PAPER *Special Section on Information and Communication System Security—Against Cyberattacks—*

GHOST Sensor: A Proactive Cyber Attack Monitoring Platform

Masashi ETO[†a)], ***Member***, **Tomohide TANAKA**[††], **Koei SUZUKI**[†], ***Nonmembers***,
Mio SUZUKI[†], **Daisuke INOUE**[†], ***and*** **Koji NAKAO**[†], ***Members***

SUMMARY A number of network monitoring sensors such as honeypot and web crawler have been launched to observe increasingly-sophisticated cyber attacks. Based on these technologies, there have been several large scale network monitoring projects launched to fight against cyber threats on the Internet. Meanwhile, these projects are facing some problems such as Difficulty of collecting wide range darknet, Burden of honeypot operation and Blacklisting problem of honeypot address. In order to address these problems, this paper proposes a novel proactive cyber attack monitoring platform called GHOST sensor, which enables effective utilization of physical and logical resources such as hardware of sensors and monitoring IP addresses as well as improves the efficiency of attack information collection. The GHOST sensor dynamically allocates targeted IP addresses to appropriate sensors so that the sensors can flexibly monitor attacks according to profiles of each attacker. Through an evaluation in a experiment environment, this paper presents the efficiency of attack observation and resource utilization.

key words: *network monitoring, cyber attack, darknet, honeypot, attack detection*

1. Introduction

As cyber-attacks becomes increasingly-sophisticated, not only remote exploit attack against OSs and server applications, but also emerging attacks against client applications such as drive-by download attack are increasing. In order to address to ever-changing cyber-attacks, various attack monitoring systems have been proposed. High-interaction, low-interaction honeypot [1] and blackhole monitoring [2] system have been proposed for observations of remote exploit attack. As one of the client honeypots, web crawler is in practical use, which explores malicious web servers that launch drive-by download attack to client web browsers. Meanwhile, there have been some research projects that focus on to deploy those various monitoring systems (sensors) over a wide range of the Internet [3]–[6].

However there are some difficulties involved in sensor operations; (1) difficulty of obtaining wide range unused IP addresses (i.e., darknet) for observations, (2) high management cost of high interaction honeypot for secure operations, and (3) obsolescence of IP addresses due to continuous operation in a long duration. In order to address these problem, this research proposes GHOST (Global, Heterogeneous, and Optimized Sensing Technology) sensor, a novel network monitoring platform [7], [8] which solves previously mentioned problems as well as establishes an integrated sensor management method. GHOST sensor applies a virtual sensing technology and a dynamic address allocation mechanism which enables efficient use of physical and logical network resources. This paper presents the architecture of GHOST sensor platform and the effectiveness of attack attraction through an implementation and evaluations of the system.

The rest of this paper is organized as follows. Section 2 describes the background and related works of this research. Section 3 presents the architecture and implementation of the proposed system. An experiment and discussions are given in Sect. 4. Finally Sect. 5 concludes this contribution and indicates future works of this research.

2. Background

2.1 Network Monitoring Projects and Their Problems

Various kinds of cyber attack monitoring technologies have been proposed to follow ever-changing cyber attacks which accompany the growth of Internet. As a remote exploit monitoring method, high-interaction and low-interaction honeypot [1], [9] are generally employed, which pretend vulnerable hosts and collect deep attack information and malware samples. Blackhole monitoring [2] is one of the cyber attack monitoring methods which observes darknet in an entirely passive manner by non-existent hosts, namely black hole sensor. In comparison with honeypots, blackhole monitoring is easier and suitable for wide range network monitoring, therefore is employed in many research projects. As for drive-by download attack, a number of client honeypot systems (e.g., web crawlers) are proposed in many research groups, which automatically explores malicious web sites. Based on these technologies, various cybersecurity research projects have been launched in order to address the increasingly-sophisticated cyber attacks. Some projects have been deploying and operating network monitoring systems [3]–[6], [10] with sensors widely distributed in the Internet so as to grasp the global trend of cyber attacks in the world. However, there are some difficulties of the operation of those wide range network monitoring systems as follows.

Manuscript received May 23, 2014.
Manuscript revised October 3, 2014.
Manuscript publicized December 4, 2014.

[†]The authors are with National Institute of Information and Communications Technology, Koganei-shi, 184–8795 Japan.
[††]The author is with clwit, Inc., Nonoichi-shi, 921–8844 Japan.
a) E-mail: eto@nict.go.jp

DOI: 10.1587/transinf.2014ICP0014

Difficulty of collecting wide range darknet
As mentioned before, the blackhole monitoring is suitable for wide range network monitoring because it is easier to deploy and operate blackhole monitoring sensors than honeypots. In order to acquire precise attack information by the blackhole monitoring, each darknet segment should have a certain size (e.g., /24 or /16 subnet), that is enough for further analysis. However in many organizations, it is difficult to allocate such a large number of unused IP addresses for blackhole monitoring from their insufficient network resources. Therefore, although they have only 2 or 3 IP addresses to be used for network monitoring, we should efficiently use those small IP addresses.

Burden of honeypot operation
When an organization has only a small number of darknet IP addresses, the IP addresses are often dedicated to high or low interaction honeypots in order to obtain further detail attack information. However, honeypot costs more than blackhole monitoring because it require many machine resources to perform sophisticated attack response. Especially, high-interaction honeypot requires greater burden and high maintenance cost to response to secondary infections and hardware/software troubles of the sophisticated system.

Blacklisting problem of honeypot address
While operating a client honeypot (e.g., web crawler) with a single IP address for a long duration, information collection efficiency become worse. This is because the used IP address are blacklisted so that accesses from the IP address are denied by malicious servers. In response to these problems, this paper proposes a novel network monitoring platform, “GHOST sensor ”, which efficiently collects attack information as well as effectively utilizes limited resources, namely physical machines and IP addresses. The two main functions of the proposed system are “virtual sensor technology ”and “dynamic address allocation mechanism ”for sensors that enable to flexibly operate a large number of sensors.

2.2 Related Works

As researches regarding cyber attack monitoring technology, there are some projects operating large scale blackhole monitoring systems [4], [5], [11] and many other projects involved in the honeynet project [12]. In the honeynet project, there are various kinds of sensors such as a low-interaction honeypot (Dionaea [9]), client honeypots (Capture-HPC [13] and HoneyC [14]) as well as an SSH server honeypot (Kippo [15]). Although they are widely used in many organizations, they are focusing on specific attack methods, and there is no proposal that comprehensively manages various kinds of sensors.

Meanwhile, in terms of sensor management system with effective utilization of physical/logical resources for sensors, some technologies have been proposed [16]–[19]. Collapsar [17] proposed a unique concept which gathered high-interaction honeypots from their proper positions (i.e., monitoring network environments) to an analysis center. The remote monitoring environments and the analysis center are connected via VPN and all attack traffic incoming to the remote environment is forwarded to the analysis center so that the deployed virtual machine based high-interaction honeypots respond to the attacks.

In addition to the Collapsar’s capabilities, Potemkin [18] dynamically instantiates a virtual machine based high-interaction honeypot in response to each incoming attack packet so that the honeypot with the targeted IP address can immediately respond to the attacker. Since Potemkin instantiates honeypots only when needed, it can reduce consumption of machine resource as well as efficiently utilize all of monitoring IP addresses.

SGNET [19] is a similar approach with Collapsar and Potemkin. As an important feature of SGNET, it distributes remote sensors in monitoring environment, which learn common server responses and respond to queries from attackers on behalf of servers in the analysis center so that network traffic between monitoring environment and the analysis center can be reduced. The sensor forwards incoming query to the analysis center only when the query is unrecognized.

These sensor management systems are effective from a perspective of efficient attack information collection and resource utilization. However, although they apply sophisticated virtual technologies for management of honeypots, the number of simultaneously instantiated honeypots is only several hundreds at maximum. As a result, many attack packets must be discarded if the volume of attacks exceed the capability of machine resources. Therefore, a novel sensor management system is required, which utilizes monitoring IP addresses and machine resources as much as possible so that all incoming packets can be somehow analyzed.

3. Proposal: GHOST Sensor

In order to address the problems of the previous works, this paper proposes GHOST sensor, a proactive cyber attack monitoring platform, which manages various kinds of sensors such as blackhole sensor, web crawler as well as high interaction honeypot. GHOST sensor applies a dynamic address allocation mechanism so as to efficiently collect attack information as well as effectively utilize physical and logical resources.

Just the same as Collapsar and Potemkin, in the proposed system as shown in Fig. 1, actual sensors are gathered to the analysis center from conventional monitoring network environments. In contrast, virtual sensors, simple layer 3 proxy agents are deployed at the monitoring environments. The virtual sensor dedicates to forward incoming attack packets to the analysis center so that actual sensors at the center practically respond to the attacks. Since a virtual sensor extends the layer 3 segment of the monitoring environment to the analysis center via VPN connection, attackers misunderstand as if they are directly communicating

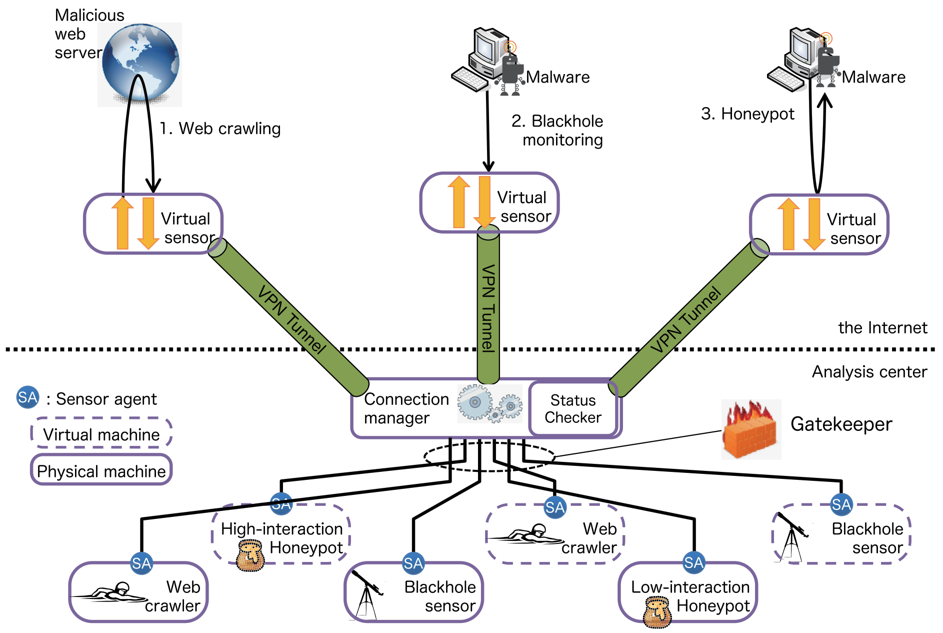


Fig. 1 Overview of GHOST sensor system.

with a host at the monitoring environment, even though the host is located at the analysis center in fact.

One of the distinguished features of the GHOST sensor is the proactive monitoring method which dynamically allocates a targeted IP address of an attack packet to a honeypot, a web crawler or a blackhole sensor according to an address allocation algorithm.

Moreover, in order to prevent second infections by a compromised high interaction honeypot, some security systems such as IPS and firewall have to be deployed just in front of the honeypot. While such solutions had to be applied to honeypots at each monitoring environment so far, all traffic can be comprehensively inspected by gate keeper in the proposed system.

3.1 Components

Virtual sensor

Virtual sensor is an L3 proxy distributed at monitoring environments. It establishes a VPN connection with an analysis center, encapsulates each incoming packet and forward it to the analysis center. Besides, it forwards response packets from an actual sensor at the analysis center to adequate hosts.

Actual sensor and sensor agent

Actual sensor is a machine in which one of the previously introduced sensors such as blackhole sensor, high-interaction and low-interaction honeypots and web crawlers is running. One of the differences from the previous works [18] is that GHOST sensor can manage any kinds of sensors that runs on both physical and virtual machines. That can be enabled because GHOST sensor deploys sensor agents on each actual sensor which flexibly controls the sensor according to the control message from the connection manager. A sensor agent controls an IP address of an actual sensor as well as sends reports periodically to the connection manager which includes information such as number of collected malware sample, number of packets, CPU load average.

Connection manager

Connection manager is deployed on border of analysis center and delivers packets from virtual sensors to appropriate actual sensors as well as send back response packets to the virtual sensors. One of the important functions of a connection manager is to change IP addresses of actual sensors by sending control messages to their sensor agents according to status of actual sensors and profile of attackers in order to respond to the attacker by the most appropriate sensor. In order to perform such controls, a connection manager collects status reports from sensor agents to determine a necessity to change IP address of the sensors.

Gatekeeper

Gatekeeper is an Intrusion Prevention System (IPS) deployed between actual sensors and the connection manager in order to inspect and control especially outgoing packets. Since the GHOST sensor gathers all sensors at one place, such security controls are much easier than the conventional systems where sensors have been distributed to many places. For instance, Gatekeeper permits only important or non-malicious traffic such as C&C communications from a compromised honeypot, and accesses to well-known web sites, whereas other traffic is denied.

3.2 Dynamic IP Address Allocation Mechanism

The dynamic IP address allocation mechanism (Fig. 2) is the

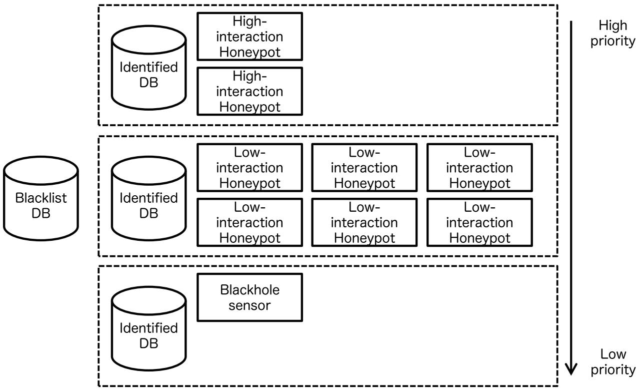


Fig. 2 Dynamic IP address allocation mechanism.

most important function of GHOST sensor platform, which is performed by a connection manager.

The mechanism categorizes sensors into several groups based on types of sensors (e.g., high-interaction honeypot, low-interaction honeypot, blackhole sensor and web crawler), and defines priorities to each group. The priority is determined based on depth of collected attack information. An example is shown in Fig. 2, in which higher priorities are given in order of high-interaction honeypot, low-interaction honeypot and blackhole sensor. The blacklist database stores a list of IP addresses of attackers that should be responded by the most high priority sensor. Entries in the **blacklist database** are stored by other analysis engines or manually so that GHOST sensor can focus on analyzing particular attackers.

Besides, the **identified databases** deployed in each sensor group store IP addresses of attackers that have been responded within last several hours by each sensor group. If an attacker whose IP address is stored in an identified database of a sensor group, the sensor group does not respond to the attacker and forwards the attacker to the next priority sensor group. Because of this mechanism, the high priority sensor can dedicate itself to respond to unidentified attackers while low priority sensors respond to already identified attackers. Based on this environment, the dynamic IP address allocation algorithm is shown in Fig. 3.

When an initial TCP SYN packet is received, the connection manager refers to the blacklist database and identified database of the top priority sensor group with the source IP address of the packet. If the source IP address (src IP in Fig. 3) is not found in the identified database (i.e., the attacker is unidentified), the connection manager allocates the destination IP address of the TCP SYN packet to one of the sensors as long as there is any idling sensor in the sensor group. Then the connection manager forwards the TCP SYN packet to the chosen sensor. Subsequently the sensor continues to respond to the attacker autonomously. On the other hand, if the source IP address is found in the identified database (i.e., the attacker is trivial), or there are no idling sensor in the sensor group, the connection manager proceeds to the next priority sensor group and repeats same steps.

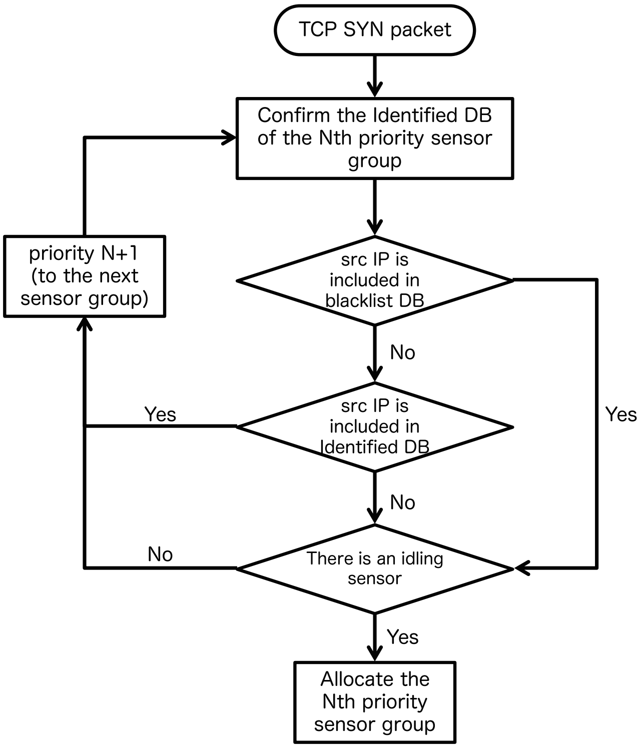

TCP SYN packet
Confirm the Identified DB of the Nth priority sensor group
priority N+1 (to the next sensor group)
src IP is included in blacklist DB
No
Yes
src IP is included in Identified DB
Yes
No
No
There is an idling sensor
Yes
Allocate the Nth priority sensor group

Fig. 3 Flowchart of the IP address allocation algorithm.

Based on this algorithm, the GHOST sensor performs the flexible attack monitoring, namely the connection manager forwards known attackers to low priority sensors while it forwards unknown attackers to high priority sensors. Besides, since all incoming attacks are forwarded to high priority sensors as long as there are idling sensors, even though the attackers are known, the GHOST sensor can efficiently use physical machine resources. Moreover, since any targeted IP address is dynamically allocated to one of the sensors, the GHOST sensor can effectively utilize the logical resources (i.e., darknet IP addresses).

4. Evaluation

We have conducted an experiment at an experiment environment using a prototype of the GHOST sensor, which is connected to the real Internet. Since the prototype of the GHOST sensor is designed to allocate high priority sensors to newer attackers, this experiment focuses on the uniqueness of the observed attacks. Besides, in terms of efficient resource management as one of the important purposes of the GHOST sensor, this experiment presents an evaluation about utilization of sensors and IP addresses.

4.1 Environment

The experiment environment is shown in Fig. 4.

In order to fairly confirm the effectiveness of the GHOST sensor, we have constructed two environments, one is an environment with GHOST sensor (GS env) and the

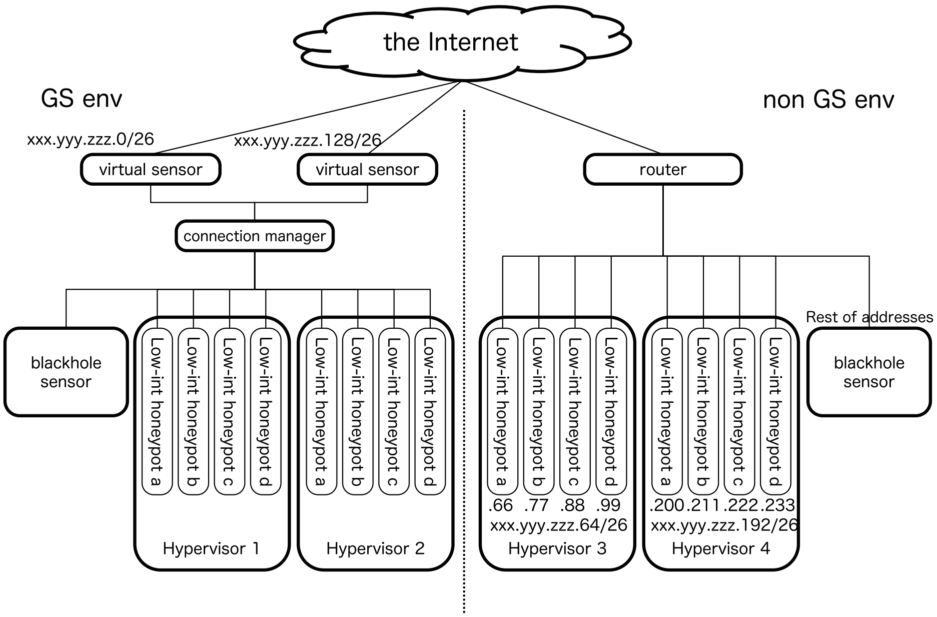


Fig. 4 Experimental environment.

other is without GHOST sensor (non GS env). As for sensor groups, we applied low-interaction honeypot Dionaea (high priority) and our blackhole sensor (low priority). Eight low-interaction honeypots and one blackhole sensor have been deployed in each environment of GS and non GS. Besides, in order to make the two environments similar as much as possible for fair comparison, we divided a class C (/24) darknet into four (A, B, C, D) subnets and allocated A and C to GS environment as well as B and D to non GS environment. In the GS environment, these IP addresses are dynamically allocated to the sensors, while single IP address is statically allocated to each of the eight honeypots in the non GS environment.

Using these environments, we monitored attacks from the Internet in the 24 hours period from 0:00:00 to 23:59:59 of 20 Nov, 2013. Note that the connection manager in GS environment was configured to automatically release IP addresses from each sensor 300 seconds after the allocation. Besides, identified database was configured to remove IP addresses of known attackers five hours after the registration.

4.2 Uniqueness of Captured Malware Samples

In this section we focus on hash values of malware samples captured by Dionaea honeypots in order to confirm that GHOST sensor can preferentially monitor unique (newer) attackers by higher priority sensors. Since the eight high-interaction honeypots in each of GS and non GS environments (i.e., 16 honeypots in total) are working independently, a malware sample from the same attacker might be redundantly captured in multiple honeypots. Therefore, we define malware samples as unique sample, which were captured by only one honeypot Just for reference, Table 1 shows the malware samples and their hash values, which are captured by the low-interaction honeypots (1a ∼ 2d).

Table 1 Captured samples (GS environment).

Honeypot ID	Hash value
1a	3c3011089708c7a49346f648f1e79384 9b175f5f727bcf1153e1aaf99798556a **4f37e1e3ab27feba48038ea03dc55901** **65de48b370a61412435074479c6219fc**
1b	3c3011089708c7a49346f648f1e79384 9b175f5f727bcf1153e1aaf99798556a **9521d5fe45b1211e886da8b7ba813ac3** **cc32d0ee45e3f69e4e9b689c8c01c01c** 4d56562a6019c05c592b9681e9ca2737 **ffb4628a96fa19abab9bbded0324fecd** 64b4345a946bc9388412fedd53fb21cf 7867de13bf22a7f3e3559044053e33e7
1c	3c3011089708c7a49346f648f1e79384 **8535926634662a4e332121a6d2b01032**
1d	3c3011089708c7a49346f648f1e79384 **eb073edcb3340705a0a45f1d14231d47** **a4619b7dc17f18ef00b714db37a0ef19** **cb4c05cae975d30d7cac15df3cdbfe3e** 64b4345a946bc9388412fedd53fb21cf
2a	3c3011089708c7a49346f648f1e79384 **ebfaf4383932b3ef39f1b29e1e574459** **9a1f8268805f01a7c3e0bfce07111cf4**
2b	92675d3f5d76e4170230d1c0294f7be9 4d56562a6019c05c592b9681e9ca2737 **e5db14583694d3ff53d3b0b9c95d82b0** 3c3011089708c7a49346f648f1e79384
2c	3c3011089708c7a49346f648f1e79384 **b202f4b1bdbb2615bb579d64fecd76a6** **7a676b8a1ad9d1efdde6ad9b0a663960** 7867de13bf22a7f3e3559044053e33e7
2d	3c3011089708c7a49346f648f1e79384 **76e669836f48491f118c8e41c678e230** **b7d4ed11a02cd3f4867299640e1e52a8**

In Table 1, the samples with underline are the unique

Table 2 Comparison of captured samples between GS and non GS environment.

	GS environment	non GS environment
Total number	33	37
Unique samples	17	9
Unique sample rate	51.5%	24.3%
Non-unique sample rate	48.5%	76.7%

Table 3 Relations between connections and IP addresses.

	GS environment	non GS environment
Number of connections	1868	1003
Observed IP address	128	8
Connections per IP address	14.6	125.4

samples captured only by corresponding honeypots. Table 2 shows the number of established connections, unique samples and rate of them to the total samples captured at each environment. In this experiment, 1868 and 1003 connections have been established in GS environment and non GS environment respectively.

The numbers of unique samples captured at both GS and non GS environments (17 (51.5%) and 9 (24.3%)) are two times different whereas the total numbers in each environment are close. Contrarily non GS environment have captured 76.7% of non-unique samples, which indicates that it was collecting the same samples from duplicated attackers. In addition, Table 3 shows relations between the number of total established connections of 8 low-interaction honeypots in the both environment and the number of monitoring IP addresses. As mentioned in Sect. 4.1, 128 IP addresses have been allocated to 8 honeypots in GS environment while 8 IP addresses have been allocated to 8 honeypots in non GS environment. As Table 3 shows, the number of connections per IP address in GS environment (14.6) is smaller than the number in non GS environment (125.4) because duplicated attackers were forwarded to the low priority sensor (i.e., blackhole sensor). This fact indicates that GHOST sensor avoided frequent attackers and successfully attracted new attackers.

4.3 Usage Rate of IP Address

As mentioned before, the experiment environment divided a class C (/24) network into four subnets and allocated two subnets for each environment. Therefore each environment has 128 darknet IP addresses. Figure 5 indicates the rate of the time duration that each IP address was allocated to one of the low-interaction honeypots in GS environment.

Figure 5 shows the rate of the allocated time (seconds) to the total time (24 hours: 172,800 seconds) for each IP address (X axis). Although there are small dispersion, most of the IP address have been allocated for 3% to 5% of the total time. This result indicates that the targeted IP addresses were allocated to honeypots almost evenly because most of attackers have swept across the monitoring network.

Consequently we confirmed that any IP address can conduct itself as a honeypot in the GHOST sensor environment whereas only fixed static IP addresses were used in the conventional monitoring environment.

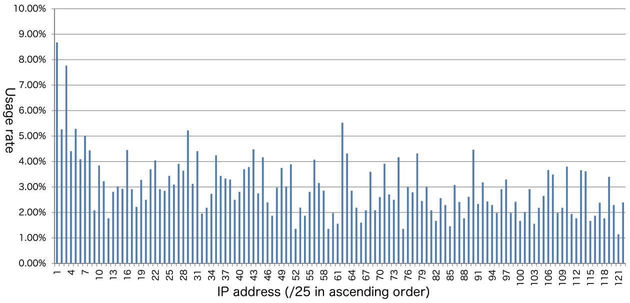


Fig. 5 Usage rate of IP address.

Table 4 Occupancy rate of machine.

Honeypot ID	Total occupancy time (sec)	operating rate (/172800 sec)
1a	64062.673	37%
1b	64062.2	37%
1c	63882.519	37%
1d	63882.67	37%
2a	63882.079	37%
2b	63882.976	37%
2c	64062.588	37%
2d	63882.71	37%

4.4 Occupancy Rate of Machine

As well as usage rate of IP address, this subsection evaluates the occupancy rate of honeypot machine. The occupancy rate of a honeypot machine can be derived by measuring the time duration that any of IP addresses was allocated to the honeypot. In this evaluation, higher occupancy rates are expected, which indicates that honeypot machines are activated for longer durations. Table 4 shows the rate of the time (seconds) to the total time (24 hours: 172,800 seconds) for each honeypot (1a ~ 2d) in the GS environment.

As a result, we found that the occupancy rates of honeypot machines were fairly constant about 37%. Besides, through further investigation of log of the connection manager, we learned that each honeypot became active every five to ten minutes (7 min 45 sec in average). Consequently, we confirmed that GHOST sensor can utilize sensor machines at a constant rate whereas a sensor keeps idling until an attack packet arrives to it in the conventional monitoring environment.

4.5 Performance Evaluation

In this experiment, the system of GHOST sensor was developed using hardware described in Table 5. Since the bottleneck of the GHOST sensor system is assumed to be the virtual sensor and the connection manager, we have evaluated the maximum performance of the both components using traffic generator. In this experiment, we performed an evaluation by sending various packets (i.e., 64Byte, 570Byte and 1500Byte) to the component systems. As a result, the

Table 5 Hardware specification of GS environment.

Host	OS	CPU	Memory	HDD
Virtual sensor	CentOS release 6.3	Intel PentiumD 3.20GHz	DDR2 4GB	SATA/300 500GB
Connection manager	CentOS release 6.3	Intel PentiumD 3.20GHz	DDR2 4GB	SATA/300 2TB
Low-int honeypots	1vCPU (Intel Xeon E3-1270 V2@3.50GHz)	DDR3 2GB	Virtual disk 500GB	

Table 6 Maximum number of processed packets by each component.

Component	Maximum number of packets/sec
Virtual sensor	150,907
Connection manager	190,642

virtual sensor processed 150,907 packets/sec where the connection manager processed 190,642 packets/sec at maximum as shown in Table 6. Meahwhile, the maximum number of attacking packets observed in our darknet monitoring environment with 240,000 IP addresses was 8,000. Therefore, we can assume that the performance of the GHOST sensor system is enough for practical operations in darknet monitoring environment.

4.6 Consideration

Deduplication of attackers At the evaluation regarding the uniqueness of captured samples in Sect. 4.2, the numbers of IP addresses allocated to the honeypots in the non GS environment (8) and the GS environment (128 at maximum because of dynamic allocation) are 16 times different. Consequently the total number of captured samples also must be 16 times, although it was not because the GHOST sensor properly eliminates consecutive attacks from known attackers.

Detail of unique samples Through the detailed investigation of the samples captured in the GS environment, we found that all of them were not executable files. Although they are a kind of garbage, since the same cases were also seen in the non GS environment, they were captured because of the limitation of the low-interaction honeypot, not the GHOST sensor.

Occupancy rate of machines At the evaluation performed in Sect. 4.4, although we found that the occupancy rate of the honeypot machines were successfully constant, the value (37%) was not so high. Namely, this rate indicates that all of the honeypots were active only ten hours in total during the 24 hours experiment. This result denotes that the number of honeypot machines (8) was overmuch compared to the number of IP addresses (128), and consequently honeypots were competing for a limited number of attackers with each other. Based on this result, we learned that three honeypots are enough for monitoring 128 IP addresses. Note that, since the number of observed attacking events depends on not the number of honeypot machines but the number of observed IP addresses, the occupancy rate do not directly affect the number of observed attacking events.

5. Conclusion

In this paper, we proposed, implemented and evaluated the GHOST sensor, a novel proactive cyber attack monitoring platform, which has a dynamic IP address allocation mechanism to flexibly respond to attackers with appropriate sensors. We presented the architecture of the GHOST sensor, which mainly consists of the virtual sensor, the connection manager, the gatekeeper, the actual sensor and the sensor agent. For the implementation of the dynamic IP address allocation mechanism, we applied the blacklist database and identified database in order to avoid frequent attackers and focus on the unidentified attackers. Through the experiment with connecting to the real Internet, we confirmed that the GHOST sensor successfully focused on unidentified attackers. Moreover, we confirmed that physical resource (honeypot machines) and logical resource (IP addresses) were efficiently used by the GHOST sensor.

5.1 Future Work

In the current implementation of the system, although the connection manager determines a corresponding sensor according to whether the attacker is new or not, we are going to apply more sophisticated allocation mechanism in order to allocate sensors based on destination port, source IP address and so on. Besides, although only passive sensors have been applied to the experiment, we are going to apply many kinds of sensors including client honeypots in the next experiment.

References

[1] Nepenthes Development Team. http://nepenthes.carnivore.it/contact

[2] D. Moore, "Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe," 17th Large Installation Systems Administration Conference (LISA'03), 2003.

[3] WOMBAT: Worldwide Observatory of Malicious Behaviors and Attack Threats. http://www.wombat-project.eu/

[4] SANS Internet Storm Center. http://isc.sans.org/

[5] F. Pouget, M. Dacier, and V. Pham, "Leurre.com: On the advantages of deploying a large scale distributed honeypot platform," E-Crime and Computer Conference (ECCE'05), 2005.

[6] K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, "Practical correlation analysis between scan and malware profiles against zero-day attacks based on darknet monitoring," IEICE Trans. Inf. & Syst., vol.E92-D, no.5, pp.787–798, May 2009.

[7] M. Eto, M. Suzuki, D. Inoue, and K. Nakao, "Proposal of multipurpose network monitoring platform," Computer Security Symposium 2013, Oct. 2011.

[8] M. Eto, T. Tanaka, K. Suzuki, D. Inoue, and K. Nakao, "Implementation and evaluation of a proactive cyber attack monitoring platform," IEICE Technical Report, ICSS2013-77, March 2014.

[9] "Dionaea catches bugs." http://dionaea.carnivore.it/

[10] PREDICT: The Protected Repository for the Defense of Infrastructure Against Cyber Threats. http://www.predict.org/

[11] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet motion sensor: A distributed blackhole monitoring system," Proc. 12th ISOC Symposium on Network and Distributed Systems Security (NDSS), pp.167–179, Citeseer, 2005.

[12] L. Spitzner, "The honeynet project: Trapping the hackers," IEEE Security & Privacy, vol.1, no.2, pp.15–23, 2003.

[13] C. Seifert and R. Steenson, "Capture-honeypot client (capture-hpc)." https://projects.honeynet.org/capture-hpc/, 2006.

[14] C. Seifert, I. Welch, P. Komisarczuk, et al., "Honeyc-the low-interaction client honeypot," Proc. 2007 NZCSRCS, Waikato University, Hamilton, New Zealand, 2007.

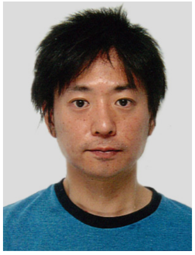
[15] U. Tamminen, "Kippo SSH honeypot," Retrieved, 2013. https://code.google.com/p/kippo/

[16] L. Spitzner, "Know your enemy: Genii honeynets," 2003. http://www.honeynet.org/papers/gen2

[17] X. Jiang and D. Xu, "Collapsar: A vm-based architecture for network attack detention center," Proc. 13th Conference on USENIX Security Symposium-vol.13, p.2, USENIX Association, 2004.

[18] M. Vrable, J. Ma, J. Chen, D. Moore, E. Vandekieft, A. Snoeren, G. Voelker, and S. Savage, "Scalability, fidelity, and containment in the potemkin virtual honeyfarm," ACM SIGOPS Operating Systems Review, vol.39, no.5, pp.148–162, 2005.

[19] C. Leita and M. Dacier, "Sgnet: A worldwide deployable framework to support the analysis of malware threat models," IEEE, Seventh European Dependable Computing Conference, pp.99–109, 2008.



Masashi Eto received LL.B degree from Keio University in 1999, received the M.E. and Ph.D. degrees from Nara Institute of Science and Technology (NIST) in 2003, 2005, respectively. From 1999 to 2003, he was a system engineer at Nihon Unisys, Ltd., Japan. He is currently a researcher at National Institute of Information and Communications Technology (NICT), Japan. His research interests include network monitoring, intrusion detection, malware analysis, and auto-configuration of the Internetworking. He received the Best Paper Award at the 2007 Symposium on Cryptography and Information Security (SCIS 2007), the commendation for science and technology by the minister of MEXT, Japan, in 2009.

Tomohide Tanaka received his M.S. degree in 1997 from JAIST (Japan Advanced Institute of Science and Technology). He founded clwit, Inc., a system development company in 2000. Currently, he is a CTO of clwit, Inc. and responsible to development of network systems.

Koei Suzuki joined a system development company in 2001 and engaged in a large-scale C language based system development. He has been involved in network security system development project from 2005 and developed a network traffic visualization system. He entered National Institute of Information and Communications Technology (NICT) in 2009, where he is in charge to the development of visualization engines such as nicter, nirvana and DAEDALUS.

Mio Suzuki received his Ph.D. degree from Nara Institute of Science and Technology (NAIST), Japan, in 2010. He is currently a researcher in National Institute of Information and Communications Technology (NICT), Japan. His research interests include network security, visualization, network operation, and Internet emulation.

Daisuke Inoue received his B.E. and M.E. degrees in electrical and computer engineering and Ph.D. degree in engineering from Yokohama National University in 1998, 2000 and 2003, respectively. He joined the Communications Research Laboratory (CRL), Japan, in 2003. The CRL was relaunched as the National Institute of Information and Communications Technology (NICT) in 2004, where he is the director of Cybersecurity Laboratory in Network Security Research Institute. His research interests include security and privacy technologies in wired and wireless networks, incident analysis and response technologies based on network monitoring and malware analysis. He received the best paper award at the 2002 Symposium on Cryptography and Information Security (SCIS 2002), the best paper award at the 2nd and 3rd Joint Workshop on Information Security (JWIS 2007 and 2008), and the commendation for science and technology by the minister of MEXT, Japan, in 2009.

Koji Nakao received the B.E. degree of Mathematics from Waseda University, in Japan, in 1979. Since joining KDDI in 1979, Koji has been engaged in the research on communication protocol, and information security technology for telecommunications in KDDI laboratory. After 2003, Koji has moved to KDDI head office to construct and manage its security systems. In 2004, he has started to additionally work for NICT (National Information Communication Technologies). His present positions are "Information Security Fellow" to manage all the security issues required in KDDI and "Distinguished Researcher" to manage research activities for network security technologies in NICT. Koji received the IPSJ Research Award in 1992, METI Ministry Award and KPMG Security Award in 2006, and Contribution Award (Japan ITU), NICT Research Award, Best Paper Award (JWIS) and MIC Bureau Award in 2007 and The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology (Prizes for Science and Technology: Research Category) in 2009. He is a member of IPJS and IEICE. Koji has also been a part-time instructor in Waseda University and Nagoya University.