(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2002 (10.05.2002)

PCT

(10) International Publication Number
WO 02/37755 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US01/45720

(22) International Filing Date: 30 October 2001 (30.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/706,503 2 November 2000 (02.11.2000) US

(71) Applicant: **ASTA NETWORKS, INC.** [US/US]; 520 Pike Street, Suite 1800, Seattle, WA 98101 (US).

(72) Inventors: **WETHERALL, David, J.**; 6106 44th Ave. NE, Seattle, WA 98115 (US). **SAVAGE, Stefan, R.**; 7595 Navigator Circle, Carlsbad, CA 92009 (US). **ANDERSON, Thomas, E.**; 1201 18th Avenue East, Seattle, WA 98112 (US).

(74) Agents: **AUYEUNG, Aloysius, T.C.** et al.; Columbia IP Law Group, PC, Suite 820, 10260 SW Greenburg Road, Portland, OR 97223 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

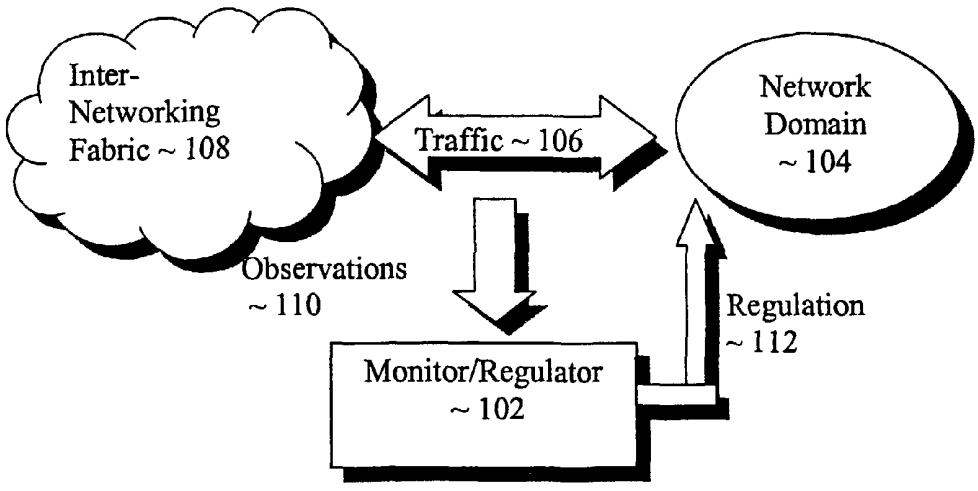
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

[Continued on next page]

(54) Title: DETECTING AND PREVENTING UNDESIRED NETWORK TRAFFIC FROM BEING SOURCED OUT OF A NETWORK DOMAIN



(57) Abstract: The present invention provides for a novel approach to protecting a system owner's system(s) from being exploited in providing involuntary assistance to a DOS attack. The present invention provides the protection by detecting and preventing undesirable or inappropriate network traffic from being sourced from a network domain. More specifically, a monitor/regulator is provided to monitor network traffic leaving a network domain. The monitor/regulator determines if undesirable/inappropriate network traffics are leaving the network domain based on the observed characteristics of the outbound and inbound network traffics. If it is determined that undesirable/inappropriate network traffics are leaving the network domain, the monitors/regulator, in one embodiment, at least warns system owners of the detection. In another embodiment, the monitors/regulator further issues regulation instruction(s) to boundary routing device(s) of the network domain(s), thereby preventing the network domain(s) from being exploited to source such undesirable/inappropriate network traffics.

WO 02/37755 A2

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Detecting and Preventing Undesired Network Traffic From Being Sourced Out Of A Network Domain

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of networking. More specifically, the present invention relates to the monitoring and regulation of routing devices of network domains to detect and prevent undesirable network traffic from being sourced out of the network domains.

2. Background Information

With advances in integrated circuit, microprocessor, networking and communication technologies, increasing number of devices, in particular, digital computing devices, are being networked together. Devices are often first coupled to a local area network, such as an Ethernet based office/home network. In turn, the local area networks are interconnected together through wide area networks, such as ATM networks, Frame Relays, and the like. Of particular notoriety is the TCP/IP based global inter-networks, Internet.

As a result of this trend of increased connectivity, increasing number of applications that are network dependent are being deployed. Examples of these network dependent applications include but are not limited to, email, net based telephony, world wide web and various types of e-commerce. Success of many of these content/service providers as well as commerce sites depend on the quality of service they provide.

Unfortunately, the connectivity that makes it possible for these servers to provide the content/service, also makes it very easy for hackers to launch

denial of service (DOS) attacks against these servers. Compounding the misfortunes is the fact that often times, innocent systems are exploited in assisting the attacks, without the system owners even knowing their systems are being exploited. The exploitation not only may affect the level of services delivered by the exploited systems, it may also leave the exploited systems vulnerable to liability for the damages inflicted on the servers being attacked.

To-date, all the known methods and apparatuses that can assist a system owner in protecting his/her systems from being exploited are basically intrusion protection oriented. That is all the methods and apparatuses are substantially oriented towards keep undesirable network traffics from entering a network domain and/or preventing unauthorized executing on the owner's systems. As experience have demonstrated, none of these methods and apparatuses is perfect. From time to time, we learned that hackers are able to get through. Thus, additional methods and apparatuses that can further prevent systems from being exploited in giving involuntary assistance to DOS attacks are desired.

SUMMARY OF THE INVENTION

The present invention provides for a novel approach to warning and/or protecting a system owner's system(s) from being exploited in providing involuntary assistance to a DOS attack. The present invention provides the protection by detecting and/or preventing undesirable or inappropriate network traffic from being sourced from a network domain. More specifically, a monitor/regulator is provided to monitor network traffic leaving a network domain. The monitor/regulator determines if undesirable/inappropriate network traffics are leaving the network domain based on the observed characteristics of the outbound and inbound network traffics. In one embodiment, if it is

determined that undesirable/inappropriate network traffics are leaving the network domain, the monitors/regulator at least issues warnings alerting system owners of the detection. In another embodiment, the monitor/regulator further issues regulation instruction(s) to boundary routing device(s) of the network domain(s), thereby preventing the network domain(s) from being exploited to source such undesirable/inappropriate network traffics.

In one embodiment, the determination is made based on differential characteristics of the outbound and inbound network traffics. In one embodiment, the differential characteristics are inferred from differences between observed aggregated statistics of the outbound and inbound network traffics. In another embodiment, the differential characteristics are aggregated from individual flow differences.

In one embodiment, the monitor/regulator monitors and/or regulates a single boundary routing device of a network domain. In another embodiment, the monitor/regulator monitors and/or regulates multiple boundary routing devices of a network domain. In yet another embodiment, the monitor/regulator monitors and/or regulates boundary routing devices of multiple network domains, with each network domain having one or more routing devices.

In one embodiment, the monitor/regulator is integrally implemented as a single component. In another embodiment, the monitor/regulator is distributedly implemented as separate components.

In one embodiment, the monitor/regulator is independently implemented, i.e. externally and remotely disposed outside of the monitored/regulated routing devices. In another embodiment, at least part of the monitor/regulator is integrally implemented with at least one of the monitored/regulated routing devices.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 illustrates an overview of the present invention, including a network traffic monitor/regulator of the present invention, in accordance with one embodiment;

Figure 2 illustrates a method view of the same invention, in accordance with one embodiment;

Figures 3a-3c illustrate the present invention in further details, in accordance with three embodiments; and

Figure 4 illustrates an example digital system suitable for use to host a software implementation of the network traffic monitor/regulator of the present invention, in accordance with one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Parts of the description will be presented in terms of operations performed by a processor based device, using terms such as receiving, analyzing, determining, instructing, and the like, consistent with the manner commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. As well understood by those skilled in the art, the quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of the processor based device; and the term processor include microprocessors, micro-controllers, digital signal processors, and the like, that are standalone, adjunct or embedded.

Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation. The terms "routing devices" and "route" are used throughout this application, in the claims as well as in the specification. The terms as used herein are intended to be genus terms that include the conventional routers and conventional routing, as well as all other variations of network trafficking, such as, switches or switching, gateways, hubs and the like. Thus, unless particularized, the terms are to be given this broader meaning. Further, the description repeatedly uses the phrase "in one embodiment", which ordinarily does not refer to the same embodiment, although it may.

Overview

Referring now first to **Figures 1-2**, wherein two block diagrams illustrating a topological view and a method view of the present invention, in accordance with one embodiment, are shown. As illustrated by these figures,

in accordance with the present invention, monitor/regulator **102** is advantageously provided to protect system owner of systems (not shown) located within network domain **104** from being exploited in providing involuntary assistance to a DOS attack against other systems (also not shown). Monitor/regulator **102** is equipped with logic to monitor or observe network traffics **106** routed between network domain **104** and internetworking fabric **108** (block **202**), and based on observations **110**, determines if undesirable or inappropriate network traffics are being sourced out of network domain **104** into internetworking fabric **108** (block **204**). If so, in one embodiment, monitor/regulator **102** is further equipped to at least issue warnings alerting system owners of the detection. In another embodiment, monitor/regulator **102** is further equipped to regulate the boundary routing device or devices of network domain **104** (not shown), such as issuing regulation instructions **112** to the routing device(s) to prevent such undesirable or inappropriate network traffics from being sourced out of network domain **104** into internetworking fabric **108** (block **206**), thereby reducing or eliminating the possibility of exploiting the systems of network domain **104**.

Network domain **104** and internetworking fabric **108** are intended to represent a broad range of local or wide area networks known in the art. For examples, network domain **104** may be a local area network of an enterprise, and internetworking fabric **108** is the private internetworking fabric of the enterprise, or network domain **104** may be a wide area (such as a metropolitan area) network of an enterprise, and the internetworking fabric **108** is a public internetworking fabric (such as the Internet).

First Embodiment

Figure 3a illustrates a first embodiment of the present invention, wherein network domain **104'** has a single egress point for network traffics **106**

to leave network domain **104'** and enters internetworking fabric **108**. As described earlier, monitor/regulator **102'** monitors or observes network traffics **106'** routed between network domain **104'** and internetworking fabric **108** through routing device **114'** (block **202**), and based on observations **110'**, determines if undesirable or inappropriate network traffics are being sourced out of network domain **104'** into internetworking fabric **108** through routing device **114'** (block **204**). If so, for one implementation of the illustrated embodiment, monitor/regulator **102'** at least issues warnings alerting system owners of the detection. In another implementation, monitor/regulator **102'** regulates routing device **114'**, issuing regulation instructions **112'** to routing device **114'** to "stop" routing certain traffic, to prevent the undesirable or inappropriate network traffics from being sourced out of network domain **104** into internetworking fabric **108** through routing device **114'** (block **206**). As a result, systems disposed inside network domain **104'** are warned and/or protected from exploitation in providing involuntary assistance to DOS attacks against other systems.

In one embodiment, routing device **114'** is of a type equipped to provide aggregate characteristic statistics on network traffics **106'** routed. Examples of these aggregate characteristic statistics include but are not limited to statistics for traffics of particular types routed in both the outbound and inbound directions. [Outbound refers to network traffics routed from network domain **104'** onto internetworking fabric **108'**, and inbound refers to the opposite.] Other examples of aggregate statistics include the number of bits per second (mbps), the number of packets per second, or the number of flows per second routed in each direction. [A flow may e.g. be a unique traffic conversation as indicated by a combination of source and destination addresses (and for certain protocol, port number also).] Further, the aggregate statistics may also include volume of data destined for specific destination addresses, lengths of

packets, distribution of Time To Live values, and so forth. These other aggregated characteristic statistics may also be provided by network traffic type. In other words, aggregate characteristic statistics may simply be whatever data necessary to provide the desired level of granularity in discerning undesirable versus desirable or appropriate versus inappropriate network traffics.

In alternate embodiments, for certain routing devices, if supported, the relevant data may additionally or alternatively be provided at the individual packet level (as opposed to being in the form of aggregate statistics) for all or selected flows. Similarly, any relevant data provided at the individual packet level may also be provided by network traffic type.

Examples of traffic types include but are not limited to TCP SYN and FIN packets. Network traffic types may further include Web, Real Networks, Secure Web, Other TCP, Other UDP, ICMP, TCP packets with ACK set, TCP packets without SYN set, and so forth. In general, any information carried as part of the packets may be used as typing criteria to divide the network traffic into different traffic types.

Numerous routing devices with such data providing capability are known in the art, including but are not limited to routing devices available from CISCO Systems, or 3COM, both of San Jose, CA, or Juniper Network of Sunnyvale, CA.

Monitor/regulator **102'** monitors/observes network traffics **106'** by periodically requesting routing device **114'** to provide it with the aggregate characteristic statistics of network traffics **106'** routed. In one embodiment, monitor/regulator **102'** periodically requests routing device **114'** to provide at least the aggregate characteristic statistics for the number of TCP SYN and FIN packets routed. In one embodiment, monitor/regulator **102'** uses traffic flow records such as Cisco's netflow (which is intended to produce one record

for each flow) to gather information. In another embodiment, monitor/regulator **102'** uses an access control list (ACL), and commands associated therewith, such as "access-list" and "show access-list" to gather up the relevant data. These commands, including their operations and constitutions, are known in the art. Additional information may be obtained from e.g. product literatures of various routing device manufacturers. In other embodiments, the relevant data may also be obtained through known network management services, such as Simple Network Management Protocol (SNMP), Remote Monitoring (RMON) or packet sampling (if one or more of these service are supported by the routing devices).

As described earlier, based on the observed characteristics of traffic **106'**, monitor/regulator **102'** determines whether undesirable/inappropriate network traffics are being sourced out of network domain **104'** onto internetworking fabric **108** through routing device **114'**.

In one embodiment, monitor/regulator **102'** makes the determination based at least on the relative difference between the number of outbound TCP SYN and FIN packets and the number of inbound response packets responding to these packets. Monitor/regulator **102'** infers that undesirable/inappropriate traffics are being sourced out of network domain **104'** if the difference exceeds a predetermined threshold. The predetermined threshold is empirically determined, and typically set a relatively high level. If notwithstanding the relatively high level, the threshold is still exceeded, the excess suggests that the target destinations of the TCP SYN and FIN packets may be unable to respond due to a deliberate concentration of network traffic targeting one or more destinations. Accordingly a high likelihood exists then, a substantial amount of these TCP SYN and FIN packets are associated with a DOS attack.

In one embodiment, monitor/regulator **102'** additionally or alternatively

makes the determination based on the relative difference between the number of outbound TCP SYN and FIN packets destined for certain destinations, and the number of follow-on non-TCP SYN and FIN packets to the same destinations (typically representative of subsequent substantive requests from a destination after the initial connections established via the TCP SYN and FIN packets). Monitor/regulator **102'** infers that undesirable/inappropriate traffics are being sourced out of network domain **104'** if the difference exceeds a predetermined threshold. The predetermined threshold is also empirically determined. If the threshold is exceeded, the lack of follow-on substantive non-TCP SYN and FIN packets suggests that the target destinations of the TCP SYN and FIN packets may be just contacted to clog up the destinations. Accordingly a high likelihood exists then, a substantial amount of these TCP SYN and FIN packets are associated with a DOS attack.

Those skilled in the art will appreciate that the above described detection and determination may be accomplished by reconfiguring the intrusion detection features equipped in many routing devices to operate in the outbound direction, as opposed to operating in the inbound direction as designed. Further, the second determination provides for earlier warning (if the inference is correct), although potentially it may be less accurate (especially if the destinations are still able to respond). The relative amount of the two different types of risk to assume, i.e. falsely concluding a DOS attack is underway, versus a failure to conclude a DOS is underway, is an application dependent decision.

In another embodiment where data are additionally or alternatively collected at the individual packet level, monitor/regulator **102'** additionally or alternatively makes the determination based on the number of incomplete flows (e.g. outbound request packets not receiving reply packets). Similarly, a "large" number of incomplete flows, exceeding a predetermined threshold

(empirically determined) suggests that the destinations of these incomplete flows are unable to respond, potentially due to the fact that they are being overwhelmed by a deliberate concentration of traffics against the destination. For this embodiment, monitor/regulator **102'** additionally monitors for the response packets of the sampled flows.

Similarly, like kind of analysis on whether substantive follow-up flows exist subsequent to the initial flows establishing connections between systems of network domain **104'** and contacted destinations may also be performed to infer whether undesirable/inappropriate network traffics are being sourced out the network domain **104'**.

In addition to the earlier described aggregate or flow level analysis of TCP SYN and FIN packets, the earlier described analyses may also be performed to detect other types of "flood" attacks, including but are not limited to TCP NUL packets (with no flags set), RST packets, DNS requests (UDP port 53). Again each of these corresponding thresholds may be empirically determined.

Further, the earlier described analyses may similarly be performed to detect Smurf or Fraggle type of DOS attacks. For examples, the earlier described analyses may be performed to detect for outgoing ICMP echo reply packets (Smurf) or UDP echo "reply" packets (Fraggle) destined for a particular (victim) destination. Alternatively, the earlier described analyses may also be performed to detect for outgoing ICMP echo request packets (Smurf) or UDP echo "request" packets (Fraggle) destined for a "broadcast" address. However, these analyses may be performed, examining only the data for the outbound direction.

Thus, it can be seen the present invention may be employed to detect undesirable or inappropriate network traffics headed directly for the victim

destinations or indirectly via third parties, as well as undesirable or inappropriate network traffics sourced directly out of the network domain or indirectly first originating from third parties (and subsequently going through the network domain).

In any event, if monitor/regulator **102'** concludes that undesirable/inappropriate network traffics are not being sourced out network domain **104'**, monitor/regulator **102'** takes no further action. On the other hand, if monitor/regulator **102'** concludes that undesirable/inappropriate network traffics are being sourced out network domain **104'**, in one embodiment, monitor/regulator **102'** issues at least warnings alerting system owners of the detections. The warnings may be delivered in any one of a number of form factors, including electronic messages (delivered e.g. to control consoles, pagers and the like), faxes, audio messages, and the like. For the illustrated embodiment, monitor/regulator **102'** further instructs routing device **114'** to regulate the manner in which routing device **114'** routes traffics 106' onto internetworking fabric 108, to attempt to "stop" these undesirable/inappropriate traffics from being sourced out of network domain **104'**.

For examples, monitor/regulator **102'** may instruct routing device **114'** to drop certain types of packets, or packets destined for certain destinations. Alternatively, monitor/regulator **102'** may instruct routing device **114'** to lower the routing priority of these packets or limiting the amount of bandwidth being given for these packets, thereby slowing the rate or reducing the volume of these packets from being sourced out of network domain **104'**. As a result, monitor/regulator **102'** effectively "stops" the undesirable/inappropriate network traffics from being sourced out of network domain **104'**. In one embodiment, monitor/regulator **102'** uses interface related commands such as "show interface rate-limit" and "rate-limit" to regulate and de-regulate routing device

114'. The functions and constitutions of these commands are also known in the art, accordingly will not be further described.

While for ease of understanding, monitor/regulator **102"** is shown as externally disposed away from routing device **114'**, the present invention may be practiced with monitor/regulator **102"** implemented as a standalone component, independently and externally disposed away from routing device **114'**, or alternatively, the present invention may be practiced with monitor/regulator **102"** integrally implemented in whole or in part, as a portion of routing device **114'**.

Second Embodiment

Figure 3b illustrates a second embodiment of the present invention, wherein network domain **104"** has multiple egress points for network traffics **106"** to leave network domain **104"** and enters internetworking fabric **108**. As described earlier, monitor/regulator **102"** monitors network traffics **106"**, determines if undesirable/inappropriate network traffics are being sourced out of network domain **104"**. If so, monitor/regulator **102"** takes appropriate action to warn and/or "stop" the undesirable/inappropriate network traffics from being sourced out of network domain **104"**. As the earlier described embodiment, monitor/regulator **102"** periodically requests characteristic data of network traffics **106"** routed, except instead of making such requests of only one routing device, monitor/regulator **102"** makes the periodic requests with all the boundary routing devices, such as routing device **114"a** as well as routing device **114"b**. Accordingly, systems disposed inside network domain **104"** are protected from exploitation in providing involuntary assistance to DOS attacks against other systems, or their owners may at least be warned of such exploitations.

Similarly, when monitor/regulator **102"** makes it determination on

whether undesirable/inappropriate network traffics are being sourced out of network domain **104"**, monitor/regulator **102"** takes all the data received into consideration. That is, when analyzing the data received from routing device **114"a**, monitor/regulator **102"** adds or otherwise factors into consideration the data received from routing device **114"b**. Similarly, when analyzing the data received from routing device **114"b**, monitor/regulator **102"** adds or otherwise factors into consideration the data received from routing device **114"a**. As described earlier, the data may be any one of the example data enumerated above, aggregated or at individual flow level.

By aggregating or otherwise takes into consideration characteristic data of network traffics sourced out of routing device **114"a** as well as routing device **114"b**, monitor/regulator **102"** is made more sensitive, and be able to detect undesirable/inappropriate network traffics being sourced out network domain **104"**, even though the decision metrics may not be exceeded at the individual boundary routing devices **114"a** and/or **114"b**.

In one embodiment, monitor/regulator **102"** warns the owner(s) of the systems of network domain **104"** of the detection. For the illustrated embodiment, monitor/regulator **102"** determines the regulation instructions, if needed, separately for the different routing devices. That is, monitor/regulator **102"** determines separate regulation instructions, if any, for the different routing devices. In alternate embodiment, monitor/regulator **102"** may determine the regulation instructions collectively, and have the regulation instructions be applied to all routing devices uniformly.

As alluded to earlier, while for ease of understanding, monitor/regulator **102"** is shown as externally disposed away from routing devices **114"a** and **114"b**, the present invention may be practiced with monitor/regulator **102"** implemented as a standalone component, independently and externally disposed away from routing device **114'**, or alternatively, the present invention

may be practiced with monitor/regulator **102"** distributively, with at least a part of monitor/regulator **102"** integrally implemented as a part of routing device **114"a** and/or routing device **114"b**, as long as the distributed pieces are communicatively coupled to each other and be able to cooperatively practice the present invention.

Third Embodiment

Figure 3c illustrates a third embodiment of the present invention, wherein monitor/regulator **102"'** monitors and regulates network traffics sourced out of multiple network domains, e.g. network domains **104"'a** as well as network domains **104"'b**. Each network domain **104"'a/104"'b** has one or more egress points for network traffics **106"'** to leave the particular network domains **104"'a/104"'b**, and enters internetworking fabric **108**. As described earlier, monitor/regulator **102"'** monitors network traffics **106"'**, determines if undesirable/inappropriate network traffics are being sourced out of network domain **104"'a** and/or **104"'b**. If so, monitor/regulator **102"'** takes appropriate action to warn and/or "stop" the undesirable/inappropriate network traffics from being sourced out of network domain **104"'a** and/or **104b"'**. Accordingly, systems disposed inside network domain **104"** are protected from exploitation in providing involuntary assistance to DOS attacks against other systems, or their owners be at least alerted of their exploitations.

As the earlier described embodiment, monitor/regulator **102"'** periodically requests characteristic data of network traffics **106"'** routed, except instead of making such requests of only routing device or device(s) of one network domain, monitor/regulator **102"'** makes the periodic requests with all the boundary routing devices, such as routing device **114"a** as well as routing device **114"b**, of all network domains **104"'a** and **104"'b**.

Similarly, when monitor/regulator **102"'** makes it determination on

whether undesirable/inappropriate network traffics are being sourced out of network domain **104"'a** and/or **104"'b**, monitor/regulator **102"'** takes all the data received into consideration. That is, when analyzing the data received from routing device **114"'a** of network domain **114"'a**, monitor/regulator **102"'** adds or otherwise factors into consideration the data received from other routing devices of the same or other network domains, such as routing device **114"'b** of network domain **104"'b**. Likewise, when analyzing the data received from routing device **114"'b** of network domain **104"'b**, monitor/regulator **102"'** adds or otherwise factors into consideration the data received from other routing devices of the same or other network domains, such as routing device **114"'a** of network domain **104"'a**. As described earlier, the data may be any one of the example data enumerated above, aggregated or at individual flow level.

By aggregating or otherwise takes into consideration characteristic data of network traffics sourced out of other network domains, monitor/regulator **102"'** is made even more sensitive, and be able to detect undesirable/inappropriate network traffics being sourced out network domain **104"'a** and/or network domain **104"'b**, even though the decision metrics may not be exceeded at the individual routing devices and/or the individual network domains. For example, upon determining that undesirable network traffics are being sourced out of one domain, the threshold criteria for concluding that undesirable network traffics are being sourced out of another domain may be "lowered", as the probability of erroneously concluding that a domain is also being exploited to support the attack is substantially lower, given it has already been determined another domain is being exploited to source an attack. Accordingly, under this embodiment, the detection and prevention can advantageously leverage on information learned and/or determination made for other domains.

In one embodiment, monitor/regulator **102'''** warns the owner(s) of the systems of network domain **104'''** of the detection. For the illustrated embodiment, monitor/regulator **102'''** determines the regulation instructions, if needed, separately for the different routing devices of the different network domains. That is, monitor/regulator **102'''** determines separate regulation instructions, if any, for the different routing devices of the different network domains. In alternate embodiment, monitor/regulator **102'''** may determine the regulation instructions collectively, and have the regulation instructions be applied to all routing devices of all network domains uniformly.

As alluded to earlier, while for ease of understanding, monitor/regulator **102'''** is shown as externally disposed away from routing devices **114'''a** and **114'''b**, the present invention may be practiced with monitor/regulator **102'''** implemented as a standalone component, independently and externally disposed away from routing devices **114'''a** and **114'''b**, or alternatively, the present invention may be practiced with monitor/regulator **102'''** distributively implemented, with at least a part of monitor/regulator **102'''** integrally implemented as a portion of routing device **114'''a** and/or routing device **114'''b**, as long as the distributed pieces are communicatively coupled to each other and be able to cooperatively practice the present invention.

Example Host Digital System

Figure 4 illustrates an example digital system suitable for use as a host to a software implementation of monitor/regulator, in accordance with one embodiment. As shown, digital system **400** includes processor **402**, and system memory **404**. Additionally, digital system **400** includes mass storage devices **406** (such as diskette, hard drive, CDROM and so forth), input/output devices **408** (such as keyboard, cursor control and so forth) and communication interfaces **410** (such as network interface cards, modems and

so forth). The elements are coupled to each other via system bus **412**, which represents one or more buses. In the case of multiple buses, they are bridged by one or more bus bridges (not shown). Each of these elements performs its conventional functions known in the art. In particular, system memory **404** and mass storage **406** are employed to store a working copy and a permanent copy of the programming instructions implementing the monitor/regulator teachings of the present invention. The permanent copy of the programming instructions may be loaded into mass storage **406** in the factory, or in the field, as described earlier, through a distribution medium (not shown) or through communication interface **410** (from a distribution server (not shown). The constitution of these elements **402-412** are known, and accordingly will not be further described.

Conclusion and Epilogue

Thus, it can be seen from the above descriptions, a novel method and apparatus for protecting a system owner's systems from being exploited in providing involuntary assistance to DOS attacks, through detection and/or stopping undesirable/inappropriate network traffics from being sourced out of the owner's network domain has been described.

While the present invention has been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. For examples, as alluded to earlier, the present invention may be practiced with more or less sensors, more directors, and so forth. Thus, the description is thus to be regarded as illustrative instead of restrictive on the present invention.

CLAIMS

What is claimed is:

1. A network comprising:

a first network domain including a first routing device for routing network traffic out of and into the first network domain; and

a monitor/regulator either integrally disposed in said first routing device or coupled to the first routing device to monitor the network traffic routed by said first routing device, and determine if the first network domain is sourcing undesirable network traffic out of the first network domain.

2. The network of claim 1, wherein said monitor/regulator makes said determination based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

3. The network of claim 2, wherein said monitor/regulator infers said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

4. The network of claim 2, wherein said monitor/regulator aggregates said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

5. The network of claim 1, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced our of said first

domain, further stops said undesirable network traffic from being sourced out of said first domain.

6. The network of claim 1, wherein

said first network domain further comprises a second routing device for routing network traffic out of and into the first network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

7. The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

8. The network of claim 6, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

9. The network of claim 6, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of said first network domain, further stops said undesirable network traffic from being sourced out of said first network domain.

10. The network of claim 1, wherein

said network further comprises a second network domain including a second routing device for routing network traffic out of and into the second network domain;

said monitor/regulator further monitors the network traffic routed by said second routing device, and determines if at least a selected one of the first and second network domains is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

11. The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

12. The network of claim 10, wherein said monitor/regulator determines if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

13. The network of claim 10, wherein said monitor/regulator, upon determining undesirable network traffics are being sourced out of at least a selected one of said first and second network domains, further stops said undesirable network traffic from being sourced out of said first and second network domains.

14. A network traffic regulation method comprising:

monitoring network traffic routed by a first routing device of a first network domain; and

determining if the first network domain is sourcing undesirable network traffic out of the first network domain.

15. The method of claim 14, wherein said determining comprises determining based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

16. The method of claim 15, wherein said determining comprises inferring said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

17. The method of claim 15, wherein said determining comprises aggregating said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

18. The method of claim 14, wherein the method further comprises stopping undesirable network traffics from being sourced out of said first network domain.

19. The method of claim 14, wherein the method further comprises

monitoring network traffic routed by a second routing device of said first network domain; and

determining if the first network domain is sourcing undesirable network

traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

20. The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

21. The method of claim 19, wherein said determining comprises determining if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

22. The method of claim 19, wherein the method further comprises stopping undesirable network traffic from being sourced out of the first network domain.

23. The method of claim 19, wherein the method further comprises determining if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

24. The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said first

network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

25. The method of claim 23, wherein said determining comprises determining if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

26. The method of claim 23, wherein the method further comprises stopping undesirable network traffic from being sourced out said first and/or second network domains.

27. An apparatus comprising:

(a) storage medium having stored therein a plurality of programming instructions designed to enable the apparatus to monitor network traffic routed by a first routing device of a first network domain, and determine if the first network domain is sourcing undesirable network traffic out of the first network domain; and

(b) a processor coupled the storage medium to execute the programming instructions.

28. The apparatus of claim 27, wherein the programming instructions enable the apparatus to make said determination based on differential characteristics of network traffic routed out of said network domain, and network traffic routed into the network domain.

29. The apparatus of claim 28, wherein the programming instructions enable the apparatus to infer said differential characteristics based on aggregated statistics of said network traffic routed out of said network domain, and aggregated statistics of said network traffic routed into the network domain.

30. The apparatus of claim 28, wherein the programming instructions enable the apparatus to aggregate said differential characteristics based on differential characteristics between request packets routed out of said network domain, and response packets routed into the network domain.

31. The apparatus of claim 27, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out of said first network domain.

32. The apparatus of claim 27, wherein the programming instructions enable the apparatus to monitor network traffic routed by a second routing device of said first network domain, and determine if the first network domain is sourcing undesirable network traffic out of the first network domain based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

33. The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

34. The apparatus of claim 32, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

35. The apparatus of claim 32, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said first network domain.

36. The apparatus of claim 27, wherein the programming instructions further enable the apparatus to determine if at least a selected one of the first and a second network domain is sourcing undesirable network traffic out of the selected one of the first and second network domains based on network traffic characteristics observed of network traffic routed through said first and second routing devices.

37. The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said first network domain through said first routing device based on network traffic characteristics observed of network traffic routed through said second as well as said first routing device.

38. The apparatus of claim 36, wherein the programming instructions enable the apparatus to determine if undesirable network traffics are being routed out of said second network domain through said second routing device based on network traffic characteristics observed of network traffic routed through said first as well as said second routing device.

39. The apparatus of claim 36, wherein the programming instructions further enable the apparatus to stop undesirable network traffic from being sourced out said
first and/or second network domains.

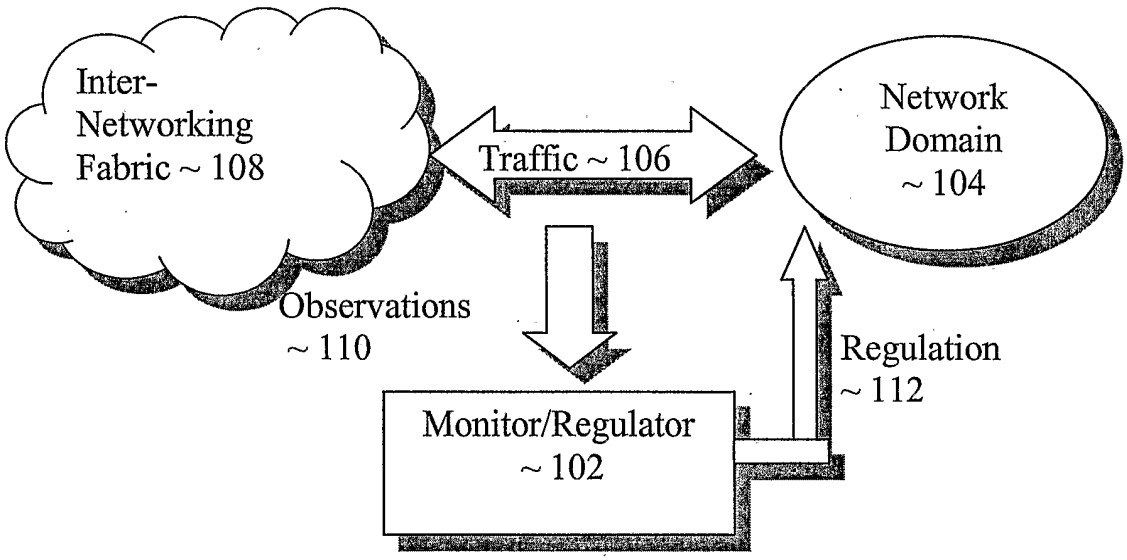

Inter-
Networking
Fabric ~ 108
Traffic ~ 106
Network
Domain
~ 104
Observations
~ 110
Regulation
~ 112
Monitor/Regulator
~ 102

Figure 1

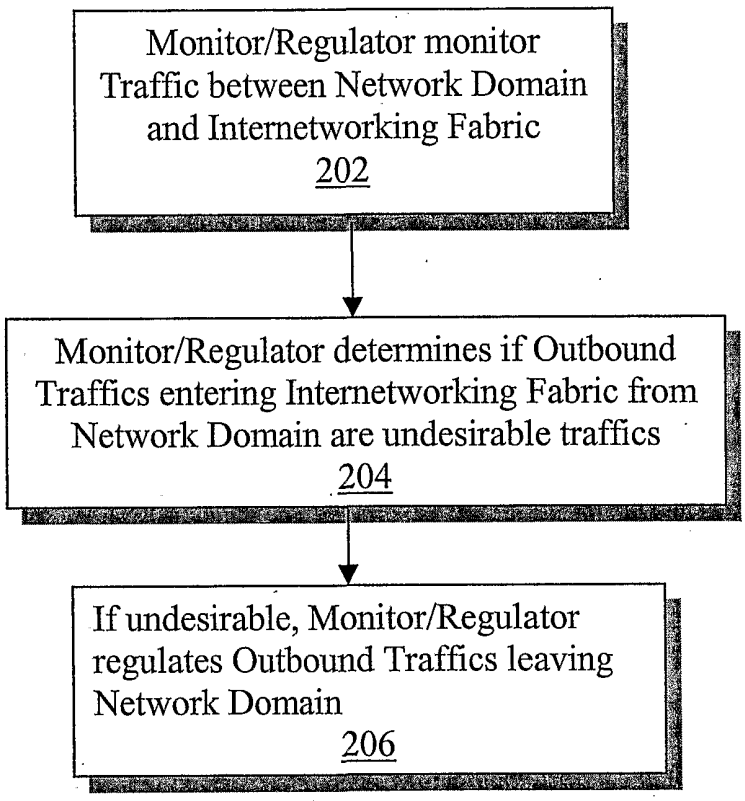

Monitor/Regulator monitor Traffic between Network Domain and Internetworking Fabric
202
Monitor/Regulator determines if Outbound Traffics entering Internetworking Fabric from Network Domain are undesirable traffics
204
If undesirable, Monitor/Regulator regulates Outbound Traffics leaving Network Domain
206
200

Figure 2

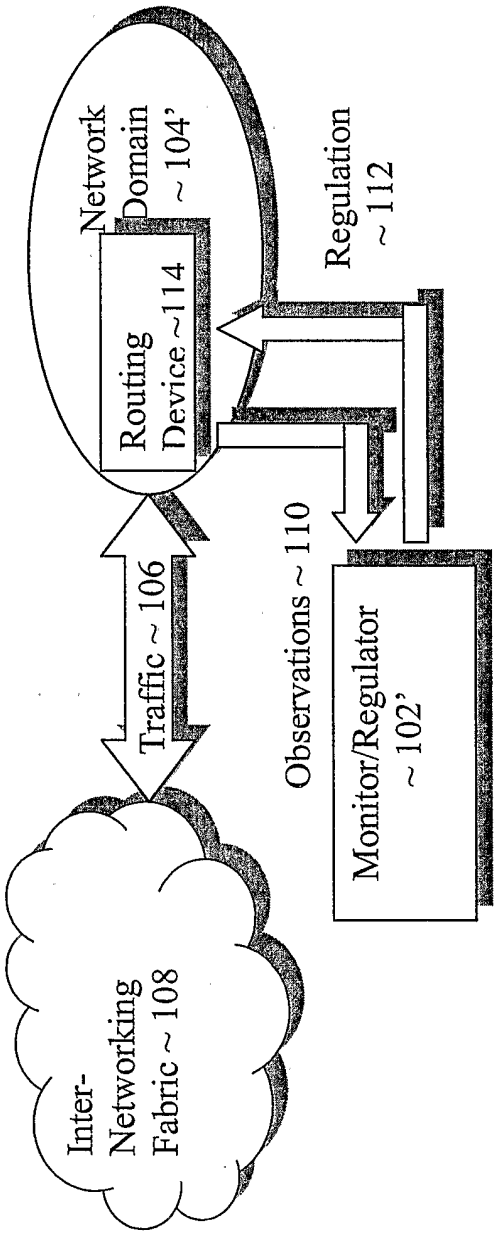

Network Domain ~ 104'
Routing Device ~114
Regulation ~ 112
Observations ~ 110
Traffic ~ 106
Monitor/Regulator ~ 102'
Inter-Networking Fabric ~ 108

Figure 3a

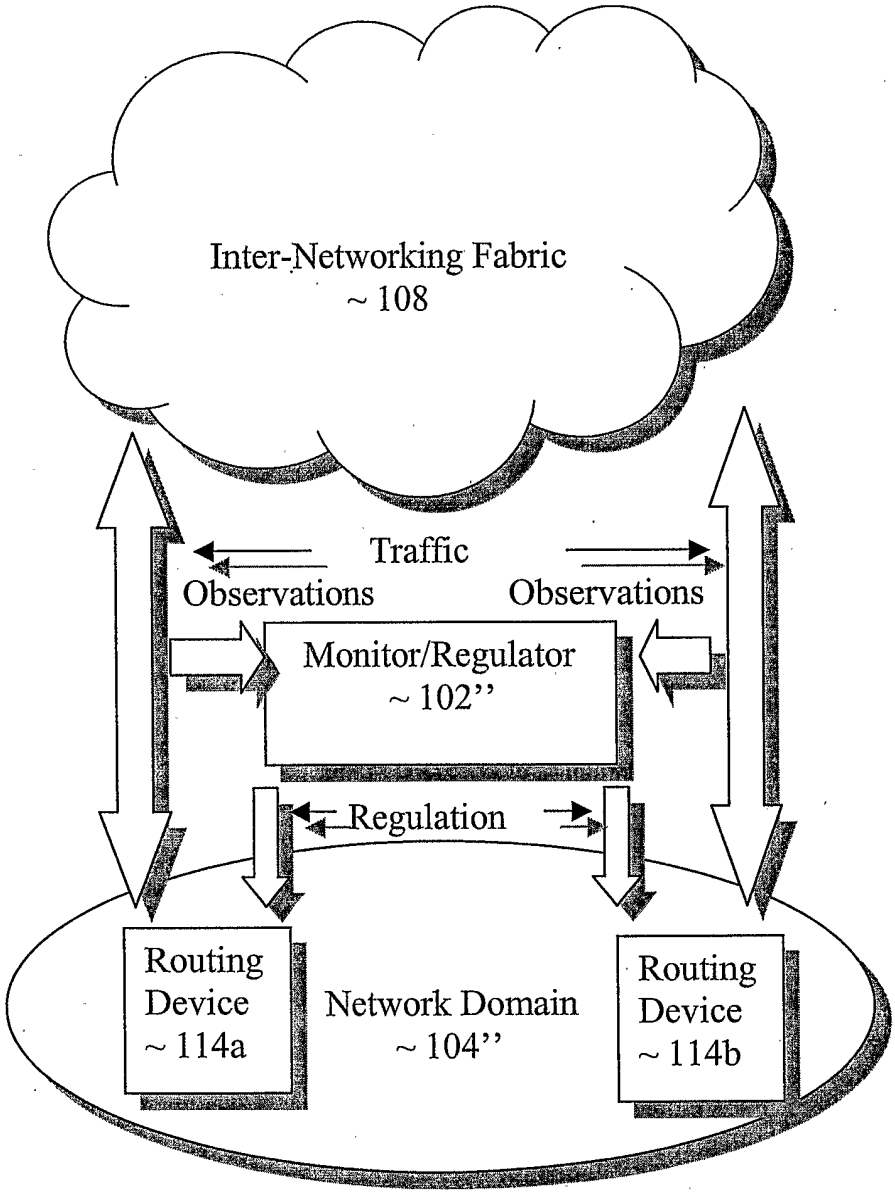

Inter-Networking Fabric
~ 108
Traffic
Observations
Observations
Monitor/Regulator
~ 102''
Regulation
Routing
Device
~ 114a
Network Domain
~ 104''
Routing
Device
~ 114b

Figure 3b

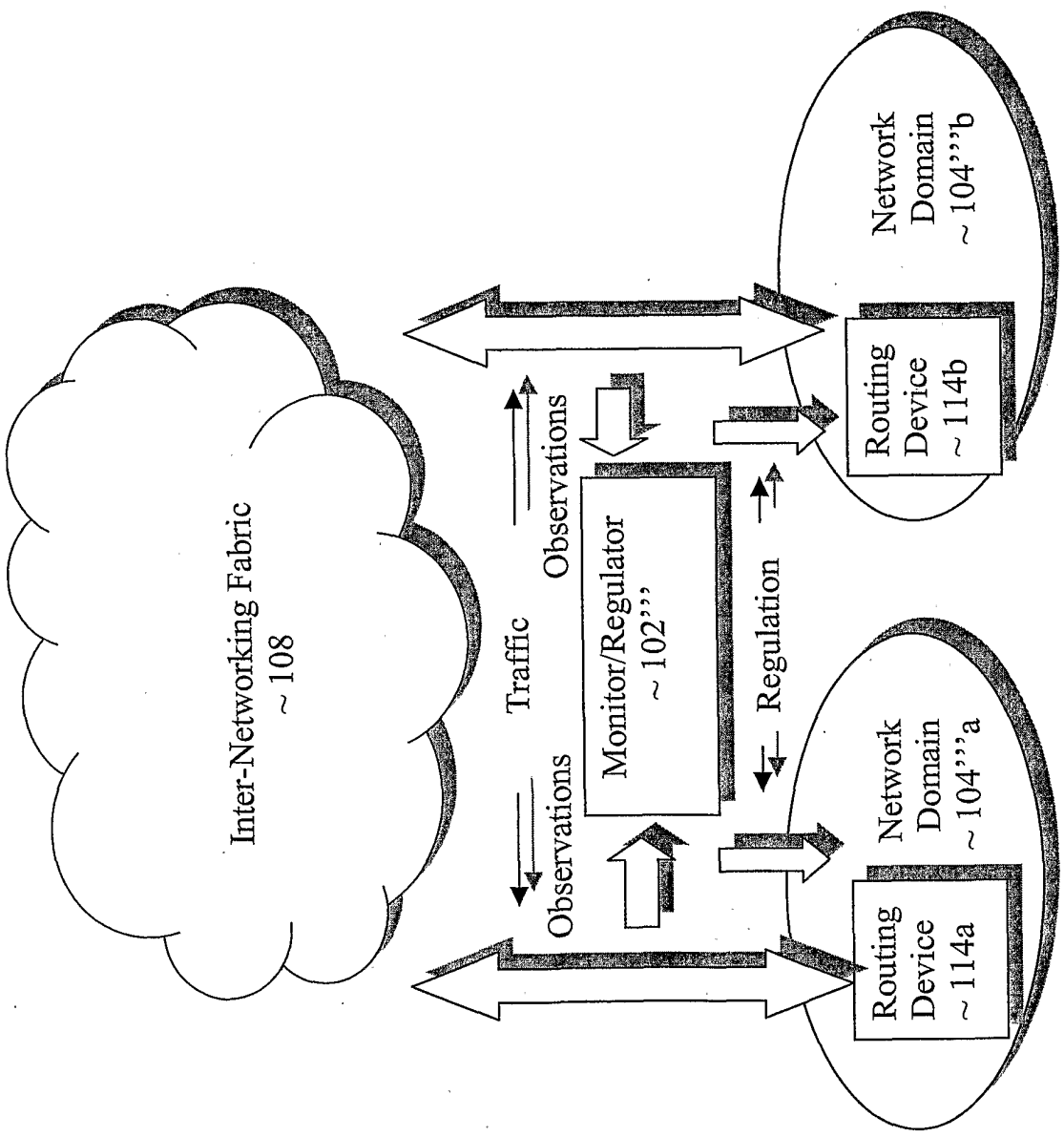

Inter-Networking Fabric
~ 108
Traffic
Observations
Observations
Monitor/Regulator
~ 102'''
Regulation
Routing
Device
~ 114b
Network
Domain
~ 104'''b
Routing
Device
~ 114a
Network
Domain
~ 104'''a

Figure 3c

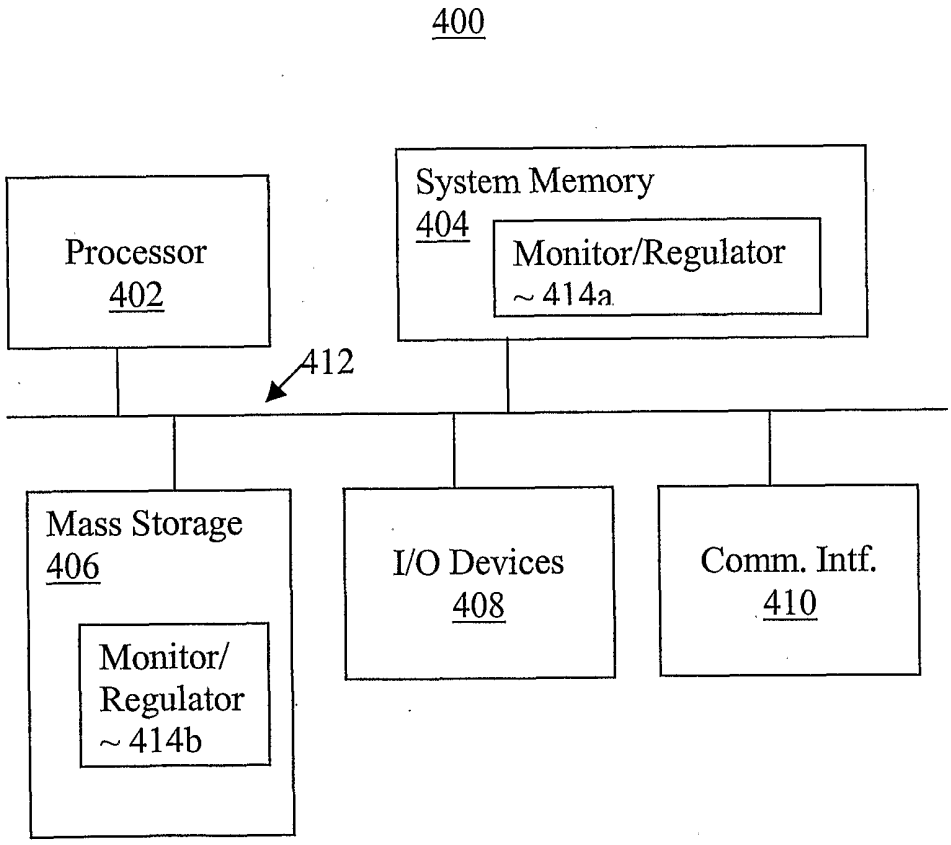

400
Processor
402
System Memory
404
Monitor/Regulator
~ 414a
412
Mass Storage
406
Monitor/
Regulator
~ 414b
I/O Devices
408
Comm. Intf.
410

Figure 4