CDs in time-series heatmap. Figure 5 shows hourly data and Fig. 6 shows daily data, and these trends are the same for both the hourly and daily aggregated data. Also, in Fig. 5 and Fig. 6, the hourly data does not show significant changes, but the daily data shows an increase in some periods. This might be caused by a low scan rate. When we observe activities that slowly scan contiguous address space with DD, in some periods, these activities cannot be observed with DD. This may be considered the reason for the inferiority of DD. On the other hand, CD can observe the activity with low scan rates without causing changes of visibility.

5.2 Case Study Result

In this section, the scale-down darknets are used to detect change points for specific events. The analysis is conducted to determine if there is any difference in the timing of the events detection between the base darknet and the scale-down darknet. The method

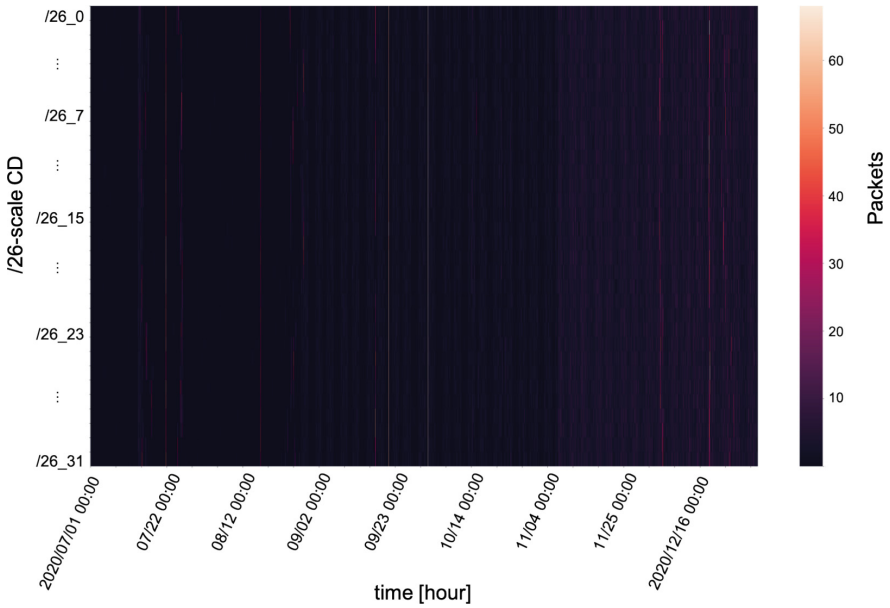

Fig. 5. Heatmap of concentration of packets on 51005/TCP of 32 /26-scale CDs (hourly data)

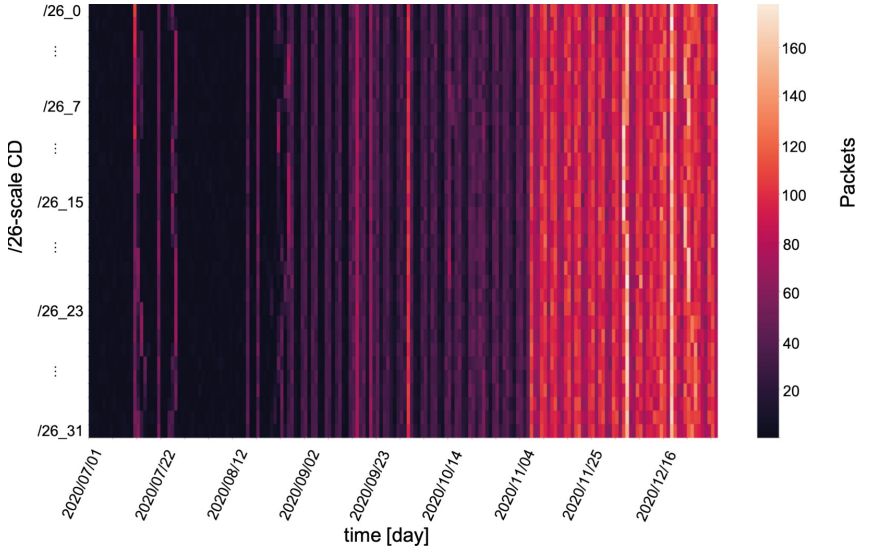

Fig. 6. Heatmap of concentration of packets on 51005/TCP of 32 /26-scale CDs (daily data)

of change point detection is shown in Sect. 4.2.1. The parameters of ChageFinder were tuned for this event with a forgetting rate $R = 0.05$ and a smoothing interval $S = 3$ days.

The events used in the case studies are picked up from the NICTER Darknet Observation Report [4, 8, 9]. These reports include time-series data aggregated on daily basis for visualization. This case study uses time-series data on the number of observed packets and source IP addresses per day to facilitate comparison to the data from NICTER darknet. The event discussed here is the event that the number of packets and source hosts on 7001/TCP and 7002/TCP used by Oracle WebLogic increased rapidly from October to December 2020, as shown in Fig. 7.

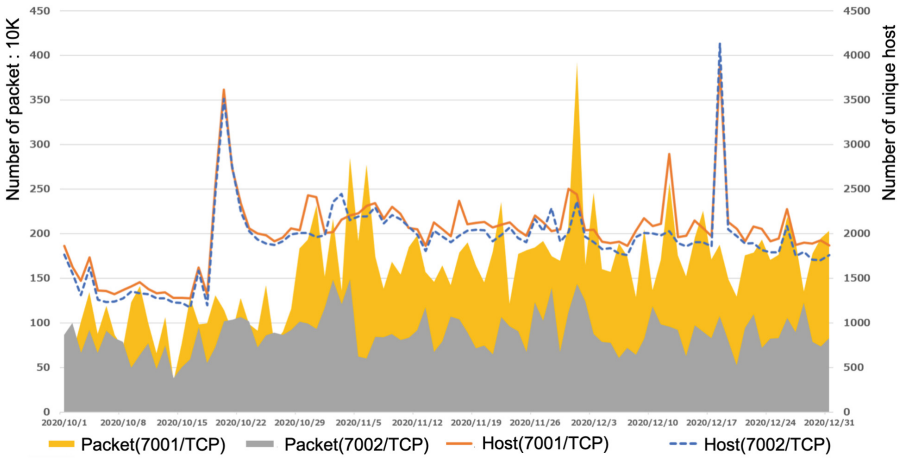

Fig. 7. # of Packets and source hosts on 7001/TCP and 7002/TCP (Quoted from [8] and translated by the authors)

First, we see how data from the base darknet can detect change points in the number of packets and source hosts for this event. Figure 8 shows the number of packets and source IP addresses on 7001/TCP and 7002/TCP observed on the base darknet from October 1, 2020 to December 31, 2020. This period aligns with Fig. 7.

Since the change point score is larger at the beginning of the observation period due to the training period of ChangeFinder, the change point score and detected change points from October 1, 2020 to October 10, 2020 are excluded from the evaluation. The change points detected in the base darknet are summarized in Table 2. Date when very significant increase is observed are shown in red.

As shown in Table 2, the most significant increase in the number of 7001/TCP packets in the base darknet is observed on 11/18. However, the observation by the NICTER darknet in Fig. 7 shows that the most significant increase was observed around 12/01 rather than 11/18 in terms of the number of packets destined to 7001/TCP.

The number of source IPs on 7001/TCP and 7002/TCP in the base darknet is rapidly increased on 10/20, which is the same date as the rapid increase in the number of unique hosts observed in the NICTER darknet. In the NICTER darknet, the most significant spike in the number of source IP addresses for 7001/TCP and 7002/TCP is seen around 12/18. In the base darknet, the change in the number of source IP addresses on 7001/TCP and 7002/TCP is detected at 11/17 and 11/19, but the increase is not as significant as the

trend in the NICTER darknet. These results indicate that there is a certain difference in visibility between the NICTER darknet and the base darknet.

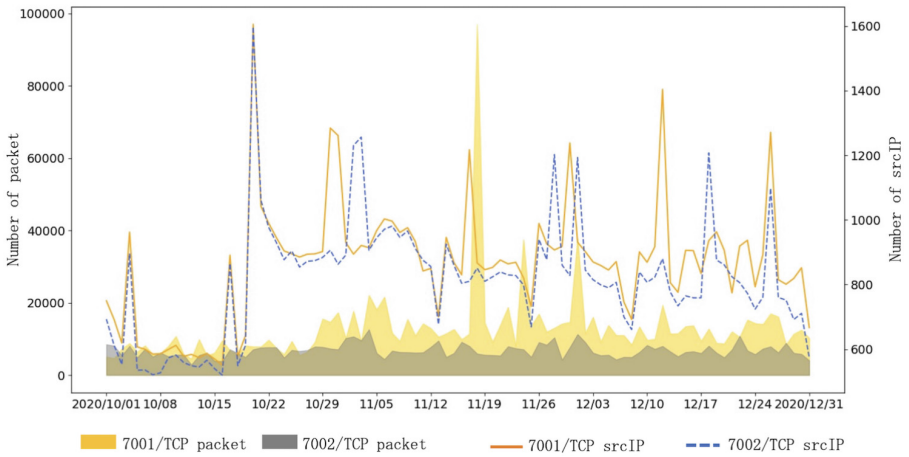

Fig. 8. # of packets on 7001,7002/TCP and their source IPs observed on the base darknet

The results of change point detection using several scale-down darknets other than the base darknet are as follows. We pick up two /23-scale CDs called type-a and type-b, and show the results of these two CDs in Fig. 9 and Fig. 10. There is a large difference in the maximum number of packets between Fig. 9 and Fig. 10, so the scale of the number of packets observed between the two /23-scale CDs is largely different. Table 3 summarizes the detected change points by these two /23-scale CDs. The most significant change in the number of 7001/TCP packets in the base darknet, 11/18, was not detected by the /23-scale CD type-b. The closest change was on 11/20. On the other hand, the most significant change in the number of packets on 7001/TCP in /23-scale CD type-a is 11/18, which is not detected in /23-scale CD type-b, and the closest change is 11/20. Thus, the /23-scale CD type-a is basically able to detect change points with the same timing as the base darknet, but in some cases the most significant change in the base darknet is detected two days later than in the base darknet.

Table 2. Detected change points using the base darknet

	Detected Change-Point
7001/TCP Packet	10/29, 11/04, 11/09, 11/18, 11/29, 12/06
7001/TCP srcIP	10/17, 10/20, 10/30, 11/17, 11/22, 11/30, 12/12, 12/17, 12/26
7002/TCP Packet	10/19, 10/29, 11/05, 11/10, 11/19, 11/24, 11/26, 11/29, 12/04, 12/20, 12/22
7002/TCP srcIP	10/17, 10/20, 11/02, 11/20, 11/28, 12/18, 12/23

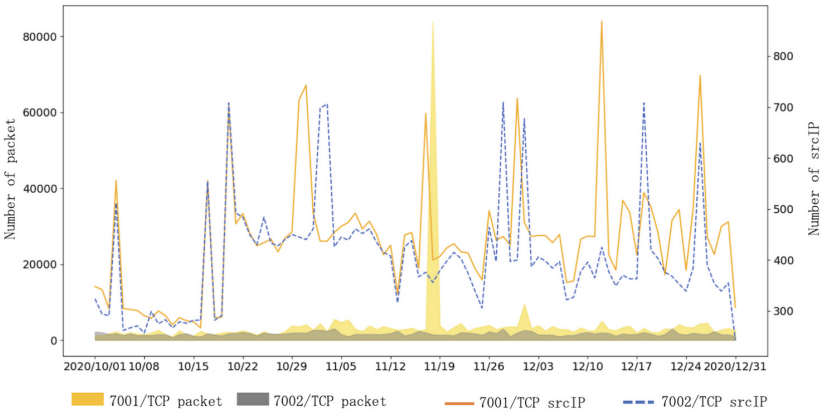

Fig. 9. # of packets on 7001/TCP and 7002/TCP and their source IP observed on /23-scale CD type-a

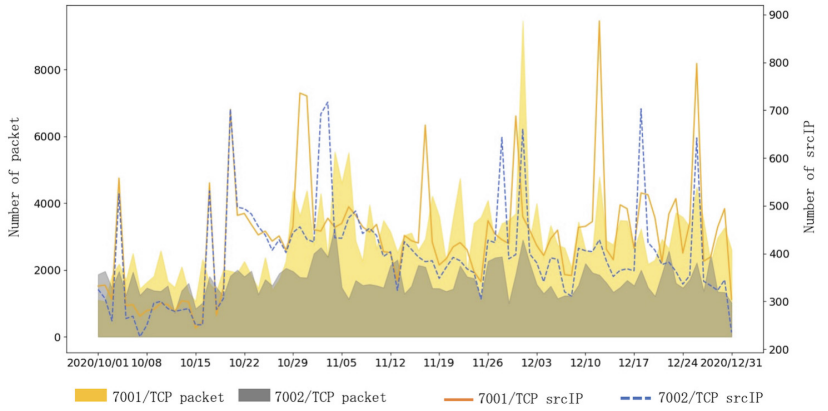

Fig. 10. # of packets on 7001/TCP and 7002/TCP and their source IP observed on /23-scale CD type-b

We also pick up two /27-scale UDBDs called type-a and type-b, and show the results in Fig. 11 and Fig. 12. Table 4 shows the change point detection results using these data. The maximum of the vertical axis of the number of packets in Fig. 11 and Fig. 12 are 2500 and 3000, indicating that the scale of the number of observed packets is not different than that of the /27-scale CD. The peak timing of the number of 7001/TCP packets was 11/18 in /27-scale UDBD type-a and /27-scale UDBD type-b. Therefore, there is no significant difference in the number of packets observed between two /27-scale UDBDs, and the timing of the peak of the 7001/TCP packet is consistent with that of the peak in the base darknet.

The comparison between /23-scale CD and /27-scale UDBD shows that CD tends to cause delays in the detection of change points and scatter in the scale of the number of observed packets. In this case study, the change point detection using the CD is not at

Table 3. Detected change points using /23-scale CDs

	/23-scale CD type-a	/23-scale CD type-b
7001/TCP Packet	11/18	10/29, 11/04, 11/20, 11/23, 11/28, 12/01, 12/30
7001/TCP srcIP	10/17, 10/30, 11/13, 11/17, 11/22, 11/30, 12/05, 12/12, 12/17, 12/26	10/17, 10/30, 11/17, 11/22, 11/30, 12/05, 12/12, 12/17, 12/25, 12/26, 12/31
7002/TCP Packet	11/28, 12/04, 12/11, 12/19, 12/22, 12/27	10/12, 10/29, 11/04, 11/26, 12/22, 12/28
7002/TCP srcIP	10/17, 10/20, 10/25, 11/02, 11/20, 11/28, 12/14, 12/18, 12/23	10/17, 10/20, 10/25, 11/02, 11/18, 11/28, 12/18, 12/23

Table 4. Detected change points using /27-scale UDBDs

	/27-scale UDBD type-a	/27-scale UDBD type-b
7001/TCP Packet	11/06, 11/18	10/29, 11/04, 11/10, 11/18
7001/TCP srcIP	10/17, 10/30, 11/09, 11/30, 12/12, 12/26	10/17, 10/25, 10/30, 11/17, 12/05, 12/12, 12/26
7002/TCP Packet	10/12, 10/18, 10/29, 11/01, 11/24, 12/06, 12/22, 12/31	11/04, 11/14, 12/01, 12/11, 12/22
7002/TCP srcIP	10/14, 10/17, 10/23, 11/02, 11/11, 11/26, 11/28, 12/04, 12/06	10/17, 10/23, 11/02, 11/07, 11/25, 11/28, 12/12, 12/26

a useful level, since there are cases where the delay is several days in the /23-scale CD compared to the results of the change point detection using the base darknet. However, the /27-scale UDBD change point detection results are very close to the results of the change point detection using the base darknet, and the timing of the change point detection tends to show relatively small scatter. For this case study, the /27-scale DD also has visibility of the change point detection close to that of the base darknet and is a useful source of information for the change point detection.

6 Discussion

The visibility of the trend of the number of packets on each of the 1000 main ports was evaluated in terms of the number of ports where the DDs have superiority over CDs in the same address size. Therefore, if the number of IP addresses in the darknet is the same, it is preferable to use distributed IP address spaces as a darknet rather than a contiguous IP address space because the visibility of a large number of ports can be improved by choosing the distributed setting. However, there are some ports that are inferior to the distributed settings, although the number is small. It is necessary to investigate and

determine, depending on the purpose of use of each darknet, whether any significant changes have occurred in the inferior ports, that is, whether there are any cases where the visibility of the inferior ports is extremely important.

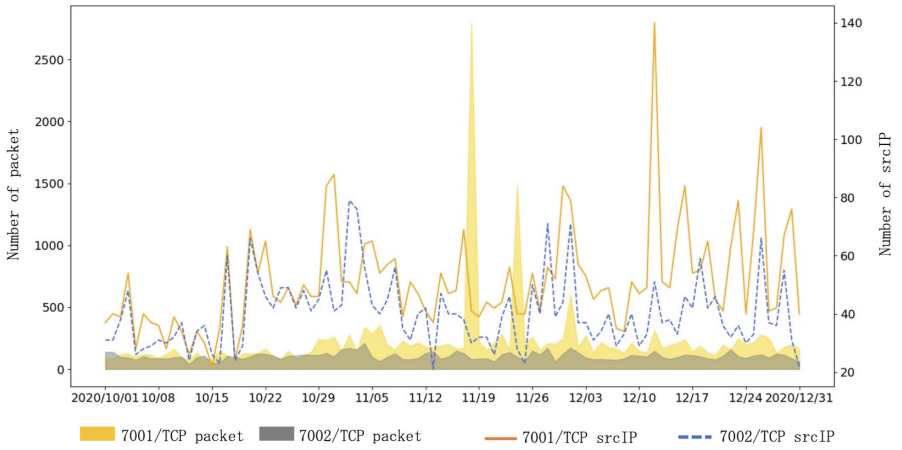

Fig. 11. # of packets on 7001/TCP and 7002/TCP and their source IP observed on /27-scale UDBD type-a

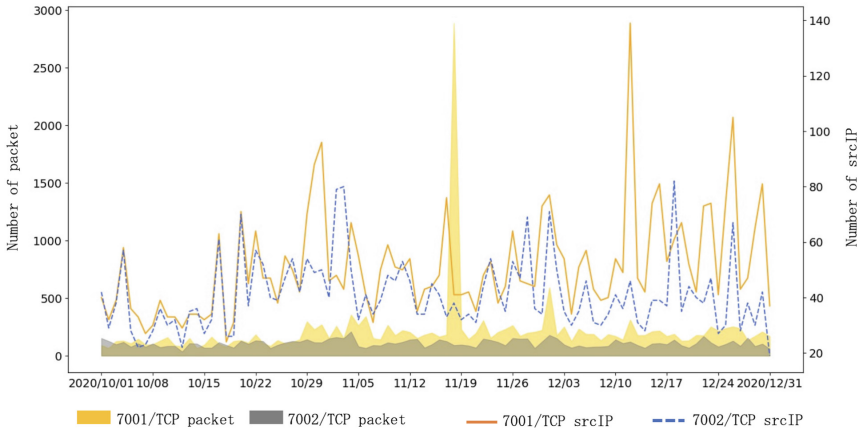

Fig. 12. # of packets on 7001/TCP and 7002/TCP and their source IP observed on /27-scale UDBD type-b

The results of this study suggest that when the same number of IP addresses are used to configure the darknet, visibility is generally higher for making IP addresses distributed than for assigning contiguous IP addresses. There is little difference between the visibility of the CDBD and the UDBD, which are constructed as two different DBDs. Furthermore, the RDD has higher visibility than DBD, suggesting that it is desirable to sparsely allocate IP addresses as much as possible when configuring a DD.

We observed that the change in the traffic volume to the port that showed superiority of CD over DD on a /26-scale was characterized as occurring only in a very narrow address space. Traffic to the port that showed inferiority of CD over DD was characterized by the fact that the change in the traffic volume occurred across the entire base darknet and by the possibility of low-rate scans.

The results show that there is a gap between the timing of events detected using the base darknet and using the CD. The timing of events detection using the DD is less likely to show gaps even when the address size is reduced to /27-scale, indicating that the accuracy of change point detection is still at a useful level. Therefore, if the purpose is to detect change points of events on TCP ports, it is likely that even /27-scale DD will be able to detect change points at a useful level.

7 Conclusion

The visibility of the number of packets on each of the 1000 major ports is improved for scan packets in Distributed address Darknet compared to the Contiguous address Darknet of the same address scale. Furthermore, by comparing the timing of events that can be detected by Distributed address Darknet with the timing of events that can be detected by Contiguous address Darknet for specific events that should be detected through case studies, it is shown that Distributed address Darknet can be expected to be useful even in /27-scale.

Future work includes that DD can be evaluated from a more practical perspective by evaluating the source IP, i.e., the number of scanners although this study focused only on the changes of the number of TCP SYN packets. We also need to conduct more case studies as well as an evaluation using other datasets.

Acknowledgments. The results of this research in part were obtained using mdx, a platform for the creation of a data-utilizing society.

References

1. Dainotti, A., Benson, K., King, A., et al.: Lost in space: improving inference of IPv4 address space utilization. IEEE J. **34**(6), 1862–1876 (2016)
2. Dainotti, A., King, A., Claffy, K.C., et al.: Analysis of a"/0" stealth scan from a botnet. In: Proceedings of the 2012 Internet Measurement Conference, pp. 1–14 (2012)
3. Durand, J., Pepelnjak, I., Doering, G.: BGP Operations and Security, 6.1.3 (2015)
4. Endo, Y.: NICTER Darknet statistical data October to December 2020 (in Japanese)
5. Fachkha, C., Bou-Harb, E., et al.: Inferring distributed reflection denial of service attacks from darknet. Comput. Commun. **62**, 59–71 (2015)
6. Harrop, W., Armitage, G.: Defining and evaluating greynets (sparse darknets). In: The IEEE Conference on LCN 30th Anniversary (LCN 2005) l, pp. 344–350. IEEE (2005)
7. Tomoharu, I., Makoto, O., et al.: Detection of new cyber-attack trend change using darknet (2019)
8. National Institute of Information and Communications Technology: NICTER darknet report 2020 (2020). (in Japanese)

9. National Institute of Information and Communications Technology: NICTER darknet report 2021 (2021). (in Japanese)
10. Soro, F., Drago, I., et al.: Are darknets all the same? On darknet visibility for security monitoring. In: 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1–6 (2019)
11. Wu, R., Keogh, E.J.: FastDTW is approximate and generally slower than the algorithm it approximates. IEEE Trans. Knowl. Data Eng. **34**(8), 3779–3785 (2020)