TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. x, No. x, April 2013, pp. 1 ∼ 15
DOI: 10.11591/telkomnika.vXiY.abcd

Countermeasures against Darknet Localisation Attacks with Packet Sampling

[redacted]

Abstract

A darknet monitoring system is developed to grasp malicious activities on the Internet at an early stage and cope with them. The darknet monitoring system consists of network sensors widely deployed on the Internet to capture incoming unsolicited packets. A goal of this system is to analyse captured malicious packets and provide effective information to protect regular non-malicious Internet users from malicious activities. To provide effective and reliable information, the location of sensors must be concealed. However, attackers routinely launch localisation attacks to detect sensors in order to evade them. If the actual location of sensors is revealed, it is almost impossible to identify the latest tactics used by attackers. Thus, in a previous study, we proposed a packet sampling method, which samples incoming packets based on an attribute of the packet sender, to increase tolerance to a localisation attack and maintain the quality of information publicised by the system. We were relatively successful in countering localisation attacks, which generate spikes on the publicised graph to detect a sensor. However, in some cases, with the previously proposed sampling method, spikes were clearly evident on the graph, which works to the attacker's advantage. Therefore, in this study, we propose advanced sampling methods such that incoming packets are sampled based on multiple attributes of the packet sender. In this paper, we present our improved methods and show a promising evaluation result obtained via a simulation.

Keywords: *Darknet Monitoring, Localisation Attack, Packet Sampling, Security*

1. Introduction

The Internet has become an indispensable resource for most people. However, a various malware is deployed to cause cyber attacks that seriously threaten the safe and reliable use of the Internet, for example stealing confidential personal data or launching Denial-of-Service (DoS) attacks on specific corporate enterprises to hinder their ability to provide services. A Symantec [1] shows that 4,818 unique websites were compromised every month in 2018. With data from a single credit card being sold for up to $45 on underground markets, just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month. Cyberattacks primarily exploit software vulnerabilities. Thus, it is essential to find and manage such vulnerabilities at an early stage to prevent various types of damage, e.g., revealing confidential information or financial harm to both corporate enterprises and general users.

Darknet monitoring systems are developed to find software vulnerabilities and identify the latest methods used by attackers. An overview of a darknet monitoring system is shown in Fig. 1.

A darknet monitoring system comprises multiple network devices, i.e., sensors, that are deployed in unused IP address space on the Internet. Note that these sensors are configured to capture only incoming packets; they do not provide any outgoing services. Such sensors may receive unsolicited packets when they are directly connected to the Internet. Sensors distributed in darknet space capture incoming unsolicited packets. Typically, packets do not arrive in unused address space, i.e., darknet. Thus, we can infer that packets arriving in these unused address spaces, which are valid and routable, are likely malicious. Organisations that operate darknet monitoring systems collect and analyse these malicious packets. Usually, the analysis results,

Received May 9, 201x; Revised August 3, 201x; Accepted August 16, 201x

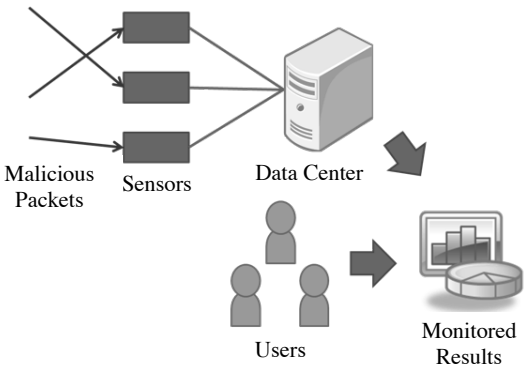

Figure 1. Overview of darknet monitoring system

which can provide effective information to protect regular, non-malicious Internet users from malicious activities, are made publicly available.

To provide effective and reliable information, the location of darknet sensors must be concealed because attackers launch localisation attacks to detect the sensors' IP addresses in order to evade them.

If the IP addresses are revealed to attackers, it is almost impossible to identify and analyse new malicious attack methods. In addition, the sensors themselves may be targeted by DoS attacks.

When attackers initiate a localisation attack, they masquerade as general Internet users. To detect sensors, they misuse information provided by organisations operating a darknet monitoring system. Thus, if organisations release time-series graphical information without taking countermeasures to protect the information, attackers can use the publicised graph to detect a sensor. In a previous study, we proposed a packet sampling method, which samples captured packets based on an attribute of the packet sender, to increase localisation attack tolerance and to ensure the quality of information provided by a darknet monitoring system in our work [2]. We were relatively successful in countering localisation attacks, which generate spikes on the publicised graph to detect a sensor. However, in some cases, unexpected spikes that could indicate the location of a sensor appeared in the graph.

Therefore, here, we propose advanced sampling methods whereby incoming packets are sampled based on multiple attributes of the packet sender. Note that the proposed method exploits knowledge gained from our previous work. A performance evaluation was conducted by simulating attackers' tactics and applying the proposed methods. We used actual captured packets provided by the Nicter[3] darknet project operated by the Japanese National Institute of Information and Communications Technology (NICT). In addition, we also discuss the degradation of publicised information by sampling captured packets compared to a no sampling case. In this paper, we present our improved methods and show a promising evaluation result.

2. Related Work

A wide variety of darknet monitoring systems are operated all over the world to identify and understand the latest attack trends on the Internet. The NICT NICTER project has many user interfaces. For example, *Cube* draws a cubical object in the centre of a window and maps captured packets on the object based on the source and destination of arrived packets. *Atlas* maps captured packets on a world map and indicates in real time the countries that sends malicious packets to Japan. In addition, NICTER counts captured packets by country of origin and classifies packets as TCP or UDP. This is available on the NICTERWeb[4]. As another example, the Japanese National Police Agency operates @police[5], a darknet monitoring system that collects firewall and intrusion detection system log data at the network entry gateway of institutions

affiliated with the police. @police provides security-related information in the form of time-series graphs and tables on their web site.

DShield[6], a community-based firewall log correlation system, recruits volunteers from across the world. The volunteers provide firewall logs that are used to analyse attack trends. DShield is the world's largest darknet community. The Cooperative Association for Internet Data Analysis, CAIDA[7], manages the University of California, San Diego's Network Telescope's Internet traffic monitoring system. This system dominates an entire globally routed /8 network that comprises approximately 1/256 of all IPv4 Internet addresses. The system captures all incoming packets to that address space.

However, attackers launch localisation attacks against darknet monitoring systems to detect and bypass sensors. Shinoda et al.[8] and Bethencourt et al.[9] reported that, to detect sensors, an attacker can send a large number of probing packets to suspicious network that includes a sensor preliminary in the short term to detect sensors. Subsequently, attackers affirm the presence of sensors if sharp spikes appear on the time-series graph publicised by the targeted system. Yu et al.[10, 11] introduced a localisation attack inspired by spread spectrum technology. This method increases attack stealth and can detect sensors with low probing packets by sending probing packets synchronised with the value of a PN code sequence.

If the IP addresses of deployed sensors are revealed by a localisation attack, attackers can bypass the sensors intentionally and launch malicious attacks on the Internet. Consequently, identifying the latest attack trends becomes difficult. In addition, the sensors themselves may be exposed to obstinate DoS attacks.

Basically, attackers infer sensor IP addresses by investigating the publicly available data provided by agencies that operate darknet monitoring systems. In short, attackers put a mark on upcoming publicised data and verify the presence of the mark to detect a sensor. If countermeasures are not implemented, attackers could exploit publicised data and easily detect sensors. Thus, establishing countermeasures against localisation attacks is imperative.

Viecco indicated and emphasised the usefulness of packet sampling techniques for captured packets as a countermeasure to localisation attacks [12] . However, they only consider a theoretical framework. They do not propose a functional sampling method and have not conducted a numerical validation. Thus, we propose a packet sampling method wherein capturing packets are sampled based on an attribute of the packet sender. Sampling is essentially a process that selects a representative subset of individuals from an entire population. We ensure that packet sampling alleviates the influence of probing packets sent by attackers in open publicised data and obtain tolerance to a localisation attack.

3. Localisation Attack by Generating Spikes

In this section, we describe the localisation attack concept, which generates spike on the publicised graph. This is based on the work by Shinoda et al.[8] and Bethencourt et al.[9]. Shinoda et al.[8] referred to a direct and intentional detecting sensor activity as marking. They also defined spikes used for marking as a marker. In this paper, we use these terms in the same manner. An overview of the localisation attack is shown in Fig. 2, and we explain the procedures in the following.

1. Attackers preliminarily narrow down lists of suspicious target networks that include a sensor by analysing materials on the web and obtaining handouts distributed in workshops by an operating organisation of the target darknet monitoring system. The investigated results are preserved by attackers and become lists of suspicious IP addresses acting as sensors on the Internet. Then, the attackers select a range of IP addresses from the lists and initiate a localisation attack by sending markers.

2. Attackers send markers over a short period to suspicious networks that include sensors, i.e., marking. If the sensor receives packets in a short period, a discriminating spike appears in the time-series graph publicised by the target darknet monitoring system.

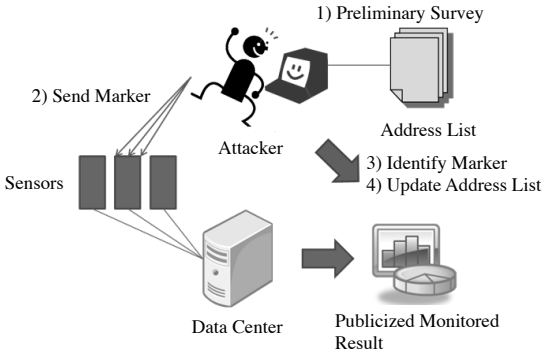

Figure 2. Overview of localisation attack

3. Attackers masquerading as general and good Internet users access a website operated by the organisation running the target darknet monitoring system. They verify the presence of a sensor in a target network by identifying the marker trace in the system's publicised time-series graph.
4. Following the result of procedure 3), the attackers update the lists of suspicious IP addresses. They precisely identify a sensor's IP address by repeating procedures 2) through 4).

The above procedures summarise localisation attacks, which produce spikes on a publicised graph. Since markers are sent as standard packets generated by a port scan, it is difficult to distinguish between markers and other packets. As a result, a darknet monitoring system unintentionally provides instructive feedback to attackers by publicising monitored results based on an all captured packets (including markers).

4. Proposed Packet Sampling Methods

We have previously proposed a packet sampling method that samples incoming packets based on an attribute of the packet sender to increase tolerance to localisation attacks in our worik [2]. Here, we propose two advanced sampling methods that sample incoming packets based on multiple attributes of packets sender based on our previous work.

4.1. Method 1: Sampling Captured Packets by Focusing on Arrival Time and Source IP Address

Initially, we determine the timing of packet capture using random numbers. This is similar to our previous work, which uses packet arrival time. Consequently, using random numbers makes it difficult for attackers to infer when sensors capture packets. In addition, we keep captured packets in chronological order. This contributes to tolerating localisation attacks.

However, successfully preventing a localisation attack is a matter of probability. In the worst case, each sensor may capture all packets sent by attackers based on the time selected by random numbers. Thus, as a second step, we also sample captured packets based on source IP address.

Generally, global IP addresses are administrated by a registration system. Users of a global IP address must register a certain amount of identity information to WHOIS[13]. WHOIS information identifies which IP addresses are assigned to which country; thus, it is easy to access information about where captured packets originated. As shown in Fig. 3 provided by Japanese National Police Agency[14], the ratio of source country of captured packets is greatly biased toward several countries. We assume that attackers manipulate multiple hosts in a botnet to send markers when they attempt a localisation attack. If the botnet comprises exploited hosts whose

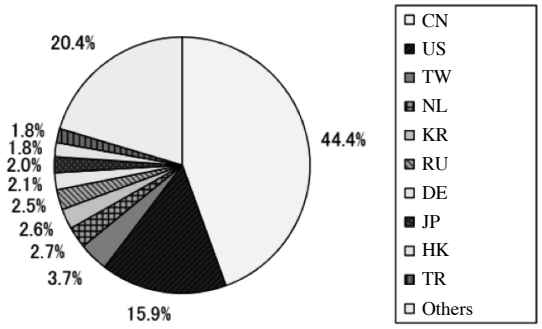

Figure 3. Ratio of source country of captured packets

source IP addresses are biased toward several countries, sampling captured packets uniformly in terms of source countries reduces a spike produced by attackers on a publicised graph even with the containing markers in the time selected by random numbers.

The procedure for sampling method 1 is described as follows.

We use GeoIP [15] to map the source IP address of captured packets to a country.

Procedure 1: Determine Capture Time:

1. Configure parameters m and n as $0 \leq m < n \leq 60$. Hereafter, (m, n) denotes the range of random numbers.
2. Divide captured packets into separate data per hour. The data are denoted ..., $D_{i-1}, D_i, D_{i+1}, ...$ Generate l random numbers for each D_i. Note that $l \in [m, n]$.
3. Generate distinct l random numbers r_j under following conditions: $1 \leq j \leq l$ and $0 \leq r_j < 60$.
4. Sample packets arrived at k minutes at each D_i, $k \in \{r_1, r_2, ..., r_l\}$.

Procedure 2: Sample Packets whose Countries are Distributed Equally:

1. Identify originating country by referencing the source IP address of a captured packet.
2. Sample or discard packets based on the result of 1).
   a. Sample a packet if it has not been captured from the identified country.
   b. If a packet has been captured from the identified country, sample it as long as packets sent from the country are below predefined threshold θ_1; otherwise, discard the packet.
3. Reset the list of the sampled country per hour.

4.2. Method 2: Sampling Captured Packets According to Arrival Time and Time-to-Live

In method 2, we initially determine packet capture timing using random numbers (similar to method 1). We then sample captured packets based on Time-to-Live (TTL).

TTL is a configured value in an IP header to prevent an endless loop of packets caused by misconfiguration in the network. The TTL value is reduced sequentially when a packet moves through a router. The corresponding packet is discarded when the TTL value is reduced to zero. Generally, the initial TTL value is defined by an operating system (Table 1).

Thus, TTL can be used to infer the number of routers passing packets along a communication path, and we can use it as an index of distance in a network. Similar to method 1, if the source distance of captured packets is greatly biased, we believe sampling captured packets

Table 1. Initial TTL value of major operating systems

Operating System	Initial TTL Value
UNIX	255
Windows	128
Linux	64

uniformly in terms of the number of network hops reduces a spike produced by attackers on a publicised graph. The procedure of sampling method 2 is described as follows.

Procedure 1: Determine Capture Time:

1. Configure parameters m and n as $0 \leq m < n \leq 60$ ((m, n) denotes the range of random numbers).
2. Divide captured packets into separate data per hour. The data is denoted ..., D_{i-1}, D_i, D_{i+1}, ... Generate l random numbers at each D_i. Note that $l \in [m, n]$.
3. Generate unique l random numbers r_j under following conditions, $1 \leq j \leq l$ and $0 \leq r_j < 60$.
4. Sample packets arrived at k minutes at each D_i, $k \in \{r_1, r_2, ..., r_l\}$.

Procedure 2: Sample Packets Uniformly in Terms of the Number of Network Hops:

1. Infer the number of network hops according to the TTL value. If the captured TTL value is t_1, we obtain t_2 because t_2 is greater than the value of t_1 and less than the minimum value listed in Table 1. We define the network hops as $t_2 - t_1$.
2. Sample or discard packets based on the result of 1).
   a. If the number of network hops has not been captured, sample it.
   b. If the number of network hops has been captured, sample it as long as the number of network hops is less than predefined threshold θ_2; otherwise, discard it.
3. Reset the list of the number of network hops per hour.

5. Performance Evaluation

5.1. Evaluation of Tolerance to Localisation Attack

1) Assumption: We simulated a localisation attack (Section 3.) and evaluated the effectiveness of the proposed methods to counteract the attack. Simulations were performed using a dataset [16] that includes packets captured in November of 2015. The dataset was provided by NICTER (a darknet monitoring system operated in Japan). Assumptions about the target darknet monitoring system and localisation attack are described in the following.

Assumption about target darknet monitoring system:
In this simulation, the target darknet monitoring system captures packets at each port. Then, the system publicises and updates the monitored results at the same time interval. As shown in Fig. 4, the transition of the number of packets captured by the system is plotted in a time-series graph per hour within the compass of one week. Here, the Y-axis is the number of packets, and the X-axis is elapsed time. Note that any general Internet user can access the publicised result; thus, malicious users can access the same information.

Assumption about localisation attack:
We assume that an attacker sends markers to the tcp port 445 as the destination. In this simulation, the number of packets arriving at tcp port 445 draws a relatively smooth graph compared to

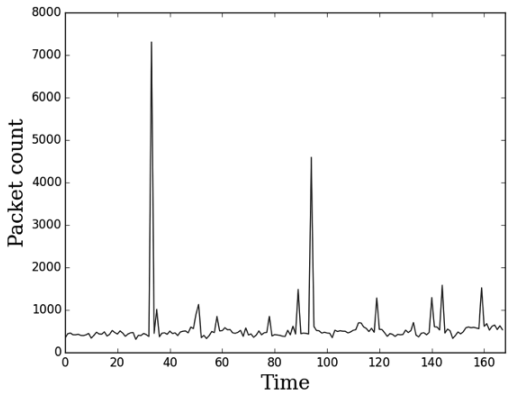

Figure 4. Graph publicised by target darknet monitoring system

Table 2. Breakdown of botnet A in terms of source countries

Country (Code)	The Number of Hosts
CN	2
US	1
RU	1

that of other ports (Fig. 4); thus, we consider that attackers are easy to identify their spikes on the publicised graph. In other words, we believe that this port is suitable for a localisation attack.

We also assume two groups of botnets, i.e., botnets A and B. These botnets are described in Tables 2 to 5. Botnet A comprises exploited hosts whose source IP addresses and network hops are greatly biased, and botnet B is the group that is the same assumption in our previous work for the comparison. The number of sent packets, markers, duration of packet sending and time interval are shown in Table 6.

2) How to Determine Markers by Attackers: After attackers attempt marking, they masquerade as good Internet users and access a darknet monitoring system to identify their markers on a publicised graph to determine the presence of a sensor. Here, the attackers must determine whether identified markers, i.e., spikes, on the graph were generated by themselves. Note that we assume the attackers determine their marker using an outlier detection method. If the spikes are identified as a statistical outlier, the attackers can identify the spikes as their own markers. In our evaluation, we adopted the most general statistical method, i.e., the 2σ outlier test. Figure 5 shows a simulated graph where attackers insert four markers. If organisations operating a darknet monitoring system provide the graph as is without implementing countermeasures, attackers can acquire advantageous feedback, and a sensor's IP address can be discovered easily.

Table 3. Breakdown of botnet A in terms of network hops

The Number of Network Hops	The Number of Hosts
18	2
15	1
12	1

Table 4. Breakdown of botnet B in terms of source countries

Country (Code)	The Number of Hosts
CN	7
US	3
TW	2
NL	2
IN	1
KR	1
TR	1
RU	1
FR	1
MX	1

Table 5. Breakdown of botnet B in terms of network hops

The Number of Network Hops	The Number of Hosts
18	4
19	4
15	2
17	2
20	1
21	1
16	1
14	1
22	1
12	1
28	1
27	1

Table 6. Marking parameters

Destination Port	445/tcp
The Number of Sending Packets	3,000
The Number of Markers	4
Time Interval among Markings	20 hours
Duration of Marking	within 1 minute

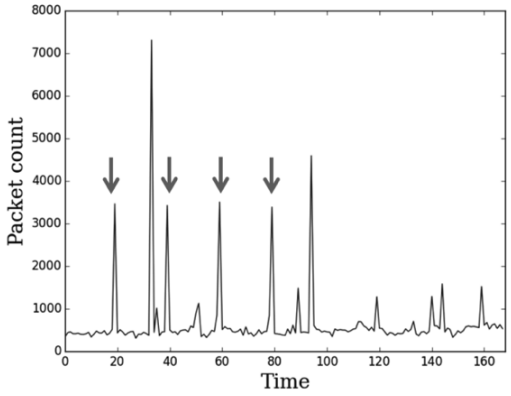

Figure 5. Markers generated by attackers

Table 7. Sampling results of previous work

(m, n)	Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	1.02	0.0694	0.833
$(25, 35)$	2.08	0.0352	0.910
$(40, 50)$	3.05	0.0140	0.949

5.2. Information Quality Evaluation

Sampling is essentially a process that decimates a part from entire and complete information. Thus, it is necessary to consider degradation of information quality caused by a darknet monitoring system when using a sampling method. Therefore, we evaluated the proposed methods in terms of information quality in sampling and no sampling cases. We compared quality obtained before and after sampling in well-known publicised formats (time-series graph and table).

1) Rate of Concordance of Most Accessed Port: Darknet monitoring systems generally publicise the most accessed top 10 port numbers on their websites in table form. The most accessed top 10 port numbers are destination ports that attackers intend to exploit. Here, we assumed two sets including the top 10 port numbers: set X represents results obtained without sampling, and set Y represents results with sampling. We then evaluated the rate of concordance of these two sets. To evaluate the concordance rate of the two sets, we computed Simpson's coefficient as follows:

$$Sim = \frac{|X \cap Y|}{min(|X|, |Y|)}.$$

2) Similarity of Time-series Graph: Darknet monitoring systems publicise the amount of arriving packets at each port as a time-series graph on their website. We compared a time-series graphs obtained without sampling $\{X_u\}$ and with sampling $\{Y_u\}$. We adopted the Bhattacharyya coefficient L as an index to compute the similarity of these two graphs.

$$L = \sum_{u=1}^{m} \sqrt{X_u Y_u},$$

$$\sum_{u=1}^{m} X_u = \sum_{u=1}^{m} Y_u = 1,$$

$$(0 \leq L \leq 1).$$

The Bhattacharyya coefficient is essentially an index used to compute the similarity of histograms. We define the value of $1 - L$ as the discrepancy of graphs, where two graphs are increasingly similar as the value approaches zero.

6. Results and Discussion

The evaluation results are shown in Tables 7 to 11. The number of markers in each table represents the number of spikes that attackers successfully identified in the publicised graphs.

Table 7 shows the results obtained by our previous method. The other tables shows the results obtained by the proposed methods. Compared to the previous method, the proposed sampling methods increased the tolerance to localisation attacks if we focus the number of appearing

Table 8. Sampling results of method 1 based on arrival time and source countries against botnet A

(m, n)	θ_1	Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	0.18	0.0621	0.742
$(10, 20)$	15%	0.62	0.0556	0.753
$(25, 35)$	10%	0.10	0.0509	0.744
$(25, 35)$	15%	0.76	0.0417	0.771
$(40, 50)$	10%	0.20	0.0466	0.743
$(40, 50)$	15%	1.82	0.0312	0.803

Table 9. Sampling results of method 1 based on arrival time and source countries against botnet B

(m, n)	θ_1	Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	1.00	0.0621	0.743
$(10, 20)$	15%	1.00	0.0617	0.750
$(25, 35)$	10%	1.92	0.0419	0.743
$(25, 35)$	15%	2.24	0.0372	0.773
$(40, 50)$	10%	3.06	0.0320	0.743
$(40, 50)$	15%	3.08	0.0226	0.796

Table 10. Sampling results of method 2 based on arrival time and TTL against botnet A

(m, n)	θ_2	Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	0.34	0.0601	0.786
$(10, 20)$	15%	0.60	0.0556	0.822
$(25, 35)$	10%	0.32	0.0482	0.839
$(25, 35)$	15%	1.18	0.0412	0.874
$(40, 50)$	10%	0.38	0.0434	0.883
$(40, 50)$	15%	1.86	0.0327	0.912

Table 11. Sampling results of method 2 based on arrival time and TTL against botnet B

(m, n)	θ_2	Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	0.76	0.0656	0.789
$(10, 20)$	15%	1.16	0.0637	0.820
$(25, 35)$	10%	2.00	0.0422	0.835
$(25, 35)$	15%	2.08	0.0392	0.873
$(40, 50)$	10%	3.00	0.0302	0.885
$(40, 50)$	15%	3.04	0.0245	0.914

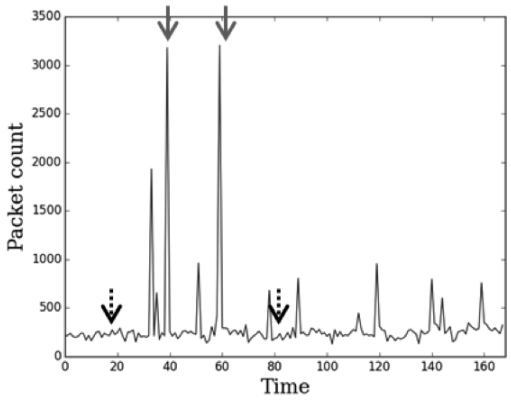

Figure 6. Publicised graph produced by our previous method under the conditions of $(m, n) = (25, 35)$

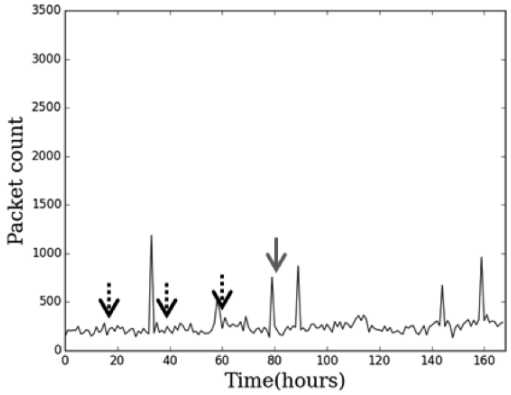

Figure 7. Publicised graph produced by method 1 to counteract botnet A under the conditions of $(m, n) = (25, 35)$, threshold $\theta_1 = 15\%$

markers. However, relative to graph discrepancy and concordance rate of the accessed port, procedure 2, i.e., sampling source countries or network hops uniformly, reduced the information quality.

Relative to the concordance rate of the accessed port, method 2 obtained better results compared to method 1. We conclude that the proposed methods can achieve higher tolerance to localisation attacks by reducing the sampling packets as a range of random number defined in procedure 1 and threshold defined in procedure 2 become small. However, degradation of information quality occurred.

In our previous work, preventing a localisation attack was dependent on the probability. As shown in Fig. 6, spikes are further emphasised if each sensor captures all packets sent by attackers based on the time selected by random numbers. This is a major problem that must be addressed. Methods 1 and 2 alleviated a problem by sampling source countries or network hops uniformly in procedure 2 if sensors capture all packets sent by attackers in procedure 1. As shown in Figs. 7 and 8, the proposed methods curb markers if the number of hosts managed by attackers is small and attributions are greatly biased. Figure 9 shows that our method can prevent markers as the threshold defined in procedure 2 is low. If the number of hosts managed by attackers is large and attributions are unbiased, the proposed methods could alleviate an impact of markers.

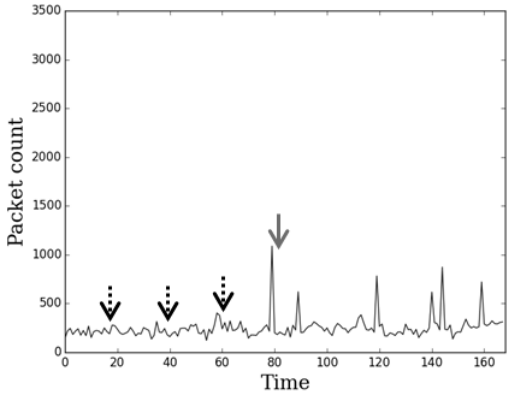

Figure 8. Publicised graph produced by method 2 to counteract botnet A under the conditions of $(m, n) = (25, 35)$, threshold $\theta_2 = 13\%$

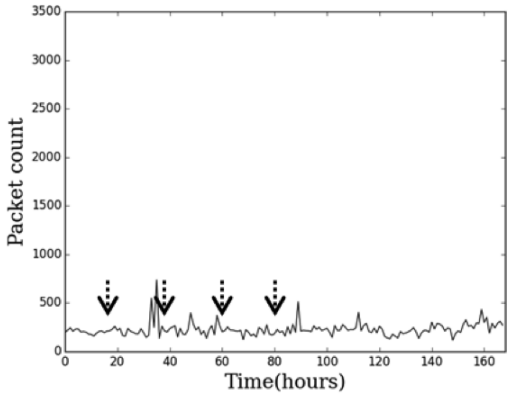

Figure 9. Publicised graph produced by method 1 to counteract botnet A under the conditions of $(m, n) = (25, 35)$, threshold $\theta_1 = 10\%$

Table 12. Proposed method 1: Experimental results (botnet B) with only random number width (m, n) of sampling method focusing on arrival time and source country

(m, n)	θ_1	The Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	1.12	0.0613	0.743
$(20, 30)$		1.66	0.0469	0.743
$(25, 35)$		1.92	0.0419	0.743
$(40, 50)$		2.68	0.0337	0.743
$(50, 60)$		3.66	0.0275	0.743

Table 13. Proposed method 1: Experimental results (botnet B) with only the threshold of sampling method focusing on arrival time and source country

(m, n)	θ_1	The Number of Markers	Discrepancy, $1 - L$	Sim
$(25, 35)$	5%	0.98	0.0584	0.678
	10%	1.92	0.0419	0.743
	15%	1.84	0.0392	0.772
	20%	2.08	0.0358	0.825

7. Considerations on Threshold Fluctuations and Verification of Trade-Off

As demonstrated by the experimental results, as the sampling parameters and the number of packets to be acquired decrease, the resistance to localisation attacks increases; however, the information quality is reduced. Conversely, if the number of packets to be acquired increases, information that is similar to the original information can be obtained. The two are in a trade-off relationship. To verify this trade-off relationship, we performed additional experiments with varying parameters for our proposed methods.

In general, similar results were obtained with methods 1 and 2, i.e., resistance to localisation attacks improved as the threshold value decreased.

By focusing on the destination port match rate, Table 14 (with a common value for threshold θ_2) shows that the match rate of the destination port fluctuates. In contrast, there is no change in the match rate of the destination in Table 12 (with a common value for threshold θ_1).

By comparing the results in Table 13 and Table 15, the destination port match rate also decreases as the threshold θ_1 decreases sharply. From this, it is considered that the influence of the ratio of transmission source country on the matching rate of the destination port is large. Note that if the method 1 is adopted, we need to configure random number width (m, n) as small and control threshold value θ_1 to realise resistance to localisation attacks and maintain high information quality.

8. Conclusion and Future Works

In this paper, we have proposed advanced packet sampling methods based on multiple attributes of packets sender to increase tolerance to localisation attacks. The proposed methods can overcome the weakness of our previous method. In other words, we conclude that the method can prevent a localisation attack without depending on sampling time determined by random numbers along of sampling packets uniformly in terms of source countries or number of network hops if the publicised graph contains markers.

In future, we plan to investigate a further optimal trade-off between tolerance to localisation attacks and quality of publicised results by a darknet monitoring system. In addition, we plan to improve the packet sampling algorithm because attackers are expected to devise increasingly complex localisation attacks.

Table 14. Proposed method 2: Experimental results (botnet B) with only random number width (m, n) of sampling method focusing on arrival time and TTL

(m, n)	θ_2	The Number of Markers	Discrepancy, $1 - L$	Sim
$(10, 20)$	10%	0.94	0.0617	0.791
$(20, 30)$		1.64	0.0467	0.821
$(25, 35)$		1.86	0.0411	0.840
$(40, 50)$		2.84	0.0309	0.883
$(50, 60)$		3.64	0.0245	0.905

Table 15. Proposed method 2: Experimental results (botnet B) with only the threshold of sampling method focusing on arrival time and TTL

(m, n)	θ_2	The Number of Markers	Discrepancy, $1 - L$	Sim
$(25, 35)$	5%	0.84	0.0638	0.747
	10%	1.86	0.0411	0.840
	15%	2.06	0.0390	0.872
	20%	2.08	0.0385	0.887

Acknowledgement

[redacted]

References

[1] Symantec, 2019 Internet Security Threat Report, Vol. 24, 2019.
[2] [redacted]
[3] M. Eto, D. Inoue, J. Song, J. Nakazato, K. Ohtaka, and K. Nakao, "nicter: A Large-Scale Network Incident Analysis System: Case Studies for Understanding Threat Landscape," *Proc. 1st Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, pp.37–45, April 2011.
[4] nicterWeb. https://www.nicter.jp/
[5] @police. http://www.npa.go.jp/cyberpolice/english/
[6] DShield. http://www.dshield.org/
[7] CAIDA. http://www.caida.org/home/
[8] Y. Shinoda, K. Ikai, and M. Itoh, "Vulnerabilities of Passive Internet Threat Monitors," *Proc. 14th USENIX Security Symposium*, pp.209–224, July 2005.
[9] J. Bethencourt, J. Franklin, and M. Vernon, "Mapping Internet Sensors with Probe Response Attacks," *Proc. 14th USENIX Security Symposium*, pp.193–208, July 2005.
[10] W. Yu, X. Wang, X. Fu, D. Xuan, and W. Zhao, "An Invisible Localization Attack to Internet Threat Monitors," *IEEE Trans. Parallel and Distributed Systems*, vol.20, no.11, pp.1611–1625, November 2009.
[11] W. Yu, N. Zhang, X. Fu, R. Bettati, and W. Zhao, "Localization Attacks to Internet Threat Monitors: Modeling and Countermeasures," *IEEE Trans. Computers*, vol.59, no.12, pp.1655–1668, December 2010.
[12] C. H. Viecco and L. J. Camp, "A Risk Based Approach to Limit the Effects of Covert Channels for Internet Sensor Data Aggregators for Sensor Privacy," *Proc. 3rd IFIP International Conf. on Trust Management*, pp.234–251, June 2009.
[13] Spammers & Hackers: Using the APNIC Whois Database to Find Their Network. http://www.

apnic.net/apnic-info/whois_search/using-whois/abuse-and-spamming
[14] Japanese National Police Agency, Internet Threat Report (The First Half of the Year in 2015). http://www.npa.go.jp/cyberpolice/detect/pdf/20150917.pdf (in Japanese)
[15] MaxMind GeoIP. http://dev.maxmind.com/geoip/
[16] Anti Malware Engineering WorkShop (MWS) 2015 Dataset. http://www.iwsec.org/mws/2015/en.html