(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 163**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.04.2008 E 08154391 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2013 EP 2109280**

(54) Título: **Procedimiento y sistema para la estrangulación o el bloqueo de áreas geográficas para la mitigación de los ataques de denegación distribuida de servicio usando una interfaz gráfica de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.04.2013

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

ROSHANDEL, MEHRAN;
GOLDSTEIN, MARKUS;
REIF, MATTHIAS;
STAHL, ARMIN y
BREUE, THOMAS

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento y sistema para la estrangulación o el bloqueo de áreas geográficas para la mitigación de los ataques de denegación distribuida de servicio usando una interfaz gráfica de usuario

Campo de la invención

La invención se refiere en general a la mitigación de ataques de Denegación Distribuida de Servicio (DDoS) sobre servicios públicos disponibles de Internet. Ejemplos de tales servicios incluyen los sitios Web, la telefonía de Internet (VoIP), los servidores de FTP, DNS, etc.

Antecedentes de la invención

En la Internet, los ataques de Denegación Distribuida de Servicio (DDoS) se han convertido hoy en día en una gran amenaza. Grandes redes escaladas de PC infectados (robots o autómatas) combinan su ancho de banda y potencia de computación para sobrecargar un servicio público disponible y denegarlo a los usuarios legales. Todos los servidores públicos son básicamente vulnerables a los ataques de DDoS debido a la estructura abierta de la Internet. Los robots los suelen adquirir automáticamente los hackers que usan herramientas software para escanear a través de la red, detectando vulnerabilidades y explotando la máquina objetivo.

El número de tales incidentes de DDoS está aumentando continuamente. Por ejemplo, los ataques contra grandes sitios de comercio electrónico en febrero de 2000 y los ataques contra los servidores de DNS raíz en 2003 y 2007 han llamado la atención pública al problema de los ataques de DDoS. Hoy en día, se atacan principalmente los sitios web de medio tamaño por delincuentes para extorsionar el dinero de protección de sus propietarios sin atraer demasiado la atención del público. Además de esto, también los Proveedores del Servicio de Internet (ISP) tienen que tratar con el problema de que el tráfico de DDoS está congestionando los anchos de banda de sus enlaces.

El software de los robots también ha evolucionado alarmantemente a lo largo del tiempo. Herramientas primitivas como *TFN, Stacheldraht, Trinoo* o *Mstream* usan estructuras de comunicaciones sin cifrar y organizadas jerárquicamente. La mayor parte de estas herramientas usaban torrentes de TCP-SYN, UDP o ICMP con posibles parámetros identificables. Como algunos de estos ataques se han mitigado satisfactoriamente, ha surgido una nueva generación de robots. *SDBot*, *Agobot* o el *Phatbot* muy mejorado son representantes conocidos que usan IRC como una comunicación robusta y segura. Estas herramientas también contienen procedimientos para difundirse por sí mismos y tienen algoritmos de ataque más sofisticados, que podrían actualizarse sobre la Internet. El tráfico de ataque de estas herramientas parece como el tráfico legal sobre la capa de transporte, lo que le hace casi imposible filtrarlo de forma efectiva con cortafuegos normalizados.

La mitigación de los ataques de DDoS en el origen o dentro del núcleo de la Internet parece que es una tarea imposible debido a la naturaleza distribuida y libre de autorización de la red basada en IP. Enfoques para conseguir este objetivo normalmente descansan en cambiar los protocolos actuales de Internet y por lo tanto no son fácilmente aplicables. El filtrado de entrada como se describe en el documento RFC 2827 (P. Ferguson y D. Senie "Network ingress filtering: Defeating denial of service attanchs which employ IP source address spoofing" Estados Unidos, 2000, disponible en http://rfc.net/rfc2827.html.) también ayuda a mitigar los ataques de DDoS con direcciones fuente de IP falsificadas (suplantación de IP) y se deberían aplicar por cada ISP. Como el filtrado de entrada solo ayuda a otros ISP sobre la Internet y no al que realmente lo está aplicando, llevó un tiempo bastante largo hasta que se estableció en muchos sitios. Además, Savage y otros (S. Savage, D. Wetherall, A. R. Karlin, y T. Aderson, "Practical network support for IP traceback", en SIGCOMM 2000, páginas 295 - 306) Rastreo sugerido de IP para encontrar la fuente de las direcciones de IP suplantadas por marcación probabilística de paquetes. Hoy en día, la suplantación de IP ya no es tan común en los ataques de DDoS, excepto para el último octeto de una dirección de IP.

Un sistema conocido para mitigar los ataques es el DefensePro de Radware con el sistema operativo APSolute (http"//www.radwar.com/Products/ApplicationNetworkSecurity/DefensePro.aspx). De acuerdo con este sistema, los paquetes de IP se examinan en busca de características llamativas comunes, por ejemplo, tamaños de paquetes idénticos, puertos de origen y objetivo, etc. Este sistema funciona bien en el caso de solo un número pequeño de fuentes de ataque, ya que el atacante generalmente genera un número comparativamente alto de peticiones o en el caso de tener paquetes de ataque idénticos.

De este modo, hoy en día hay una fuerte necesidad de mitigar los ataques de DDoS cerca del objetivo, que parece ser la única solución al problema en la infraestructura de Internet actual. El objetivo de tal sistema de protección es limitar su efecto desestabilizante sobre el servidor mediante la identificación de las peticiones maliciosas.

De este modo, los ataques de Denegación Distribuida de Servicio (DDoS) son hoy en día el factor más desestabilizante en la Internet global y hay una fuerte necesidad de soluciones sofisticadas.

Normalmente, los sistemas de ordenadores se protegen por un componente de seguridad, un cortafuegos. La configuración de tales cortafuegos se realiza mediante conjuntos de normas que describen las características de los paquetes entrantes que se permite que pasen el cortafuegos o que se rechazan. Los parámetros para una norma son diversos y dependientes del sistema utilizado. En muchos casos, se indican el protocolo, la puerta objetivo y la

puerta de origen, las direcciones de red objetivo y de origen y la dirección del flujo de los paquetes de datos. En la internet la dirección de la red objetivo y de origen consisten de las direcciones de IP (que es una dirección abstracta del ordenador) y la máscara de red. El rechazo o el permiso de paso a una pluralidad de intervalos no conectados requiere la definición de muchas normas para el cortafuegos. Sin embargo, como no hay ninguna relación directa entre las direcciones de IP y la localización geográfica de un ordenador, es de hecho necesario un gran número de tales normas para definir un país, por ejemplo.

La tecnología relacionada se describe en los documentos US 2006/267802, US 2006/010389 o la Gestión Remota de Tecnología "Bloques de IP de País", 11 de enero de 2008.

Sumario de la invención

La invención comienza de la idea de monitorización de las peticiones reales a un sistema de ordenadores y la prevención de situaciones de sobrecarga sobre la base de la información acerca del origen geográfico de las peticiones con una interfaz gráfica de usuario (GUI).

De acuerdo con un primer aspecto, la invención proporciona un procedimiento de acuerdo con la reivindicación 1 de protección de un sistema de ordenadores de los ataques sobre una red a la que se conecta el sistema de ordenadores, comprendiendo el procedimiento las etapas de (a) monitorización de las peticiones actuales al sistema de ordenadores; (b) medición de una o más características de la red sobre la base de las peticiones actuales; (c) provisión de una interfaz gráfica de usuario que visualiza una o más características medidas de la red para al menos un área geográfica del origen de las peticiones, (d) recibir una entrada de usuario que selecciona al menos un área geográfica; (e) acceder sobre la base del área geográfica, al menos una, seleccionada, a una base de datos que asocia, para la, al menos un área geográfica de origen, cada uno de los países con los intervalos de direcciones de IP correspondientes; y (f) generar automáticamente normas de cortafuegos para el sistema de ordenadores sobre la base de las direcciones de IP recuperadas de la base de datos para el área geográfica, al menos una, seleccionada. La etapa a) preferentemente también comprende acceder a la base de datos sobre la base de las direcciones de IP monitorizadas para recuperar información de las mismas con respecto al país desde el que está viniendo la petición monitorizada.

El procedimiento comprende la etapa adicional g) de filtrar un remitente o las peticiones desde un remitente dependiendo de las normas generadas de cortafuegos para el área geográfica, al menos una, seleccionada. La etapa de filtrar comprende de un algoritmo de estrangulamiento del ancho de banda, en el que el límite para un remitente particular corresponde al área geográfica de origen. De este modo, ciertas peticiones o el remitente no se bloquean completamente. Más bien, el número de peticiones aceptadas o el ancho de banda proporcionado para un remitente o país particular, por ejemplo, se estrangula, es decir algunas peticiones se retrasan o incluso se deniegan. Técnicamente, esto corresponde a una limitación artificial del ancho de banda disponible para este remitente particular poniendo en cola o abandonando paquetes de IP, también conocido como estrangulamiento de ancho de banda, conformación de tráfico o vigilancia.

La suma de todos los límites para todos los remitentes se selecciona sobre la base de la carga del servidor o el uso de ancho de banda del sistema de ordenador.

Las características medidas de la red se seleccionan preferentemente del grupo que comprende: el país de origen, las tasas de paquetes, las características de aplicación, y el volumen de transmisión o combinaciones de las mismas.

La interfaz gráfica de usuario preferentemente comprende un mapa geográfico. De acuerdo con una realización preferida, la interfaz gráfica de usuario proporciona diferentes niveles de mapas geográficos, comprendiendo los niveles un mapa del mudo, mapas continentales, mapas locales, mapas de países individuales, mapas de ciudades. La una o más características medidas de la red para cada una de las áreas geográficas se visualizan por la interfaz gráfica de usuario en diferentes características gráficas. Por ejemplo, la característica gráfica se selecciona a partir del grupo que comprende del color, patrón gráfico, parpadeo o combinaciones de las mismas. El área geográfica se selecciona, por ejemplo, a partir del grupo que comprende el país, provincia, estado, o ciudad.

De acuerdo con la invención, la petición es preferentemente un paquete de IP, un correo electrónico, una petición de DNS, una descarga FTP, una llamada de VoIP o una petición de HTTP.

De acuerdo con un segundo aspecto, la invención proporciona un sistema de acuerdo con la reivindicación 10 para protección de los sistemas de ordenadores de ataques sobre la red a la cual se conecta el sistema de ordenadores.

Breve descripción de los dibujos

Se describe una realización preferida de la invención con más detalle a continuación con referencia a los dibujos adjuntos, que es solo a modo de ejemplo.

la Fig. 1 muestra un diagrama de flujo de datos de acuerdo con una realización preferida de la invención; y
la Fig. 2 muestra un ejemplo para una interfaz gráfica de usuario en la forma de un mapa del mundo.

Descripción detallada

La Fig. 1 muestra un diagrama de flujo de datos de acuerdo a una realización de la invención. Como se muestra en la Fig. 1, el sistema monitoriza el tráfico real de datos y mide las características de la red con respecto a las áreas geográficas, tales como los países. Las características medidas de la red se procesan a continuación para la visualización con la interfaz gráfica de usuario. Un ejemplo de tal interfaz gráfica de usuario se describirá con detalle con referencia al ejemplo mostrado en la Fig. 2. La interfaz gráfica de usuario proporciona al usuario con detalles acerca del tráfico actual de internet y asiste al usuario para identificar los ataques al sistema de ordenadores. Por lo tanto el origen de un ataque (potencial) se puede localizar fácil y rápidamente. Con referencia a la interfaz gráfica de usuario, el usuario del sistema de ordenadores puede seleccionar una o más áreas geográficas que aparecen para representar una amenaza al sistema de ordenadores. Tal selección causa que el sistema acceda a la base de datos que asocia cada una de las áreas geográficas, por ejemplo el país, con las direcciones de IP correspondientes. Sobre la base de esta información obtenida de la base de datos, el sistema genera automáticamente normas para el cortafuegos como una medida protectora frente a los ataques.

De acuerdo con la invención, ciertas peticiones o remitentes o países preferentemente no se bloquean completamente si se determina que son anormales. Más bien, el número de peticiones aceptadas desde un país se reduce / restringe, es decir algunas peticiones del remitente se aceptan y otras se rechazan. Esto corresponde a una limitación artificial o estrangulamiento del ancho de banda disponible para este país particular. El número global de peticiones a rechazar o la cantidad de ancho de banda estrangulado son ajustables a través de la interfaz gráfica de usuario para un administrador de modo que se impide una sobrecarga.

La Fig. 2 muestra un ejemplo de una parte de una interfaz gráfica de usuario en la forma de un mapa del mundo. Con tal interfaz gráfica de usuario, el tráfico de internet actual se puede visualizar fácilmente y rápidamente para asistir a la generación automática de las normas de cortafuegos. Las interfaces gráficas de usuario en la forma de mapas se pueden representar en uno o más niveles. El nivel más alto se representa por un mapa del mundo como se muestra en la Fig. 2. En los niveles inferiores respectivos seleccionables por el usuario se pueden visualizar preferentemente áreas como continentes individuales, países individuales, provincias o estados, o incluso ciudades individuales.

La visualización proporciona al usuario, por ejemplo por medio de diferentes colores, detalles acerca de las características de la red tales como el tráfico de Internet para cada área geográfica, por ejemplo sobre la base de un país. El ejemplo de la Fig. 2 muestra un color oscuro para Rusia que representa un volumen de tráfico anormalmente alto originado desde Rusia, en donde los Estados Unidos están coloreados con un color más brillante representando menos tráfico anormal desde este punto. En lugar de usar diferentes colores, se podrían usar diferentes patrones gráficos para distinguir entre áreas que tienen tráficos diferentes, o las fronteras de países podrían parpadear a diferentes frecuencias para proporcionar tales detalles para cada uno de los países.

El color individual o patrón, por ejemplo, corresponden cada uno en el mapa a un valor de la característica de red medida, tal como el número de peticiones, el volumen de transmisión o el número de atacantes estimado.

De acuerdo con la invención, el sistema espera una entrada de un usuario seleccionando un área geográfica específica, por ejemplo un país específico. Tal selección se puede hacer con un ratón de ordenador o un panel táctil u otro dispositivo de entrada apuntando sobre el país deseado sobre el mapa representado. Tal selección inicia una acción correspondiente en el sistema de cortafuegos del sistema de ordenadores. Por ejemplo, seleccionando un país específico, este país se puede bloquear completamente o al menos se puede limitar el tráfico originado desde el mismo. Por ejemplo se puede iniciar un algoritmo de estrangulamiento de ancho de banda limitando el ancho de banda para el país seleccionado a 10 Mbits/s. Para el ajuste de estos valores de limitación, se usan elementos adicionales de la interfaz gráfica de usuario (no mostrados en la Fig. 2). De este modo, el sistema de ordenadores está aún totalmente disponible para todas las peticiones procedentes de otros países. El usuario de este país particular probablemente no tenga éxito en el acceso al sistema de ordenadores solicitado.

La presente invención se ha descrito con referencia a varias realizaciones de la misma. Será evidente para los expertos en la materia que se pueden efectuar muchos cambios en las realizaciones descritas sin apartarse del alcance de la presente invención. De este modo el alcance de la presente invención no se debería limitar a los procedimientos y sistemas descritos en esta solicitud, sino solo los procedimientos y sistemas descritos por el lenguaje de las reivindicaciones y equivalentes de los mismos.

REIVINDICACIONES

1. Un procedimiento para controlar un sistema de cortafuegos para la protección de un sistema de ordenadores de los ataques sobre la red a la cual está conectado el sistema de ordenadores, comprendiendo el procedimiento las etapas de:

a. monitorizar las peticiones actuales al sistema de ordenadores;
b. medir una o más características de la red sobre la base de las peticiones actuales;
c. proporcionar una interfaz gráfica de usuario que visualice la una o más características de la red medidas para al menos un área geográfica del origen de las peticiones, comprendiendo cada una de dicha, al menos un área geográfica al menos un país;
d. recibir una entrada de usuario seleccionando al menos un área geográfica;
e. acceder, sobre la base de la al menos un área geográfica seleccionada, a una base de datos que asocia, para la, al menos un área geográfica de origen cada uno de los países con las direcciones de IP correspondientes;
f. generar automáticamente normas de cortafuegos para el sistema de ordenadores sobre la base de las direcciones de IP recuperadas de la base de datos para la al menos un área geográfica seleccionada; y
g. filtrar un remitente o las peticiones de un remitente dependiendo de las normas del cortafuegos generadas para la, al menos un área geográfica seleccionada, en donde la etapa de filtrado comprende iniciar un algoritmo de estrangulamiento del ancho de banda que limita el ancho de banda para la, al menos un área geográfica seleccionada, en el que el límite para un remitente particular corresponde al área geográfica de origen, y en el que la suma de todos los límites para todos los remitentes se selecciona en base a la carga del servidor o al uso del ancho de banda del sistema de ordenadores.

2. El procedimiento de la reivindicación 1, en el que la etapa a) preferentemente también comprende el acceso a la base de datos sobre la base de las direcciones de IP monitorizadas para recuperar información de las mismas con respecto al país del que está viniendo la petición monitorizada.

3. El procedimiento de la reivindicación 1, en el que las características medidas de la red se seleccionan del grupo que comprende: el país de origen, las tasas de paquetes, las características de aplicación, el volumen de transmisión, el número estimado de peticiones en un intervalo de tiempo definido, o combinaciones de las mimas.

4. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que en la etapa c) la interfaz gráfica de usuario comprende un mapa geográfico.

5. El procedimiento de la reivindicación 4, en el que la interfaz gráfica de usuario proporciona diferentes niveles de los mapas geográficos, niveles que comprenden el mapa del mundo, mapas continentales, mapas locales, mapas de países individuales y mapas de ciudades.

6. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que la una o más características medidas de la red para cada una de las áreas geográficas se visualizan por medio de la interfaz gráfica de usuario en diferentes características gráficas.

7. El procedimiento de la reivindicación 6, en el que la característica gráfica se selecciona del grupo que comprende: color, patrón gráfico, parpadeo o combinaciones de las mimas.

8. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que una petición es un paquete de IP, un correo electrónico, una petición de DNS, una descarga de FTP, una llamada de VoIP o una petición de HTTP.

9. El procedimiento de cualquiera de las reivindicaciones anteriores, en el que el área geográfica se selecciona del grupo que comprende país, provincia, estado o ciudad.

10. Un sistema para controlar un sistema de cortafuegos para proteger un sistema de ordenadores de ataques sobre una red a la cual se conecta el sistema de ordenadores, comprendiendo el sistema:

medios para monitorizar las peticiones actuales al sistema de ordenadores;
medios para medir una o más características de la red en base a las peticiones actuales;
medios de representación para proporcionar una interfaz gráfica de usuario que visualiza la una o más características medidas de la red para al menos un área geográfica del origen de las peticiones, comprendiendo cada una de dicha al menos un área geográfica al menos un país;
un medio de entrada que recibe una entrada de usuario que selecciona al menos un área geográfica;
una base de datos que asocia, para la al menos un área geográfica de origen, cada uno de los países con las direcciones de IP correspondientes;
medios para la generación automática de normas de cortafuegos para el sistema de ordenadores sobre la base de las direcciones de IP recuperadas de la base de datos para la al menos un área geográfica seleccionada; y
un filtro para filtrar un remitente o las peticiones de un remitente dependiendo de las normas de cortafuegos generadas para la al menos un área geográfica seleccionada, en donde el filtro comprende un algoritmo de estrangulamiento del ancho de banda que limita el ancho de banda para la al menos un área geográfica

seleccionada, en donde el límite para un remitente particular corresponde al área geográfica de origen, y en donde la suma de todos los límites para todos los remitentes se selecciona en base a la carga del servidor o al uso de ancho de banda del sistema de ordenadores.

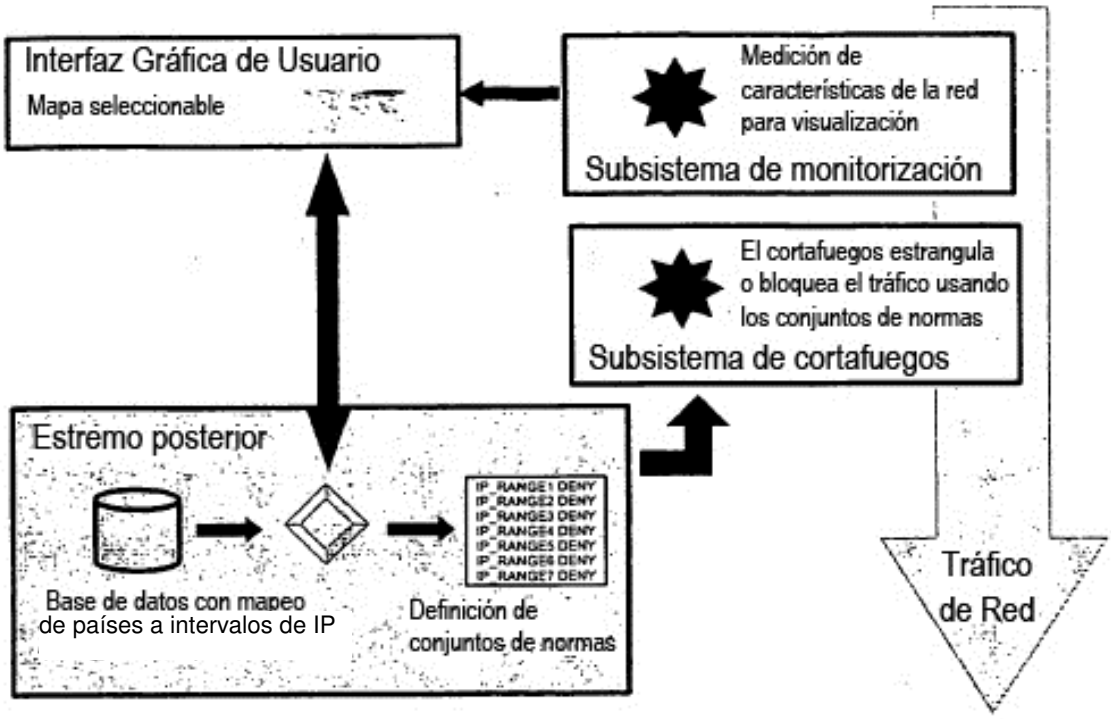
Interfaz Gráfica de Usuario
Mapa seleccionable
Medición de características de la red para visualización
Subsistema de monitorización
El cortafuegos estrangula o bloquea el tráfico usando los conjuntos de normas
Subsistema de cortafuegos
Estremo posterior
IP_RANGE1 DENY
IP_RANGE2 DENY
IP_RANGE3 DENY
IP_RANGE4 DENY
IP_RANGE5 DENY
IP_RANGE6 DENY
IP_RANGE7 DENY
Base de datos con mapeo de países a intervalos de IP
Definición de conjuntos de normas
Tráfico de Red

Fig. 1

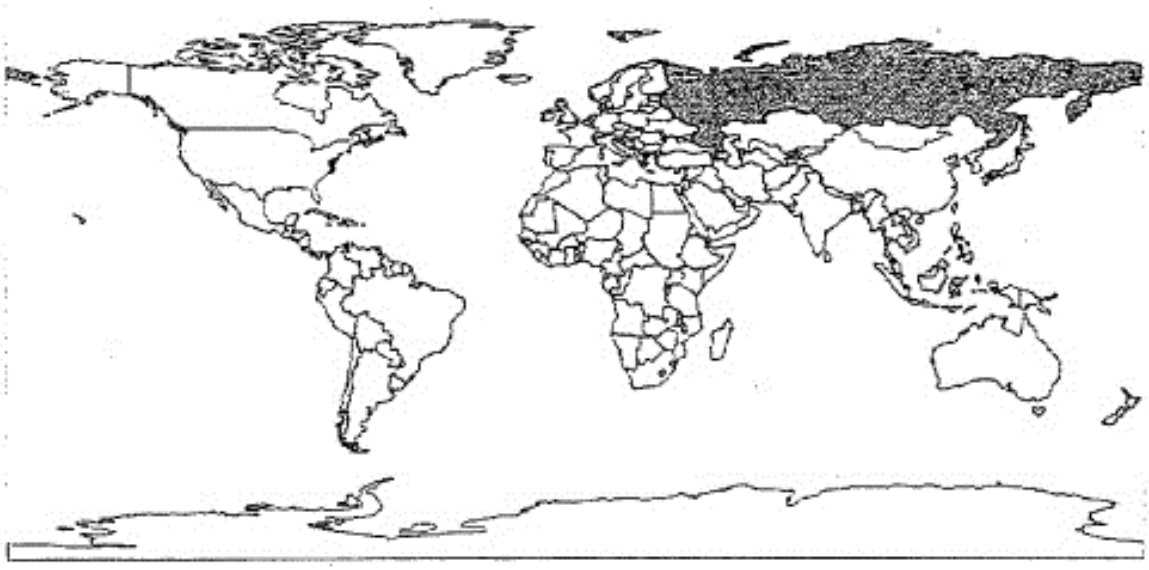

Fig. 2