

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
8 January 2009 (08.01.2009)

PCT

(10) International Publication Number
WO 2009/005187 A1

(51) International Patent Classification:

G06F 15/00 (2006.01)

(21) International Application Number:

PCT/KR2007/005797

(22) International Filing Date:

19 November 2007 (19.11.2007)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

10-2007-0067268 4 July 2007 (04.07.2007) KR

(71) Applicant (for all designated States except US): ELEC-
TRONICS AND TELECOMMUNICATIONS RE-
SEARCH INSTITUTE [KR/KR]; 161 Gajeong-dong,
Yuseong-gu, Daejeon 305-350 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): JEONG, Chi Yoon
[KR/KR]; #302, 140-8 Sinseong-dong, Yuseong-gu, Dae-
jeon 305-345 (KR). CHANG, Beom Hwan [KR/KR];
405-1205 Expo Apt., Jeonmin-dong, Yuseong-gu, Dae-
jeon 305-762 (KR). SOHN, Seon Gyoung [KR/KR];
103-1105 Daelim-Dure Apt. Sinseong-dong Yuseong-gu,
Daejeon 305-720 (KR). KIM, Geon Lyang [KR/KR];
#327 ETRI Dormitory, 236-1 Gajeong-dong Yuseong-gu,

Daejeon 305-350 (KR). KIM, Jong Hyun [KR/KR];
2-104 KAIST Gyosoo Apt. 383-1, Doryong-dong,
Yuseong-gu, Daejeon 305-340 (KR). RYU, Jong Ho
[KR/KR]; A-203 Shinhanhomepistel Bongmyeong-dong,
Cheonan, Choongcheongnam-do 330-100 (KR). NA,
Jung Chan [KR/KR]; 119-1304 Hanvit Apt. Eoeun-dong,
Yuseong-gu, Daejeon 305-755 (KR). JANG, Jong Soo
[KR/KR]; 303-903 Expo Apt., Jeonmin-dong, Yuseong-gu,
Daejeon 305-761 (KR). SOHN, Sung Won [KR/KR]; 161
Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR).

(74) Agent: C & S LOGOS PATENT AND LAW OFFICE;
13th Floor, Seocho-Pyunghwa Building, 1451-34 Seocho-
dong, Seocho-gu, Seoul 137-070 (KR).

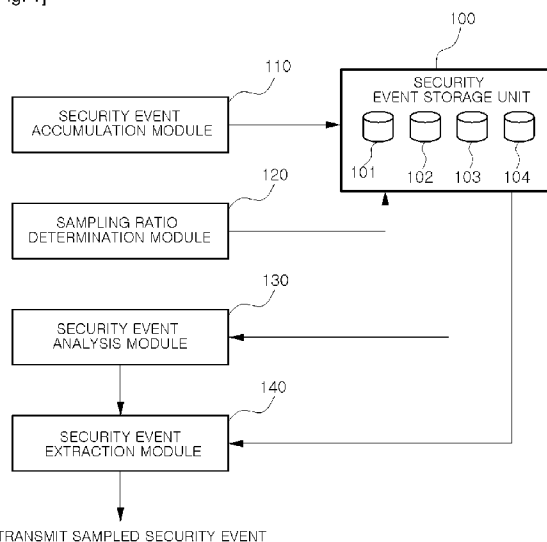
(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG,
ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR,
LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,
RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR SAMPLING SECURITY EVENT BASED ON CONTENTS OF THE SECURITY
EVENT

[Fig. 1]



(57) Abstract: There are provided an apparatus and method for sampling a security event based on contents of the security event, the apparatus including: a security event accumulation module collecting security events occurring in a network system and storing the security events for each type according to contents of the security event; a security event analysis module calculating distribution of the security events for each type by analyzing the stored security events; and a security event extraction module sampling the stored security events according to the calculated distribution of the security events for each type. The apparatus and method may improve speed of visualization of a security event and a security event analysis apparatus and may increase accuracy thereof.

WO 2009/005187 A1



GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

Description

APPARATUS AND METHOD FOR SAMPLING SECURITY EVENT BASED ON CONTENTS OF THE SECURITY EVENT

Technical Field

- [1] The present invention relates to a security event sampling apparatus and method to protect characteristic information of security events, and more particularly, to an apparatus and method for sampling a security event received from a network system by using contents of the security event to protect characteristic information of the security event.
- [2] The work related to the present invention was partly supported by the IT R&D program of MIC/IITA [2005-S-022-01, Title: The Development of Smart Monitoring and Tracing System against Cyber-attack in All-IP Network].
- [3]

Background Art

- [4] Recently, as sampling methods used in collecting and analyzing security events on a network, there are a systematic sampling method extracting security events at regular intervals, a random sampling method randomly extracting a security event from security events, and a stratified random sampling method dividing security events into homogeneous layers and randomly extracting from the homogeneous layers.
- [5] In association with this, there is Korean Patent Application No. 10-2005-032363 entitled An apparatus for capturing Internet Protocol (IP) packet with sampling and signature searching function, and a method thereof, which embodies sampling function and signature searching function in hardware and supports periodical sampling, random sampling, and Hash-based sampling to improve performance of sampling. However, there is still a problem of distortions of content characteristics of security events before and after sampling.
- [6] Generally, contents of security events include a source Internet protocol (IP) address, a destination IP address, a source port, a destination port, and a protocol. Distribution of information included in the contents of the security events becomes important characteristics to determine a security state of a network.
- [7] Also, cyber attacks presently performed on a network use a method of fixing both of a source port and a destination port, a method of fixing a source port and randomly varying a destination port, and a method of randomly varying both of a source port and a destination port. Accordingly, distribution of a relation between a source port and a destination port plays an important role in analyzing and visualizing a cyber attack state.

- [8] Since security events are sampled without using content characteristic information of the security events in conventional sampling methods, content characteristics of security events after sampling become different from content characteristics of security events prior to sampling. That is, when sampling without using contents of security events, information on distribution of a relation between a source port and destination port is damaged, thereby deteriorating performance of a network visualization and analysis apparatus.

[9]

Disclosure of Invention

Technical Problem

- [10] An aspect of the present invention provides a security event sampling apparatus and method capable of maintaining content characteristic information of security events prior to sampling and content characteristic information after the sampling to be identical without change when sampling security events received from network systems existing on a network.

[11]

Technical Solution

- [12] According to an aspect of the present invention, there is provided an apparatus for sampling a security event based on contents of the security event, the apparatus including: a security event accumulation module collecting security events occurring in a network system and storing the security events for each type according to contents of the security event; a security event analysis module calculating distribution of the security events for each type by analyzing the stored security events; and a security event extraction module sampling the stored security events according to the calculated distribution of the security events for each type.
- [13] The apparatus may further include a security event storage unit having a plurality of storage areas storing the security events for each type.
- [14] The apparatus may further include a sampling ratio determination module determining a sampling ratio in proportion to processing performance of a system and an average number of received security events per second for a set T amount of time.
- [15] According to another aspect of the present invention, there is provided a method of sampling a security event based on contents of the security event, the method including: collecting security events occurring in a network system; classifying and storing the security events for each type according to a relation between a source port and a destination port of contents of the collected security event; analyzing the number of the security events stored for each type and calculating a port relation distribution; and sampling the security event by using the calculated port relation distribution.

[16] The method may further include determining a sampling ratio of the security event by comparing the set maximum number of the processed the security events for each stage and an average number of security events received per second for a T amount of time, before the calculating the port relation distribution.

[17]

[18]

Brief Description of the Drawings

[19] FIG. 1 is a configuration diagram illustrating an apparatus for sampling a security event based on contents of the security event, according to an exemplary embodiment of the present invention;

[20] FIG. 2 is a flowchart illustrating a method of sampling a security event based on contents of the security event, according to an exemplary embodiment of the present invention;

[21] FIG. 3 is a flowchart illustrating an algorithm of determining a sampling ratio of a sampling ratio determination module 120 according to an exemplary embodiment of the present invention; and

[22] FIG. 4 is a flowchart illustrating a process of calculating content relation distribution with respect to security events stored for each type in an event analysis module 130 according to an exemplary embodiment of the present invention.

[23]

Best Mode for Carrying Out the Invention

[24] Hereinafter, exemplary embodiments of the present invention will now be described in detail with reference to the accompanying drawings.

[25] Only, in describing operations of the exemplary embodiments in detail, when it is considered that a detailed description on related well-known functions or constitutions unnecessarily may make essential points of the present invention be unclear, the detailed description will be omitted.

[26] In the drawings, the same reference numerals are used throughout to designate the same or similar components.

[27] Throughout the specification, when it is describe that a part is "connected to" another part, this includes not only a case of "being directly connected to" but also a case of "being electrically connected to" interposing another device therebetween.

[28] Also, when it is described that an apparatus "includes" an element while there is no opposite description thereof, this is not designate that the apparatus excludes other elements but designates that the apparatus may further include other elements.

[29] The term of "module" indicates a unit for processing a certain function or operation, which can be embodied by software, hardware, or a combination of software and

hardware.

- [30] FIG. 1 is a diagram illustrating an apparatus for sampling security events based on contents of the security events, according to an exemplary embodiment of the present invention.
- [31] Referring to FIG. 1, the apparatus includes a security event storage unit 100, a security event accumulation module 110, a sampling ratio determination module 120, a security event analysis module 130, and a security event extraction module 140.
- [32] The security event accumulation module 110 collects security events generated from a network system existing in a network, classifies contents of the collected security events for each type, and stores in respective memories 101 to 104 of the event security storage unit 100.
- [33] That is, in the respective memories 101 to 104 of the security event storage unit 100, there are stored only security events corresponding to four types classified by the security event analysis module 130 according to a port relation between a source port and a destination port in the contents.
- [34] In this case, contents of a security event include a source Internet Protocol (IP) address, a source port, a destination IP address, a destination port, and a protocol. The contents are important to determine a security state of a network.
- [35] Accordingly, in the present invention, there is used port relation distribution where security events are classified for each port relation between the source port and the destination port in the contents of the security event. Also, instead of the port relation distribution, there may be used IP address relation distribution where IP addresses are classified for each country or domain.
- [36] Also, the sampling ratio determination module 120 determines a sampling ratio by comparing an average number of security events received per second for a preset T amount of time with a maximum number of processed security events, which is previously defined security event processing performance of a system for each stage. A process of determining the sampling ratio by the sampling ratio determination module 120 will be described in detail with reference to FIG. 3.
- [37] The security event analysis module 130 calculates port relation distribution by analyzing a number of security events stored in the respective memories 101 to 104. That is, the security event analysis module 130 calculates the port relation distribution by calculating an existence ratio of the number of security events stored in the respective memories 101 to 104 with respect to a number of overall security events.
- [38] Also, the security event analysis module 130 sets and previously defines a type of a security event according to a port relation between a source port and a destination port in contents of the security event in such a way that the security event accumulation module 110 stores the security events in a plurality of storage areas in the security

event storage unit 100. A process of calculating the port relation distribution by the security event analysis module 130 will be described in detail with reference to FIG. 4.

[39] The security event extraction module 140 extracts and samples security events by using the sampling ratio determined by the sampling ratio determination module 120 and the port relation distribution calculated by the security event analysis module 130 and transmits the sampled security events.

[40] FIG. 2 is a flowchart illustrating a method of sampling a security event based on contents of the security event, according to an exemplary embodiment of the present invention.

[41] Referring to FIG. 2, the security event accumulation module 110 collects security events from network systems present in a network (S100).

[42] The security event accumulation module 110 classifies the security events for each type according to a port relation between a source port and destination port in contents of the collected security event and stores in respective memories 101 to 104 of the security event storage unit 100.

[43] In this case, each type of security events stored in each of the memories 101 to 104 of the security event storage unit 100 is previously defined by the security event analysis module 130. For example, based on well-known 1024th port, there are four types in the port relation between a source port and destination port.

[44] Instead of the well-known 1024 port, a security event type may be defined by classifying IP addresses for each country or domain.

[45] The sampling ratio determination module 120 determines a sampling ratio of the security events by comparing an average number A of received security events per second for a T amount of time set by a user with a maximum number of processing security events, which is previously defined security event processing performance of a system for each of a plurality of stages (S120).

[46] The security event analysis module 130 calculates port relation distribution of the security event by analyzing a number of security events for each type stored in each of the memories 101 to 104 of the security event storage unit 100 (S130).

[47] The security event extraction module 140 samples the security events stored in the security event storage unit 100 by using the sampling ratio determined by the sampling ratio determination module 120 and the port relation distribution calculated by the security event analysis module 130 (S140).

[48] On the other hand, in the present invention, the sampling ratio may be fixed without performing S120.

[49] FIG. 3 is a flowchart illustrating the process where the sampling ratio determination module 120 determines the sampling ratio by comparing the average number of received security events per second for a T amount of time with the maximum number

of processing security events, which is the previously defined security event processing performance of the system for each stage.

- [50] To sample suitably for system performance, a maximum number of security events capable of being processed for each stage of security event processing performance of the system is defined. An initial value of the maximum number P of presently processing security events in the system is a maximum number of P_t of processing security events at a t stage corresponding to present processing performance of the system ($P=R \cdot P_t$, R is a constant).
- [51] As described above, in a state where a maximum number of security events for each processing performance of the system is determined, when collecting a number of security events is finished, the sampling ratio determination module 120 calculates the average number A of the received security events per second for the T amount of time set by the user by using a number of security events received per second (S200).
- [52] After that, it is checked whether the average number A of the received security events per second is greater than the maximum number of P_t presently set in the system ($P=R \cdot P_t$, R is a constant) (S210).
- [53] As a result of the checking in S210, when the average number A of the received security events per second is identical to or greater than the maximum number of processing security events ($P=R \cdot P_t$, R is a constant), the sampling ratio is increased by increasing from a t stage to a $t+1$ stage among stages defining processing performance of a system. In addition, a maximum number of processing security events in a present system is increased to a $t+1$ stage.
- [54] Accordingly, a sampling ratio S of the present system and a maximum number P of processing security events are adjusted to $K \cdot S_{t+1}$ and $K \cdot P_{t+1}$ (K is a constant) (S220).
- [55] On the other hand, as a result of S210, when the average number A of the received security events per second is not identical to nor greater than a present maximum number of processing security events ($P=R \cdot P_t$, R is a constant), it is checked whether the average number A of the received security events per second is close to a maximum number (P_{t-1}) of processing security events corresponding to a $t-1$ stage lower than the present t stage (S230).
- [56] As a result of the checking in S230, when the average number A of the received security events is smaller than the maximum number P_{t-1} of processing security events at the $t-1$ stage, an adjacent stage is searched by comparing each of maximum numbers P_{t-2} , P_{t-3} , ..., and P_{t-n} stored in each of stages $t-2$, $t-3$, ..., and $t-n$, substitute $t=t-1$) with the average number A of the received security events while decreasing a level of a stage (S240).
- [57] As a result of the searching in S240, when the average number A of the received

security events gets close to the maximum number P_{t-n} of processing security events at the $t-n$ stage, the sampling ratio S of the present system and the maximum number P of processing security events are changed into $S=K \cdot S_{t-n}$, $P=K \cdot P_{t-n}$ (K is a constant) to be suitable for the close $t-n$ stage (S250).

- [58] According to this, a suitable sampling ratio is set to processing performance of the present system.
- [59] FIG. 4 is a flowchart illustrating a detailed process where the security event analysis module 130 calculates relation distribution by analyzing a number of security events stored in each of the memories 101 to 104 of the security event storage unit 100.
- [60] Generally, there are shown a lot of network attacks in a type of randomly varying a source port or a destination port smaller than 1024 port and well-known or randomly varying both of the source port and destination port while performing the network attack.
- [61] Also, since most of cases when both of the source port and the destination port are smaller than the well-known 1024 port are normal network traffics, it becomes very important characteristics whether both of the source port and the destination port are well-known and smaller than 1024 port.
- [62] Accordingly, the security event analysis module 130 defines a type of a security event based on 1024 port as one of following four types.
- [63] (1) a case where both of a source port and destination port are smaller than 1024 port
- [64] (2) a case where a source port is smaller than 1024 port and a destination port is greater than 1024 port
- [65] (3) a case where a source port is greater than 1024 port and a destination port is smaller than 1024 port
- [66] (4) a case where both of a source port and destination port are greater than 1024 port
- [67] Accordingly, the security event accumulation module 110 classifies received security events according to the four types defined as described above and stores the security events in the respective memories 101 to 104 of the security event storage unit 100.
- [68] Then, the security event analysis module 130 analyzes a number of security events for each type present in the four memories 101 to 104 of the security event storage unit 100 (S300), calculates an existence ratio of the number of security events for each type with respect to a number of overall security events (S310), and calculates port relation distribution X (S320).
- [69] For example, when there are security events corresponding to four types such as (1), (2), (3), and (4) in four memories of the security event storage unit 100 as 10, 20, 40, and 30, respectively, since port relation distribution X of the security events is an existence ratio (10/100, 20/100, 40/100, and 30/100) of each of the types with respect to a number of overall security events (10+20+40+30=100), the port relation dis-

tribution X becomes {0.1, 0.2, 0.4, and 0.3}.

[70] Accordingly, as a result of calculating the port relation distribution X, since a number of the security events of (3) type is largest, sampling is performed in such a way that a number of the security events of (3) types is largest when transmitting the security events after sampling.

[71] The invention can also be embodied as computer readable codes on a computer readable recording medium. The computer readable recording medium is any data storage device that can store data which can be thereafter read by a computer system.

[72] Examples of the computer readable recording medium include read-only memory (ROM), random-access memory (RAM), CD-ROMs, magnetic tapes, floppy disks, optical data storage devices, and carrier waves (such as data transmission through the Internet).

[73] The computer readable recording medium can also be distributed over network coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

[74] Also, functional programs, codes, and code segments for accomplishing the present invention can be easily construed by programmers skilled in the art to which the present invention pertains.

[75] While the present invention has been shown and described in connection with the exemplary embodiments, it will be apparent to those skilled in the art that modifications and variations can be made without departing from the spirit and scope of the invention as defined by the appended claims.

[76]

Claims

- [1] An apparatus for sampling a security event based on contents of the security event, the apparatus comprising:
a security event accumulation module collecting security events occurring in a network system and storing the security events for each type according to contents of the security event;
a security event analysis module calculating distribution of the security events for each type by analyzing the stored security events; and
a security event extraction module sampling the stored security events according to the calculated distribution of the security events for each type.
- [2] The apparatus of claim 1, wherein the contents of the security event comprises a source Internet Protocol (IP) address, a destination IP address, a source port, a destination port, and a protocol.
- [3] The apparatus of claim 1, further comprising a security event storage unit having a plurality of storage areas for storing the security events for each type.
- [4] The apparatus of claim 3, wherein the security event analysis module analyzes a number of the security events stored in the plurality of storage areas, obtains an existence ratio of the security events for each type stored in each of the plurality of storage areas with respect to the entire security events, and calculates port relation distribution.
- [5] The apparatus of claim 4, wherein the security events for each type are classified into four types based on 1024 port with respect to the source port and destination port of the contents.
- [6] The apparatus of claim 5, wherein the four types are a case where both of the source port and destination port of the contents are smaller than 1024 port, a case where the source port is smaller than 1024 port and the destination port is greater than 1024 port, a case where the source port is greater than 1024 port and the destination port is smaller than 1024 port, and a case where both of the source port and the destination port are greater than 1024 port.
- [7] The apparatus of claim 4, wherein the security events for each type are classified according to references set with respect to the source IP address and the destination IP address of the contents.
- [8] The apparatus of claim 1, further comprising a sampling ratio determination module determining a sampling ratio in proportion to processing performance of a system and an average number of received security events per second for a set T amount of time.
- [9] The apparatus of claim 8, wherein the sampling ratio determination module

compares the average number of the received security events per second for the set T amount of time with a previously defined maximum number of processing the security events for each stage, obtains a maximum number of processing the security events of an adjacent stage, and controls the sampling ratio to be corresponding to the obtained maximum number of processing the security events of the stage.

[10] The apparatus of claim 9, wherein the security event extraction module samples the security events by using the distribution of the security events for each type calculated by the security event analysis module and the sampling ratio determined by the sampling ratio determination module.

[11] A method of sampling a security event based on contents of the security event, the method comprising:
collecting security events occurring in a network system;
classifying and storing the security events for each type according to a relation between a source port and a destination port of contents of the collected security event;
analyzing a number of the security events stored for each type and calculating a port relation distribution; and
sampling the security event by using the calculated port relation distribution.

[12] The method of claim 11, wherein, in the classifying and storing the security events for each type, the types of the security events are divided, based on 1024 port, into a case where both of the source port and destination port of the contents are smaller than 1024 port, a case where the source port is smaller than 1024 port and the destination port is greater than 1024 port, a case where the source port is greater than 1024 port and the destination port is smaller than 1024 port, and a case where both of the source port and the destination port are greater than 1024 port.

[13] The method of claim 12, further comprising, before the calculating the port relation distribution:
dividing a security event processing process into a plurality of stages and setting a maximum number of processed security events and a sampling ratio for each stage; and
determining a sampling ratio of the security event by comparing the set maximum number of the processed the security events for each stage and an average number of security events received per second for a T amount of time.

[14] The method of claim 13, wherein the determining a sampling ratio of the security event comprises:
calculating the average number A of the security events received per second for

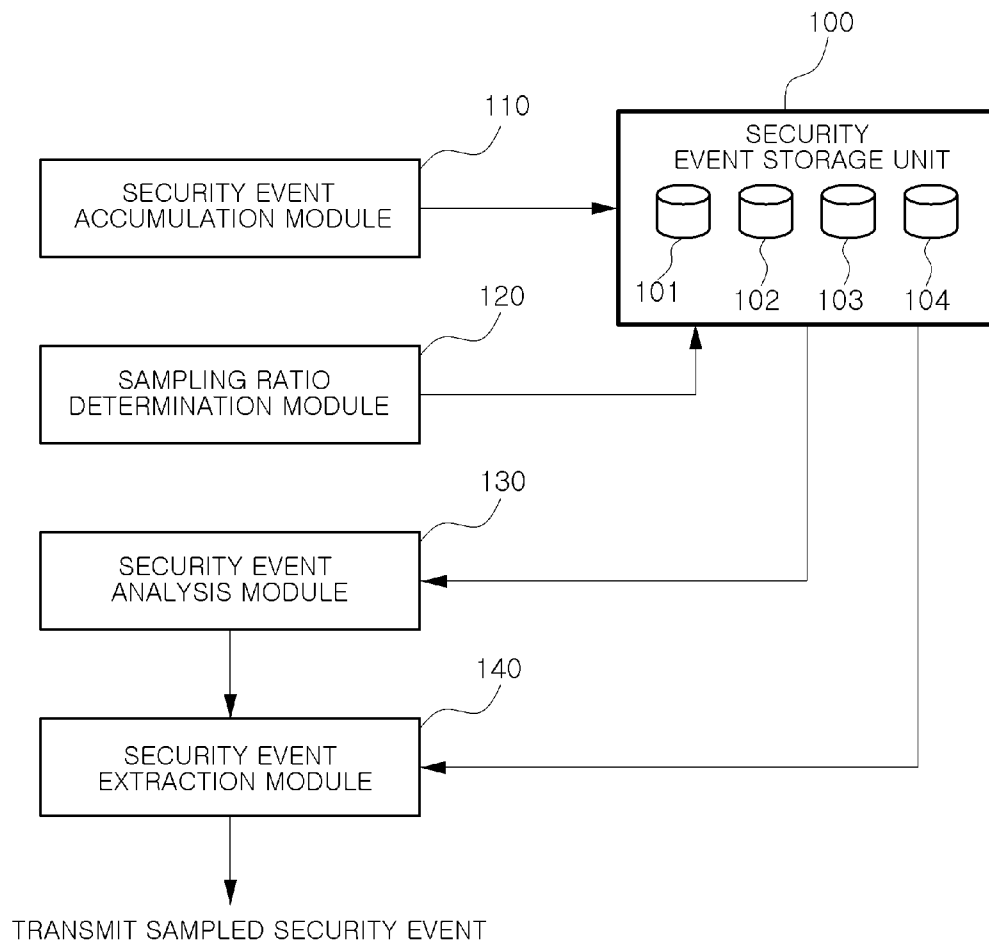
the T amount of time;

checking whether the average number A of the security events received per second for the T amount of time is close to a maximum number P_t of security events processed in a t stage corresponding to present security event processing performance; and

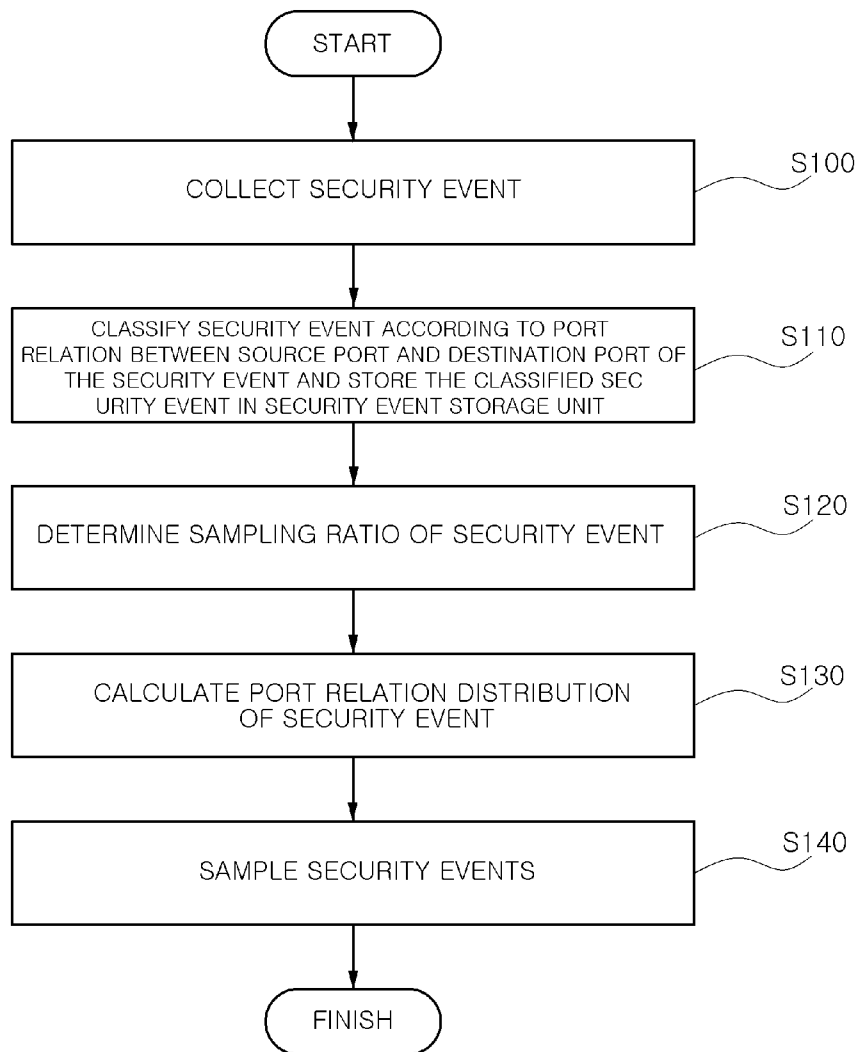
increasing the sampling ratio and the security event processing performance of the system from the t stage to a t+1 stage when the average number A of the security events received per second is close to the maximum number P_t of the security events processed in the t stage as a result of the checking.

- [15] The method of claim 14, wherein, when the average number of the security events received per second is not close to the maximum number P_t of the security events processed in the t stage as the result of the checking, the determining a sampling ratio of the security event comprises:
- checking whether the average number A of the security events received per second is close to a maximum number P_{t-1} of security events processed in a t-1 stage lower than the present t stage and adjusting the sampling ratio and the security event processing performance of the system to be suitable for the t-1 stage when the average number A of the security events received per second is close to the maximum number P_{t-1} of the security events processed in the t-1 stage;
- searching a t-n stage that is close by comparing the average number A of the security events received per second with maximum numbers of security events processed in the respective stages obtained by dividing the security event processing performance of the system when the average number A of the security events received per second is not close to the maximum number P_{t-1} of the security events processed in the t-1 stage; and
- adjusting the sampling ratio and the security event processing performance of the system to be suitable for the t-n stage when a maximum number of security events processed in the t-n stage to which the average number A of the security events received per second is close is searched.

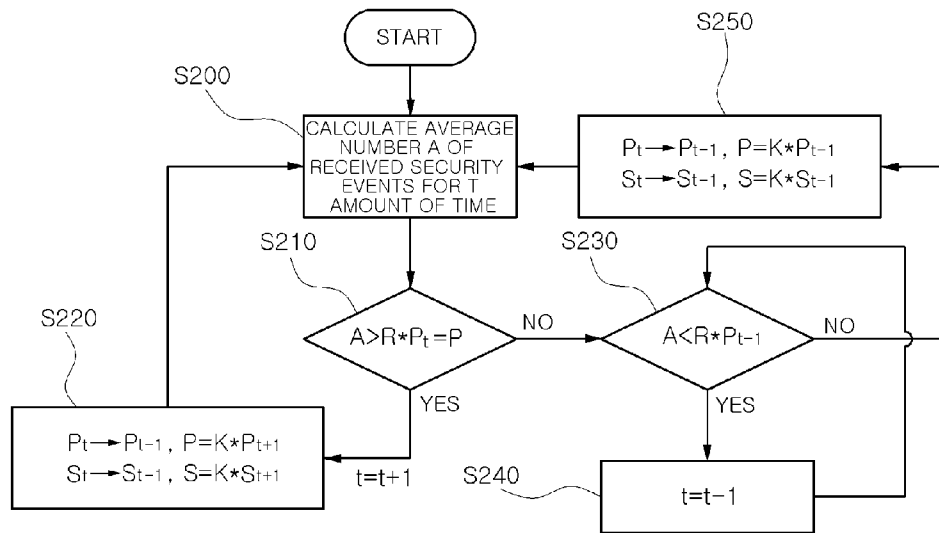
[Fig. 1]



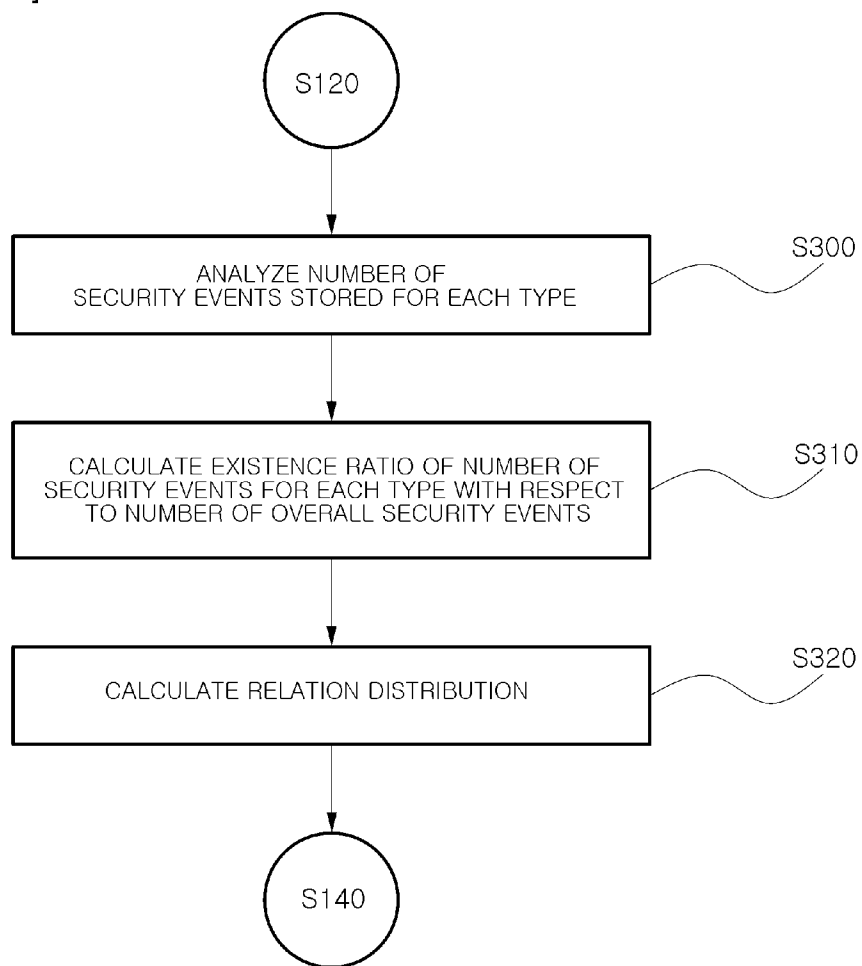
[Fig. 2]



[Fig. 3]



[Fig. 4]



A. CLASSIFICATION OF SUBJECT MATTER**G06F 15/00(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : G05F 15/00, H04L 9/00, H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility Models and applications for Utility Model since 1975

Japanese Utility Models and applications for Utility Model since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKIPASS(KIPO internal) "sampling", "intrusion", "analyze"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 1020040092314 A (LGNSYS INC.) 03 November 2004 See abstract, claims	1-15
A	Animesh Patcha et al. 'An Adaptive Sampling algorithm with Applications to Denial-of-Service Attack Detection.' In: Proceedings 15th International Conference on Computer Communications and Networks, 2006 ICCCN 2006, 31 October 2006, pp.11-16	1-15
A	WO 2006127012 A2 (LANCOPE, INC.) 30 November 2006 See abstract, claims	1-15
A	KR 1020010085057 (KIM SANG-WOOK) 07 September 2001 See abstract, claims	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

10 MARCH 2008 (10.03.2008)

Date of mailing of the international search report

10 MARCH 2008 (10.03.2008)

Name and mailing address of the ISA/KR

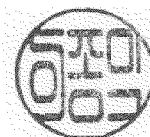
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Jong Ick

Telephone No. 82-42-481-8373



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2007/005797Patent document
cited in search reportPublication
datePatent family
member(s)Publication
date

KR 1020040092314 A

03.11.2004

NONE

WO 2006127012 A2

30.11.2006

US 2005210533 AA

22.09.2005

KR 1020010085057 A

07.09.2001

NONE