SLOVENSKÁ REPUBLIKA

(19) **SK**

ÚRAD
PRIEMYSELNÉHO
VLASTNÍCTVA
SLOVENSKEJ REPUBLIKY

ZVEREJNENÁ PRIHLÁŠKA VYNÁLEZU

(11), (21) Číslo dokumentu:

2023-2000

(22) Dátum podania prihlášky: **2. 7. 1999**

(31) Číslo prioritnej prihlášky: **9802415-1**

(32) Dátum podania prioritnej prihlášky: **2. 7. 1998**

(33) Krajina alebo regionálna organizácia priority: **SE**

(40) Dátum zverejnenia prihlášky: **11. 9. 2001**
Vestník ÚPV SR č.: **09/2001**

(62) Číslo pôvodnej prihlášky v prípade vylúčenej prihlášky:

(86) Číslo podania medzinárodnej prihlášky podľa PCT: **PCT/SE99/01202**

(87) Číslo zverejnenia medzinárodnej prihlášky podľa PCT: **WO00/02114**

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7] :

G06F 1/00,
G06F 13/00,
H04L 9/00,
H04L 29/06,
H04L 12/56,
G06F 9/46

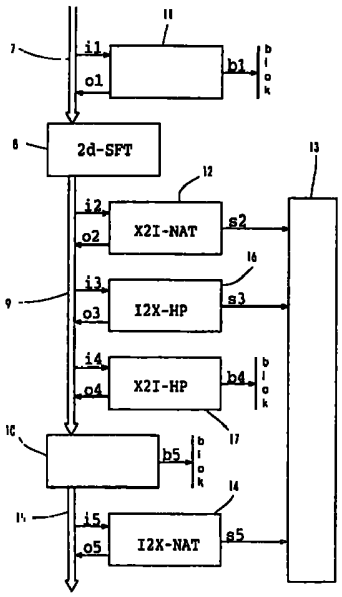
(71) Prihlasovateľ: **EFFNET GROUP AB, Bromma, SE;**

(72) Pôvodca: **Sundström Mikael, Lulea, SE;**
Johansson Olof, Newark, DE, US;
Lindholm Joel, Lulea, SE;
Brodnik Andrej, Ljubljana, SI;
Carlsson Svante, Lulea, SE;

(74) Zástupca: **Majlingová Marta, Ing., Bratislava, SK;**

(54) Názov: **Ochranná stena na riadenie sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami a spôsob jej riadenia**

(57) Anotácia:
Ochranná stena (3) na riadenie sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami (1, 5, 4), zahŕňajúca filtračné prostriedky vyberajúce z celého súboru pravidiel v závislosti od obsahu údajových polí údajového paketu, ktorý sa prenáša medzi uvedenými sieťami, pravidlo aplikovateľné na uvedený údajový paket, aby sa uvedený paket zablokoval alebo aby sa uvedený paket odoslal cez ochrannú stenu (3). Prostriedky (8) na 2-rozmerné vyhľadávanie adries uskutočňujú 2-rozmerné vyhľadávanie zdrojových adries a adries miesta určenia paketu v súbore adresových prefixov, pričom každý prefix má podsúbor pravidiel z celého súboru pravidiel, aby sa našiel prefix prostredníctvom svojej reprezentácie, priradený uvedeným zdrojovým adresám a adresám miesta určenia, a prostriedky (10) na hľadanie zhody s pravidlami na nájdenie zhody s pravidlami na základe obsahu uvedených údajových polí, aby sa našlo pravidlo aplikovateľné na údajový paket.



SK 2023-2000 A3

PV2023-2000
09.04.01

Ochranná stena na riadenie sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami a spôsob jej riadenia

Oblasť techniky

Vynález sa týka vo všeobecnosti aparátu ochrannej steny a spôsobu riadenia sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami a konkrétnejšie ochranného zariadenia, zahrnujúceho filtračné prostriedky na výber pravidla, aplikovateľného na údajový paket, z úplného súboru pravidiel v závislosti od obsahu údajových polí údajového paketu, ktorý sa má preniesť medzi uvedenými sieťami, aby sa uvedený paket zablokoval alebo preniesol cez ochrannú stenu, a príslušného spôsobu.

Doterajší stav techniky

Dôležitým problémom pre väčšinu na Internet napojených organizácií je bezpečnosť a v dôsledku toho sa ochranné steny stávajú dôležitou súčasťou väčšiny stratégií bezpečnosti počítačov a sietí vo väčšine organizácií. Užívatelia, ktorí majú prístup k sieťovému serveru alebo iným verejným službám organizácie, nesmú byť schopní získať prístup k vnútorným službám, ako sú účtovné systémy, Intranetové informačné servery a iné možné informácie, citlivé pre túto spoločnosť. Služby systémov sa nesmú prerušiť – servery a pracovné stanice musia byť chránené proti príznakom odopretia-služby (DOS) od užívateľov na Internete.

Ochranná stena alebo filtračný smerovač je zariadenie, ktoré pracuje v zásade rovnakým spôsobom ako smerovač. To znamená, že prijíma pakety na vstupnom rozhraní, preskúma adresy miesta určenia paketov a odošle paket na správne (vzhľadom na adresu miesta určenia) výstupné rozhranie. Avšak ochranná stena uskutoční oveľa starostlivejšiu kontrolu každého paketu. Zdrojová adresa a adresa miesta určenia, zdrojový port a port miesta určenia, pole protokolu, indikátory a voľby sa tiež kontrolujú a porovnávajú sa so zoznamom pravidiel ochrannej steny. V závislosti od toho, ktoré pravidlo zodpovedá paketu, by ochranná

stena mohla rozhodnúť neodoslať paket, napríklad ak mu zodpovedá blokovacie pravidlo.

Okrem neoprávneného prístupu existujú iné hrozby, ktoré vznikajú, keď je organizácia pripojená na Internet. Najnižšou úrovňou je to, že sa údajom, prijatým z neznámych zdrojov, nedá veriť. Hľadanie vírusov a trójskych koňov v elektronickej pošte a na webovských (sieťových) stránkach je povinnosťou, ktorú vykonávajú niektoré ochranné steny doterajšieho stavu techniky.

Ďalej, ako sa zväčšuje šírka pásma siete, výkon ochranných stien sa stáva vážnym problémom.

Ochranné steny môžu pracovať na mnohých odlišných úrovniach a poskytujú odlišné typy pôsobenia pri skenovaní údajov, ktoré nimi prechádzajú. Avšak základnou úlohou všetkých ochranných stien je zaviesť filtrovanie na základe obsahu hlavičiek sieťových (IP = Internet Protocol (Internetový protokol)) a transportných (UDP = User Datagram Protocol (protokol užívateľských datagramov)), TCP = Transmission Control Protocol (protokol riadenia prenosu)) úrovní. Bez takéhoto IP filtrovania by všetko ďalšie pôsobenie, ako je skenovanie údajov, bolo zbytočné, to znamená, že užívatelia na vnútornej sieti by mohli tiež nakonfigurovať svoje sieťové aplikácie tak, aby pri napojení na vzdialené servery neprechádzali cez skener a teda obišli všetky bezpečnostné opatrenia.

Spoločnosti alebo organizácie sú napojené na Internet z rozličných príčin, napríklad aby zverejnili informácie o spoločnosti, jej výrobkoch a službách na sieti, aby získali prístup k informáciám, dostupným na Internete, a aby korešpondovali cez elektronickú poštu.

Spoločnosť má často vnútorné informácie, ku ktorým sa užívatelia Internetu nesmú dostať, ako sú Intranetové informačné servery, súborové servery atď. Najčastejšie používanou konfiguráciou je umožniť spojenie z Internetu na súbor serverov (sieť, elektronická pošta a iné verejné služby), ale zabrániť prístupu k iným hostiteľom (napríklad Intranetové servery). Aby sa toto dosiahlo, vytvorí sa „demilitarizovaná zóna“ (DMZ). Pripojenia k počítačom v DMZ sa dajú uskutočňovať tak z Internetu, ako aj z Intranetu, ale prístup k Intranetu z Internetu je obmedzený. V sieťach v doterajšom stave techniky sa vnútorná sieť, ako je Intranet, spojí s demilitarizovanou zónou cez ochrannú stenu a DMZ sa spojí s Internetom cez

smerovač. V dôsledku toho môže sieťová prevádzka voľne prechádzať medzi Internetom a DMZ, čo vôbec nie je chránené pred užívateľmi na Intranete. Dôvodom pre to je, že ochranné steny v doterajšom stave techniky tiež nemajú možnosť spojiť viac než dve siete – jednu vnútornú a jednu vonkajšiu sieť.

Iné ochranné steny majú tri sieťové rozhrania. Tu sa dajú urobiť obmedzenia, ktoré sa týkajú prevádzky tak medzi Internetom a DMZ, ako aj Intranetom. Niektoré obmedzenia sú urobené pre prevádzku ku a od hostiteľov v DMZ, napríklad sieťový server potrebuje len byť dostupný na HTTP (Hypertext Transfer Protocol (protokol prenosu hypertextu)) porte. Užívatelia Internetu by nemali byť schopní pripojiť sa k žiadnym iným službám. Avšak užívatelia na Intranete by mohli chcieť mať prístup na sieťový server viacerými spôsobmi než užívatelia Internetu z administratívnych dôvodov, teda medzi týmito dvoma sieťami by mal byť povolený širší prístup. Podobné pravidlá sú potrebné pre server elektronickej pošty; SMTP (Simple Mail Transfer Protocol (protokol jednoduchého prenosu pošty)) spojenia by mali byť povolené z Internetu, ale čítanie elektronickej pošty by malo byť možné len pre určitých povolených hostiteľov na Intranete a podľa možnosti tiež z niektorého hostiteľa na Internete.

V prostredí ochrannej steny je počet strojov v DMZ napríklad 30. Pravidlá pre stroje v DMZ môžu byť odlišné pre každý stroj, ale počet pravidiel na jeden stroj je pomerne malý, napríklad 10 až 15. Viac pravidiel by sa mohlo použiť pre prevádzku z Intranetu do DMZ, ale tieto budú pravdepodobne všeobecnejšie. Teda pre všetky stroje v DMZ platí značne nízky počet pravidiel.

Ďalej, pravidiel, ktoré sa týkajú prevádzky medzi Internetom a Intranetom(mi), je vo väčšine prípadov len niekoľko, ak vôbec nejaké sú. Väčšina prevádzky by mala byť zablokovaná. Avšak prevádzka, ktorá sa iniciovala z Intranetu, by mala byť povolená.

Tak ako počet užívateľov Internetu rastie, verejné servery budú navštevované častejšie, čo spôsobí väčšiu prevádzku. Prevádzka ku a z Intranetu rastie, ako užívatelia Intranetu využívajú zväčšujúce sa množstvo informácií, dostupných na Internete. V dôsledku toho sa zvyšujú nároky na šírku pásma. To kladie zvýšené požiadavky na výkon použitých ochranných stien.

Teda hlavnou úlohou ochrannej steny je filtrovať pakety, t. j. pre daný IP paket a súbor pravidiel určovať, ktoré pravidlo by sa malo na tento paket aplikovať. Ak tomu istému paketu zodpovedá niekoľko pravidiel, musia byť definované zásady, ktoré špecifikujú, ktoré pravidlo sa má vybrať. Pre tento problém sú v doterajšom stave techniky známe dve riešenia. Jedným riešením je vybrať pravidlo, ktoré zodpovedá najväčšiemu počtu polí paketu, a ak dve pravidlá zodpovedajú rovnakému počtu polí, ale odlišných, musí sa medzi nimi špecifikovať poradie. Toto sa používa v algoritme na klasifikáciu paketov autorov Borga a Flodina v Borg, N. Flodin, Malin, packet classification (Malin, klasifikácia paketov), jún 1997; Borg N., A Packet Classifier for IP Networks (Klasifikátor paketov pre IP siete), Masters Lic., Luleå University of Technology, február 1998. Iným riešením je definovať poradie medzi pravidlami a použiť toto poradie na definovanie, ktoré pravidlo vybrať. Výhodou druhého riešenia je to, že poskytuje väčšiu flexibilitu pri definovaní pravidiel filtrovania a túto metódu využíva kód NetBSD ochrannej steny, opísaný v sieťovom mieste www.netbsd.org.

Pravidlo filtrovania zahrnuje súbor kritérií, ktoré musia byť splnené, a činnosť, ktorá sa má vykonať, ak sú splnené. Tieto kritériá sa zakladajú na IP zdrojových adresách a adresách miesta určenia (32-bitové prefixy), poli IP protokolu (8-bitové celé číslo) bez ohľadu na to, či má paket nastavené IP voľby a aké tieto voľby sú (celé čísla) na základe čísel IP/TCP zdrojových portov a portov miesta určenia (2 16-bitové celočíselné rozsahy), na indikátoroch TCP hlavičiek (3 bity), type hlavičky a kódových poliach ICMP (2 8-bitové celé čísla), na tom, z akého rozhrania bol paket načítaný (8 + 8 bitov) a k akému rozhraniu sa má paket odoslať (8 + 8 bitov).

Väčšina dnešných ochranných stien sa zvlášť nezaoberá problémom zhody s pravidlami. Je bežné, že je k dispozícii pripojený zoznam (alebo pole) pravidiel a paket sa porovnáva s každým z nich, kým sa nenájde zhoda. To však nie je efektívne. Iným prístupom je transformácia (kľúčovanie) pravidiel. Ako metódu rozlíšenia nejednoznačností medzi pravidlami, t. j. ak dve pravidlá zodpovedajú tomu istému paketu, väčšina implementácií rieši tento problém definovaním prvého alebo posledného zodpovedajúceho pravidla ako toho, podľa ktorého sa treba riadiť.

Jedna z ochranných stien v doterajšom stave techniky, PIX ochranná stena firmy Cisco Systems, opísaná v sieťovom mieste www.cisco.com, je na spojenie

orientovaným bezpečnostným zariadením, ktoré chráni vnútornú sieť pred vonkajšou sieťou. PIX ochranná stena je veľmi drahým zariadením a má horné obmedzenie asi 16 000 súčasných spojení. Hlavnou časťou PIX ochrannej steny je ochranná schéma, zakladajúca sa na adaptívnom bezpečnostnom algoritme (ASA), ktorý poskytuje bezpečnosť, orientovanú na spojenie pri úplne definovanom stave. ASA sleduje adresu zdroja a miesta určenia, TCP sekvenčné čísla, čísla portov a ďalšie TCP indikátory každého paketu. Táto informácia sa zapamätá do tabuľky a všetky prichádzajúce a odchádzajúce pakety sa porovnávajú so vstupmi v tabuľke. Preto musí byť informácia o každom nadviazanom spojení zapamätaná počas existencie spojenia, a teda počet možných spojení je definovaný dostupnou kapacitou pamäte. Plne obsadená Cisco PIX ochranná stena môže pracovať s asi 90 Mbit/s. Avšak Cisco PIX ochranná stena tiež podporuje prevádzanie adries portov (PAT), v dôsledku čoho sa môže obslúžiť viac než 64 000 vnútorných hostiteľov s jedinou vonkajšou IP adresou.

Zahrnutý je paketový filter doterajšieho stavu techniky, nazývaný ipf (IP filter), so štandardnou distribúciou netBSD 1.3.

Súbory pravidiel v ipf sú rozložené na rozhrania, na ktorých platia. Ďalej sa tieto pravidlá kontrolujú dvakrát, prvý raz, keď paket vstupuje do hostiteľa a druhý raz, keď paket hostiteľa opúšťa. Pravidlá, ktoré platia len pre prichádzajúce pakety, sa nepridajú do zoznamu pravidiel, kontrolovaných vo výstupnom porte a naopak. Štruktúrou údajov je v zásade optimalizovaný pripojený zoznam.

Exokernel v Engler D., Kaashoek M. F., O' Tool Jr. J., Exokernel: An operating system architecture..., Proceedings of the 15th ACM symposium on Operating Systems principles, december 1995, používa odlišný prístup k zvládnutiu demultiplexovania paketov, nazývaný DPF, Angler D., Kaashoek M. F.: Fast, flexible message demultiplexing..., Engler D., Kaashoek M. F., Computer Communication Review 26(4), október 1996. Pravidlá sa napíšu v špeciálnom programovacom jazyku a potom sa kompilujú. Kompilátor pozná všetky špecifikované pravidlá a generované kódy sa dajú optimalizovať pre očakávané prevádzkové situácie.

Cieľom tohto vynálezu je poskytnúť zlepšené zariadenie ochrannej steny a spôsob riadenia sieťovej prevádzky medzi vnútornými a vonkajšími sieťami zabezpečením efektívneho vyhľadávania adries a procesu vyhľadávania zhody

pravidiel, aby sa dosiahlo efektívne a rýchle filtrovanie IP paketov a neobmedzený počet spojení cez ochrannú stenu.

Podstata vynálezu

Cieľ vynálezu sa uskutoční ochrannou stenou a spôsobom podľa tohto vynálezu, kde sa súbor pravidiel, ktoré sa musia prehľadávať sekvenčne, zmenší segmentovaním súboru pravidiel.

Podstatou vynálezu je preto ochranná stena, ktorá zahrnuje prostriedky na 2-rozmerné vyhľadávanie adries, ktoré vykonávajú dvojstupňové vyhľadávanie, najprv zdrojových adries a adries miesta určenia paketu v súbore adresových prefixov. Každý prefix sa priradí k podsúboru pravidiel z celého súboru pravidiel. Na výslednom podsúbore sa uskutoční lineárne vyhľadávanie, aby sa našlo pravidlo, aplikovateľné na aktuálny údajový paket.

Ďalej vynález poskytuje fragmentovací stroj, umožňujúci filtrovať všetky fragmenty vo fragmentovanom pakete.

Ďalej vynález poskytuej prostriedky na prevádzanie sieťových adries, ktoré prevádzajú vnútorné zdrojové adresy na vonkajšie zdrojové adresy paketu, prenášaného z ochrannej steny, alebo vonkajšie zdrojové adresy na vnútorné zdrojové adresy paketu, prenášaného do ochrannej steny.

Ďalej vynález poskytuje prostriedky na prevádzanie sieťových adries, ktoré prevádzajú vnútorné zdrojové adresy na vonkajšie zdrojové adresy paketu, prenášaného z vnútornej siete do vonkajšej siete, alebo vonkajšie zdrojové adresy na vnútorné zdrojové adresy paketu, prenášaného z vonkajšej siete do vnútornej siete.

Ďalej vynález poskytuje dierovacie prostriedky, vykonávajúce dočasnú výnimku z vonkajšieho-do-vnútorného blokovacieho pravidla na spojenie, iniciované z vnútornej siete, kde sa vytvorí spätný kanál cez ochrannú stenu pre pakety, prenášané z vonkajšej siete do vnútornej siete.

Ďalej vynález poskytuje ochrannú stenu, schopnú spracovať prinajmenšom 1000 rozličných pravidiel.

Výhodou ochrannej steny a spôsobu jej uskutočnenia podľa tohto vynálezu sú neobmedzený počet možných súčasných spojení, rýchle IP filtrovanie a veľký počet podporovaných možných pravidiel.

Ochranná stena podľa tohto vynálezu poskytuje ochrannú stenu, zahrnujúcu smerovač.

Aby sme podrobnejšie vysvetlili vynález a výhody a znaky vynálezu, v ďalšom podrobne opíšeme výhodné uskutočnenia, pričom budeme odkazovať na priložené obrázky.

Prehľad obrázkov na výkresoch

Obr. 1 znázorňuje topológiu bežnej siete, zahrnujúcej ochrannú stenu podľa tohto vynálezu,

Obr. 2 je bloková schéma ochrannej steny podľa tohto vynálezu,

Obr. 3 je ilustratívny pohľad na oddiel dvojrozmerného hustého zväzku,

Obr. 4 je ilustratívny pohľad na údajovú štruktúru podľa tohto vynálezu,

Obr. 5 je ilustratívny pohľad na diel triedy (0,0),

Obr. 6 je ilustratívny pohľad na diel triedy (1,1),

Obr. 7 je ilustratívny pohľad na diel triedy (1,2),

Obr. 8 je ilustratívny pohľad na diel triedy (2,1),

Obr. 9 je ilustratívny pohľad na diel triedy (1,3+),

Obr. 10 je ilustratívny pohľad na diel triedy (3+,1),

Obr. 11 je ilustratívny pohľad na diel triedy (2+,2+),

Obr. 12 znázorňuje príklad neúspešného hľadania pre konkrétny dopytový kľúč v Patricia strome, obsahujúcom šesť kľúčov, a

Obr. 13 znázorňuje Patricia strom, ktorý je výsledkom vloženia dopytového kľúča z neúspešného hľadania podľa obr. 12.

Príklady uskutočnenia vynálezu

Príklad topológie modernej siete z hľadiska spoločnosti alebo organizácie je znázornený na obr. 1. Vnútorná sieť 1, ako je Intranet, zahrnuje niekoľko sieťových

uzlov 2, ako sú osobné počítače (PC), pracovné stanice, súborové servery atď., ktoré sú pripojené k ochrannej stene 3. Spoločnosti alebo organizácie, ktoré sú pripojené k vonkajšej sieti 4 (Internet), chcú zverejniť informácie, týkajúce sa spoločnosti, na sieti, mať prístup k informáciám, zverejneným inými spoločnosťami alebo organizáciami na Internete, a korešpondovať prostredníctvom elektronickej pošty. Avšak spoločnosť môže mať vnútorné informácie, ku ktorým užívatelia na Internete nemajú povolený prístup, napríklad informácie, dostupné cez Intranetové informačné servery, súborové servery atď. Teda aby sa užívateľom Internetu umožnil prístup k verejným informáciám, povolí sa im pripojiť sa k obmedzenému súboru serverov, napríklad na sieť, elektronickú poštu atď., a zabráni sa im v prístupe k informáciám na iných hostiteľoch, ako sú Intranetové servery. Verejné servery sú dostupné v „demilitarizovanej zóne" (DMZ) 5, ktorá je pripojená k ochrannej stene 3. Ďalej, ochranná stena 3 je pripojená k Internetu cez smerovač 6, a preto sa spojenia s uzlami v DMZ 5 môžu uskutočňovať z vonkajšej siete alebo Internetu 4, ako aj z Intranetu 1, ale prístupy k Intranetu 1 z Internetu 4 sú obmedzené.

V nasledujúcom opise sú podrobne uvedené početné špecifické detaily, aby sa poskytol dôkladnejší opis tohto vynálezu. Pre odborníkov v tejto oblasti bude zrejmé, že tento vynález sa môže realizovať bez týchto špecifických detailov. Niektoré dobre známe znaky nie sú opísané podrobne, aby sa tento vynález nestal neprehľadným.

Jedno uskutočnenie ochrannej steny a rozličných modulov v rýchlej dráhe a to, ako filtrované pakety po nej prúdia podľa tohto vynálezu, je znázornené na obr. 2.

V jednoduchom prípade sa paket prijme zo siete 1, 4 alebo 5 vo vstupnom vedení 7 ochrannej steny a zavedie sa na vstup prostriedkov na vyhľadávanie 2-rozmerných adries alebo 2d-SFT blok 8. Medzivedenie 9 spája 2d-SFT s prostriedkami (blokom) 10 na hľadanie zhody s pravidlami, kde sa paket buď prepustí (ďalej) alebo sa zablokuje b5. Avšak aby ochranná stena podľa tohto vynálezu pracovala správne, má viaceré prídavné moduly.

V tomto uskutočnení sa vyhľadávanie zdrojových adries a adries miesta určenia uskutočňuje v 2d-SFT bloku 8, čo vedie k jednému pravidlu alebo ku

krátkemu zoznamu pravidiel. Zoznam pravidiel zostane v bloku 10 na hľadanie zhody s pravidlami, kým sa tento zoznam neprehľadá a nenájde sa zodpovedajúce pravidlo. Naviac 2d-SFT vyhľadávanie vygeneruje informáciu, či paket bude prípadne potrebovať spracovanie inými modulmi alebo nie. Niektoré z týchto rozhodnutí sa prijmú počas hľadania zhody s pravidlami, čo znamená, že hľadanie zhody s pravidlami začne fakticky pred vstupom do bloku 10, ako je znázornené na obr. 2. 2d-SFT blok 8 je podrobne opísaný ďalej.

Ak je paket príliš veľký na to, aby sa odoslal po linke, fragmentuje sa. To znamená, že všetko, čo nasleduje po IP hlavičke, sa rozdelí na časti (fragmenty) a každý fragment sa vybaví svojou vlastnou IP hlavičkou. V každom fragmente sa nastaví prídavný indikátor fragmentu a ofset fragmentu, aby sa indikovalo, či ide o posledný fragment alebo nie, a zaznamenalo, kam patria údaje z fragmentu do pôvodného (nefragmentovaného) paketu.

Keď je paket fragmentovaný, len prvý fragment, hlavička fragmentu, obsahuje transportnú hlavičku (TCP, UDP alebo ICMP hlavičku). To znamená, že pre nasledujúce fragmenty sa nedá určiť zhoda s pravidlom, ktoré napríklad zahrnuje porty.

Podľa tohto vynálezu fragmentovací stroj 11 zberá fragmenty z každého fragmentovaného paketu, kým sa neprijme hlavička fragmentu (fragmenty nemusia nevyhnutne prísť v správnom poradí). Potom sa časti informácie, ktoré sú prítomné len v hlavičke fragmentu, zapamätajú v zázname, priradenom fragmentovanému paketu, a pozberané fragmenty sa privedú k výstupu o1, pripojenému k vedeniu 7, najprv s hlavičkou fragmentu. Každý fragment, ktorý sa prenesie z fragmentovacieho stroja, sa vybaví informáciou o hlavičke fragmentu, takže sa dá spracovať filtrom, ako keby to bol nefragmentovaný paket. Prídavný indikátor fragmentu a ofset fragmentu sa skontrolujú, aby sa zistilo, či je paket privedený na vstup i1 – pripojený k vedeniu 7 – fragmentovacieho stroja 11 alebo nie.

Keď boli všetky fragmenty fragmentovaného paketu prijaté do fragmentovacieho stroja 11, záznam pre paket sa odstráni.

V určitých bodoch by fragmentovací stroj tiež mohol rozhodnúť zablokovať fragmenty. To sa stane vtedy, keď prídu porušené fragmentované pakety (prípadne ako výsledok napadnutia), ak počet pozberaných fragmentov prekračuje určitý limit,

alebo jednoducho ako výsledok pozberania odpadu (staré vstupy sa odstránia, aby urobili miesto novým).

Network Address Translation (Prevádzanie sieťových adries) (NAT) sa bežne používa, keď má spoločnosť sieť s mnohými vnútornými IP adresami a len niekoľko vonkajších (reálnych) IP adries. Niektoré časti IP adresového priestoru sú rezervované pre vnútorné adresy, ako sú 10.*.*.*, 192.168.*.* a 172.16.*.*. Tieto adresy sa môžu voľne používať na vnútorných/privátnych sieťach. Nikdy však nesmú byť viditeľné na vonkajšej strane. Preto sa nastaví ochranná stena, aby previedla vnútorné zdrojové adresy na vonkajšie zdrojové adresy, keď paket prechádza z vnútornej do vonkajšej siete. Pre pakety, ktoré prechádzajú v druhom smere, sa vonkajšia adresa miesta určenia prevedie na vnútornú adresu, keď paket prechádza cez ochrannú stenu. Aby sa mnoho vnútorných adries zmapovalo na niekoľko vonkajších adries, používajú sa tiež porty.

Napríklad sa ochranná stena nastaví na mapovanie vnútorných adries od 10.1.0.0 po 10.1.255.255 (2^{16} adries) na vonkajšie adresy 194.22.187.0 až 194.22.187.255 (2^8 adries) s použitím portov 20000 až 20255 (2^8 portov).

Keď sa spojenie iniciuje z 10.1.1.1 port 4000 k 130.240.64.46 port 6000, adresa a a port p sa vyberú z rozsahu adries a portov tak, aby (a, p) nekolidovalo s iným NAT spojením. Potom pre každý odchádzajúci, vnútorný do vonkajšieho (I2X), paket z tohto spojenia sa zdrojová adresa 10.1.1.1 a port 4000 nahradia a a p. Pre každý prichádzajúci, vonkajší do vnútorného (X2I), paket sa adresa a miesta určenia a port p nahradia 10.1.1.1 a 4000.

Týmto spôsobom môže 256 vonkajších adries spolu s 256 portami reprezentovať 65 536 adries vnútornej siete.

Ako výsledok 2d-SFT vyhľadávania sa tiež získa informácia o tom, či sa paket podrobil prevádzaniu vnútornej adresy na vonkajšiu, a paket sa privedie na vstup i2 X2I-NAT bloku 12, ktorý vykonáva prevádzanie vonkajšej adresy na vnútornú adresu. Preto sa indikátor na vykonanie X2I-NAT vyhľadávania odstráni na všetkých paketoch, ktoré nevyžadujú prevádzanie. Pre pakety, u ktorých sa uskutoční X2I-NAT vyhľadávanie, sa tieto v prípade zlyhania odošlú do prostriedkov 13 pomalej dráhy cez jeho výstup s2 pomalej dráhy, pretože tu sa spracúvajú aktualizácie NAT údajovej štruktúry. Ak sa uskutoční úspešné X2I-NAT

vyhľadávanie, adresy a porty sa zmenia a výsledky hľadania zhody s pravidlami sa vytiahnu predtým, než sa paket odošle do nasledujúceho filtračného kroku cez jeho výstup o2.

Tiež ako výsledok 2d-SFT vyhľadávania alebo X2I-NAT vyhľadávania je jasné, či sa paket podrobil prevádzaniu vnútornej na vonkajšiu (I2X) adresu. To sa uskutoční v zásade rovnakým spôsobom ako X2I-NAT, ale uskutoční sa ako posledný krok filtrovania. Paket, ktorý sa podrobil prevádzaniu vnútornej adresy na vonkajšiu (I2X), prijatý z výstupného vedenia 15 bloku 10 na hľadanie zhody s pravidlami, sa privedie na vstup i5 I2X-NAT bloku 14, ktorý vykonáva prevádzanie vnútornej adresy na vonkajšiu adresu. Pakety, pre ktoré sa vykoná I2X-NAT vyhľadávanie, sa v prípade zlyhania odošlú do prostriedkov 13 pomalej dráhy cez jeho výstup s5 pomalej dráhy, pretože tu sa spracúvajú aktualizácie NAT údajovej štruktúry. Ak sa uskutoční úspešné X2I-NAT vyhľadávanie, adresy a porty sa zmenia a paket sa prenesie do príslušnej siete cez jeho výstup o2 a výstupné vedenie 15.

Dôvodom pre to, že X2I-NAT je prvým krokom po 2d-SFT vyhľadávaní a I2X-NAT je posledným krokom, je to, že filtračné pravidlá sú stanovené vzhľadom na vnútorné adresy, ktoré sú fixné, a nie NAT adresy, ktoré sa priraďujú dynamicky.

Obyčajne sa väčšina prevádzky, ktorá prechádza z vonkajšej siete 4 do vnútornej siete 1, zablokuje, aby sa chránila vnútorná sieť. Avšak hostitelia na vnútornej sieti majú obyčajne povolený prístup k hostiteľom na vonkajšej sieti 4. Aby sa prijala akákoľvek spätná prevádzka z vonkajšej siete, musí sa urobiť dočasná výnimka z vonkajšie-do-vnútorného blokovacieho pravidla pre spojenia, ktoré boli iniciované z vnútornej siete. Na toto sa odkazuje ako na dierovanie (HP), t. j. pre návrat paketov sa cez ochrannú stenu vyrazí diera. Táto diera existuje len počas existencie spojenia a týka sa len paketov z tohto spojenia.

Dierovanie tiež sleduje TCP sekvenčné čísla, aby sa dierované spojenia chránili pred napadnutím. Preto je nevyhnutné vykonať HP vyhľadávanie tak na odchádzajúcich (I2X) paketoch, ktoré vykonáva I2X-HP blok 16, ako aj na prichádzajúcich (X2I) paketoch, ktoré vykonáva X2I-HP blok 17.

Ako výsledok 2d-SFT vyhľadávania alebo X2I-NAT vyhľadávania vieme, či bol paket podrobený dierovaniu vnútorné na vonkajšie (I2X) alebo vonkajšie na

vnútorné (X2I). To znamená, že sa môžeme vyhnúť dodatočným nárokom na vykonanie HP vyhľadávaní pri paketoch, ktoré sa nemôžu podrobiť dierovaniu. Odchádzajúci paket, ktorý sa podrobil dierovaniu, sa privedie k vstupu i3 I2X-HP bloku 16, pričom sa vyhľadajú zdrojové adresy a porty, adresy a porty miesta určenia a protokol, aby sa zistil existujúci stav. Ak takýto stav neexistuje, paket sa odošle do prostriedkov 13 pomalej dráhy cez jeho výstup s3 pomalej dráhy, kde sa HP údajová štruktúra aktualizuje a stav sa vytvorí. Ak sa zistí zodpovedajúci stav, TCP sekvenčné čísla atď. sa aktualizujú predtým, než sa paket odošle k nasledujúcemu kroku filtrovania cez iný výstup o3.

X2I-HP sa vykoná tým istým spôsobom. Prichádzajúci paket, ktorý sa podrobil dierovaniu, sa privedie k vstupu i4 X2I-HP bloku 17, pričom sa vyhľadajú zdrojové adresy a porty, adresy a porty miesta určenia a protokol, aby sa zistil existujúci stav. Ak takýto stav neexistuje, vykonal sa pokus odoslať paket cez neexistujúcu dieru v blokovacom pravidle a paket sa zablokuje na jeho výstupe b4. Ak sa zistí zodpovedajúci stav, aktualizuje sa predtým, než sa paket odošle k nasledujúcemu kroku filtrovania cez iný výstup o4.

Opäť odkazujúc na 2d-SFT blok 8, v závislosti od obsahu údajových polí údajového paketu, prenášaného medzi uvedenými sieťami, sa pravidlo, aplikovateľné na údajový paket, vyberie z celého súboru pravidiel, pričom sa uvedený paket zablokuje alebo odošle cez ochrannú stenu. Aby sa zmenšil súbor pravidiel, ktorý treba prehľadávať lineárne, tento súbor pravidiel sa segmentuje. Podľa tohto vynálezu sa toto vykoná pomocou 2-rozmerného vyhľadávania zdrojových adries a adries miesta určenia paketu v súbore adresových prefixov, pričom každý prefix má podsúbor pravidiel z celého súboru pravidiel, aby sa našiel prefix, ktorý je priradený k zdrojovým adresám a adresám miesta určenia. Potom sa na základe obsahu uvedených údajových polí uskutoční hľadanie zhody s pravidlami prostredníctvom prostriedkov 10 na hľadanie zhody s pravidlami, aby sa našlo pravidlo, ktoré sa dá aplikovať na údajový paket.

Pri uskutočňovaní 2-rozmerného vyhľadávania adries sa na každé pravidlo dívame ako na pokrývajúce pravouhlú oblasť 2-rozmernej roviny, pričom ofset a veľkosť pravouholníka sú určené adresovými prefixami a dĺžkami prefixov. Preto vyhľadávanie možno považovať za ten istý problém ako hľadanie pravouholníka,

obklopujúceho bod v rovine. Aby sa vyhľadávanie zjednodušilo, urobí sa obmedzenie, aby sa zabezpečilo, že každý bod v rovine bude krytý jedným a len jedným pravouholníkom, čo povedie k ľahšej procedúre vyhľadávania.

Po uskutočnení 2-rozmerného vyhľadávania adries vyhľadávanie pokračuje s výsledným podsúborom pravidiel, priradených k zistenému aktuálnemu prefixu. V konečnom hľadaní zhody s pravidlami sa však adresové polia nepoužijú. Teda ak pravidlo neplatí pre adresy aktuálneho paketu, nie je v zozname pravidiel, vyplývajúcich z vyhľadávania adries.

Pretože každé pravidlo je reprezentované pravouholníkom, ktorý kryje časť celého adresového priestoru, a niekoľko pravidiel môže zodpovedať tým istým adresám, pravouholníky sa môžu prekrývať. Avšak aby metóda podľa tohto vynálezu pracovala správnym spôsobom, prekrývanie pravouholníkov nie je povolené. Z toho dôvodu, aby sa splnili kritériá neprekrývania, musia sa vykonať nasledujúce kroky:

1. Pre každé pravidlo sa vytvorí pravouholník v adresovom priestore.

2. Vytvorí sa súbor, ktorý bude obsahovať len novovytvorený pravouholník. Tento súbor sa bude nazývať porovnávací súbor.

3. Všetky pravouholníky, ktoré už sú v rovine, sa porovnajú s každým pravouholníkom v porovnávacom súbore.

4. Ak sa prekrývajú, vyseknú sa neprekrývajúce sa časti. K zoznamu pravidiel prekrývajúcich sa častí sa priradí pravidlo z nového pravouholníka, pridaného na jeho koniec.

5. Pre všetky časti - ak táto časť už bola časťou pravouholníka v rovine, vráti sa do roviny. Ak nie, pridá sa k súboru pravouholníkov, ktoré sa majú porovnávať.

6. Ak porovnávací súbor nie je prázdny, vrátime sa ku kroku 3. Pravouholníky, ktoré už sú v rovine a tie, ktoré sa už porovnávali, možno vynechať.

7. V tomto stave je porovnávací súbor prázdny. Ak by niektoré pravouholníky prekrývali nový pravouholník, rozložia sa na menšie časti, ak je to potrebné, pričom spoločné časti majú zoznamy pravidiel, ktoré obsahujú nové pravidlo.

V inej metóde splnenia kritérií neprekrývania sa nie je len súbor pravouholníkov v rovine. Namiesto toho každý pravouholník obsahuje popri svojich súradniciach a indexe zoznamu pravidiel súbor pravouholníkov alebo pod-

pravouholníkov. Každý z týchto podpravouholníkov má ďalší súbor podpravouholníkov. Avšak niekedy je nevyhnutné odkazovať na ten istý podpravouholník a prechádzať smerovaným necyklickým grafom (DAG) hĺbky pravouholníkov.

Vždy existuje jeden koreňový pravouholník, ktorý pokrýva celú rovinu. To reprezentuje štandardné nastavenie, ktoré bude platiť, keď zlyhajú všetky ostatné porovnávania.

Pravouholník, nazývaný koreň, je koreňový pravouholník, ku ktorému sa má pridať nový pravouholník.

Ak majú koreň a nové pravouholníky rovnakú veľkosť, pravidlá v novom pravouholníku sa pridajú k zoznamu pravidiel, priradených koreňovému pravouholníku.

Iteruje sa cez všetky podpravouholníky koreňového pravouholníka. Ak sa nový pravouholník dá úplne pokryť ľubovoľným z nich, vykoná sa rekurzívne volanie s týmto podpravouholníkom namiesto koreňa a potom návrat.

Ešte raz sa iteruje cez všetky podpravouholníky v koreňovom pravouholníku.

Ak je podpravouholník úplne obsiahnutý v novom pravouholníku, presunie sa z koreňového pravouholníka do nového pravouholníka. Zoznam pravidiel podpravouholníka a všetkých pravouholníkov pod ním sa musí modifikovať, aby zahrnul aj pravidlo nového pravouholníka.

Ak sa podpravouholník pretína s novým pravouholníkom, vytvorí sa nový pravouholník, obsahujúci ich spoločnú časť. Zoznam pravidiel pretínajúceho sa pravouholníka je kombináciou pôvodných. Potom sa nový pravouholník pridá tak k pôvodnému podpravouholníku, ako aj k novému pravouholníku.

Akonáhle sa všetky pravouholníky pridali k DAG, graf sa môže prejsť a môže sa vytvoriť zoznam pravouholníkov s definovanými prefixami, ktorý je potrebný pre dvojrozmerný vyhľadávací kód. Pretínajúci sa pravouholník bude správne prefixom definovaný pravouholník, ale zvyšok obklopujúceho pravouholníka po vyseknutí podpravouholníkov nemusí byť správne definovaný prefixami.

Keď sa údajová štruktúra použije na filtrovanie vyhľadávaní, ako sme opísali vyššie, vyhľadávanie sa uskutoční vo dvoch krokoch. Najprv sa uskutoční dvojrozmerné vyhľadávanie adresy, ktoré vedie k číslu typu integer. Toto celé číslo je indexom do poľa pravidiel, kde každé pravidlo špecifikuje, ktoré polia sa majú

porovnávať a aká činnosť sa má vykonať, ak sa našla zhoda. Každé pravidlo má nasledujúce pole, ktoré indikuje, s ktorým pravidlom sa má pokračovať v prípade nezhody. Prechádzanie zoznamom pravidiel pokračuje, kým sa nenájde zhoda, a keď sa uskutočnia príslušné činnosti, aby sa paket zablokoval alebo odoslal.

Problém 2-rozmerných prefixov je vyriešený nasledovne.

Adresový priestor alebo obor **U** je 2-rozmerný priestor, pozostávajúci z párov (s, d) celých čísel, vyhovujúcich podmienke $0 \leq s < 2^{32}$, $0 \leq d < 2^{32}$.

Podmnožina R z **U**, ktorá vyhovuje podmienke: $(s, d) \in R$, ak $s_0 \leq s < s_1$, $d_0 \leq d < d_1$, kde (s_0, d_0), $(s_1, d_1) \in \mathbf{U}$, sa nazýva pravouholník. Ďalej, pár bodov $[(s_0, d_0),(s_1, d_1)]$ jednoznačne definuje R.

Pravouholník, definovaný $[(s_0, d_0),(s_1, d_1)]$, kde $s_1 - s_0 = s_1 - 2^{i_s} * k_s = 2^{i_s}$ a $d_1 - d_0 = = d_1 - 2^{i_d} * k_d = 2^{i_d}$ pre niektoré nezáporné celé čísla i_s, i_d, k_s a k_d, sa nazýva prefix.

Ak je daný bod $(s, d) \in \mathbf{U}$ a množina prefixov $\mathbf{P} = \{P_1, P_2, \ldots P_n\}$ taká, že **P** je oddielom U, problém zhody 2-rozmerných prefixov je problémom, ako vypočítať i tak, že $(s, d) \in P_i$.

Časť problému filtrovania ochrannou stenou, týkajúca sa zdroja-miesta určenia, je reprezentovaná ako problém zhody 2-rozmerných prefixov, kde sa množina **P** získa konvertovaním smerovej tabuľky a pravidiel filtrovania do oddielov prefixov. Pretože každý paket, ktorý sa má filtrovať, vyžaduje vyhľadanie zhody prefixov, je nevyhnutné nájsť reprezentáciu P takú, aby sa zhoda prefixov dala vypočítať efektívne.

Viaceré prefixy, ktoré delia malý, 32 x 32-bitový obor, sú znázornené na obr. 3. Čierne štvorčeky 18 reprezentujú bity, ktoré sú nastavené na 1 (reprezentanti) a biele štvorčeky 19 reprezentujú nenastavené bity. Poznámka: bod (0, 0) je umiestnený v ľavom hornom rohu na obr. 3.

Pre každý prefix $P = [(s_0, d_0), (s_1, d_1)] \in \mathbf{P}$ je bod $p_0 = (s_0, d_0)$ vybraný ako reprezentant P. Ďalej nech $\mathbf{p} = \{p_1, p_2,\ldots,p_n\} = \{(s_1, d_1), (s_2, d_2),\ldots, (s_n, d_n),\}$ označuje súbor reprezentantov prefixov v **P**.

Ak je daný bod $(s_d, d_d) \in \mathbf{U}$, pre každý $(s, d) \in \mathbf{U}$ taký, že $s_d \geq s$ a $d_d \geq d$, (s_d, d_d) je majorantným bodom k (s, d) alebo alternatívne, (s, d) je majorizovaný (s_d, d_d).

Ak je daný pár bodov (s_1, d_1), $(s_2, d_2) \in \mathbf{U}$, vzdialenosť medzi týmito bodmi pod normou L_∞ je daná výrazom:

$$\lim_{k\to\infty} (|s_1-s_2|^k + |d_1-d_2|^k)^{1/k} = \max(|s_1-s_2|, |d_1-d_2|)$$

Ak je teraz daný bod p = (s, d), problém nájdenia zhodného prefixu v **P** je ekvivalentný problému nájdenia najbližšieho majorantného bodu k p v **p** pod normou L_∞, t. j. majorantný bod $p_i \in \mathbf{p}$ z p, minimalizujúci L_∞-vzdialenosť medzi p_i a p. Preto stačí reprezentovať len majorantné body namiesto prefixov samotných.

Ako je znázornené na obr. 4, množina **p** je koncepčne reprezentovaná ako bitová matica s 2^{32} x 2^{32} bodmi, kde bit p je nastavený na 1, ak $p \in \mathbf{p}$. Aby sa zmenšil priestor, potrebný na reprezentáciu, v skutočnosti reprezentujeme **p** ako štvorúrovňový 2^{8+8}-násobný strom. Každá úroveň je (zasa) koncepčne reprezentovaná ako bitová matica s 2^8 x 2^8 bitmi, kde bit (s, d) je nastavený na 1, ak v substrome pod ním existuje majorantný bod. To znamená, že na úrovni 1 (horná úroveň) bit (s, d) reprezentuje prítomnosť alebo neprítomnosť majorantného bodu v pravouholníku $[(2^{24}*s, 2^{24}*d), (2^{24}*(s+1), 2^{24}*(d+1))]$ z **U**.

Skutočnou reprezentáciou úrovne je 2-rozmerný hustý zväzok alebo jednoducho 2d-zväzok. Ako a kedy sa dá úroveň reprezentovať 1-rozmerným hustým zväzkom, vysvetlíme neskôr. 2d-zväzok pozostáva z 32 x 32 dielov, kde každý diel reprezentuje 8 x 8 bitov. Pretože body, ktoré definujú diel, sú majorantnými bodmi prefixov, nie je možných všetkých 2^{64} druhov dielov. V skutočnosti kladieme na diely obmedzenia, takže je možných len 677 rozličných druhov.

Ak v dieli T existuje bod (bod v niektorých z podoborov, reprezentovaný jedným z bitov v dieli), ktorý má svoj najbližší majorantný bod v inom dieli T_d, potom všetky body v T majú svoje najbližšie majorantné body v T_d. Definícia majorantného bodu je rozšírená na majorantný diel. Diel T_d sa nazýva majorantným dielom T, alebo alternatívne, diel T je majorizovaný dielom T_d.

Aby sa splnila požiadavka predchádzajúcej definície, je potrebná nasledujúca veta.

Ak P = [(s_0, d_0), (s_1, d_1)] je prefix, vyhovujúci podmienke, že s_1-s_0 > 1, potom [(s_0, d_0), (s_0+2^i, d_0)] a [(s_0+2^i, d_0), (s_1, d_1)], kde s_1-s_0 = 2^i pre niektoré nezáporné celé číslo i, sú tiež prefixami. Veta pre druhý rozmer je symetrická.

Na základe vyššie uvedenej vety sa dá prefix rozdeliť na 2 časti, kedykoľvek je to potrebné. Preto, ak je daná množina prefixov $\mathbf{P}_d$ s reprezentantami v dieli T_d, môžeme ich opakovane deliť, kým všetky prefixy nebudú mať svoje koncové body v tom istom dieli, v oboch rozmeroch, aby sa splnila vyššie uvedená požiadavka. Toto sa nazýva delením dielov a je to kritická časť konštrukcie hustých 2d-zväzkov.

Rozličné druhy dielov sú rozdelené na sedem tried, znázornených na obr. 5 až 11. Pre každú triedu je určitý/nejaký diel znázornený ako bitová matica in (hviezdičky reprezentujú bity, ktoré môžu byť buď 0 alebo 1). Pre každý nastavený bit (nie *) a triedu dielov existujú aj čiary, indikujúce zaručené hranice podmnožiny, majorizovanej týmto bitom (bodom). Všimnime si, že nastavený bit v dieli môže byť typicky majorantným pre body v iných dieloch napravo a/alebo pod ním. Tiež udávame počet rozličných druhov dielov v triede a rozlišujeme prirodzené a obmedzené triedy dielov. Nakoniec opíšeme, ako sú diely reprezentované/-zakódované v hustom 2d-zväzku.

Diel triedy (0, 0) je znázornený na obr. 5. Žiadny bit nie je nastavený na 1: prirodzený, 1 druh, a vždy je majorizovaný dielom T_d z triedy (1, 1), (1, 2), (2, 1), (1, 3+) alebo (3+, 1). Nájsť majorantný bod k bodu v bite (s_b, d_b) v dieli triedy (0, 0) je presne to isté ako nájsť majorantný bod k zodpovedajúcemu bodu v bite (s_b, d_b) jeho majorantného dielu T_d. Preto diel triedy (0, 0) môže byť a mal by byť vždy zakódovaný presne tým istým spôsobom ako jeho majorantný diel T_d.

Diel triedy (1, 1) je znázornený na obr. 6. Jeden bit je nastavený na 1: prirodzený, 1 druh, a prípadne majorizuje diely triedy (0, 0) napravo a/alebo pod ním. Pretože všetky body v tomto dieli majú ten istý najbližší majorantný bod, jednoducho zakódujeme odkaz na tento bod v dieli samotnom.

Diel triedy (1, 2) je znázornený na obr. 7. Dva bity v prvom riadku (D-rozmer) sú nastavené na 1: prirodzený, 1 druh, a prípadne majorizuje diely triedy (0, 0) pod ním. Nemôže majorizovať diely triedy (0, 0) napravo.

Existujú dva najbližšie majorantné body k bodom v tomto dieli, jeden pre body v ľavej polovici a jeden pre body v pravej polovici. Zakódujeme odkazy na oba tieto majorantné body ako pole s dĺžkou 2 a potom môžeme použiť ľavú/pravú polovicu dopytového bodu ako indexy.

Diel triedy (2, 1) je znázornený na obr. 8. Dva bity v prvom stĺpci (S-rozmer) sú nastavené na 1: prirodzený, 1 druh, a prípadne majorizuje diely triedy (0, 0) napravo. Nemôže majorizovať diely triedy (0, 0) pod ním. Existujú dva najbližšie majorantné body k bodom v tomto dieli, jeden pre body v hornej polovici a jeden pre body v spodnej polovici. Odkazy na oba tieto majorantné body zakódujeme ako pole s dĺžkou 2 a potom môžeme použiť hornú/spodnú polovicu dopytového bodu ako indexy.

Diel triedy (1, 3+) je znázornený na obr. 9. Nastavené na 1 sú tri alebo viac bitov v prvom riadku: prirodzený, 24 druhov, a prípadne majorizuje diely triedy (0, 0) pod ním. Nemôže majorizovať diely triedy (0, 0) napravo. Môže existovať veľa majorantných bodov k bodom v tejto triede dielov. Je nevyhnutné zakódovať druh dielu, pretože existuje 24 rôznych druhov dielov. Ďalej, pre každý bit v prvom riadku, nastavený na 1, sa zakóduje smerník k majorantnému bodu pod ním (ak existuje len jeden) alebo k zväzku nasledujúcej úrovne (ak existuje niekoľko majorantných bodov). Nakoniec sa zakóduje odkaz na prvý smerník (základný smerník). Týmto spôsobom sa dá nájsť majorantný bod (alebo odkaz na zväzok nasledujúcej úrovne) k dopytovému bodu (s, d) jednoducho vyhľadaním stĺpca, v ktorom sa d nachádza, a spolu s druhom zväzku vykonať prehľadávanie tabuľky, aby sa získal ofset x smerníka, a nakoniec získať smerníky smerníka x od základného smerníka. Všimnime si, že stačí, keď akýkoľvek zväzok nasledujúcej úrovne je jedno(D-)rozmerný, pretože všetci reprezentanti v tomto dieli ležia na tej istej S-súradnici.

Diel triedy (3+, 1) je znázornený na obr. 10. Tri alebo viac bitov v prvom stĺpci sú nastavené na 1: prirodzený, 24 druhov, a prípadne majorizuje diely triedy (0, 0) napravo. Nemôže majorizovať diely triedy (0, 0) pod ním. Môže existovať veľa majorantných bodov k bodom v tejto triede dielov. Je nevyhnutné zakódovať druh dielu, pretože existuje 24 rôznych druhov. Ďalej, pre každý bit v prvom stĺpci, nastavený na 1, sa zakóduje smerník k majorantnému bodu nadol (ak existuje len jeden) alebo k zväzku nasledujúcej úrovne (ak existuje niekoľko majorantných

bodov). Nakoniec sa zakóduje odkaz na prvý smerník (základný smerník). Týmto spôsobom sa dá nájsť majorantný bod (alebo odkaz na zväzok nasledujúcej úrovne) k dopytovému bodu (s, d) jednoducho vyhľadaním riadku, v ktorom sa s nachádza, a spolu s druhom zväzku vykonať prehľadávanie tabuľky, aby sa získal ofset x smerníka, a nakoniec získať smerníky smerníka x od základného smerníka. Všimnime si, že stačí, keď akýkoľvek zväzok nasledujúcej úrovne je jedno(S-)rozmerný, pretože všetci reprezentanti v tomto dieli ležia na tej istej D-súradnici.

Diel triedy (2+, 2+) je znázornený na obr. 11. Dva alebo viac bitov je nastavených na 1 tak v prvom riadku, ako aj v prvom stĺpci: obmedzený, 625 druhov, nemôže majorizovať iný diel a nemôže byť majorizovaný iným dielom. Typicky existuje v tejto triede dielov veľa majorantných bodov. Zakódovanie sa uskutočňuje presne tak ako pre diely triedy (1, 3+) a (3+, 1). Je však zavedené obmedzenie, aby sa znížil počet rozličných druhov pred uskutočnením faktického zakódovania. Prvou úlohou je zaviesť obmedzenie, podobné obmedzeniu dielu z definície 8, na každý bit. Potom sa vypočíta pár bitových vektorov s dĺžkou 8, Sv a Dv, kde

S_i = 1, ak existuje v i-tom riadku bit, nastavený na 1, a
0 v inom prípade

D_i = 1, ak existuje v i-tom stĺpci bit, nastavený na 1, a
0 v inom prípade.

Nakoniec sa vytvorí nový diel vypočítaním súčinu Sv a Dv^T s použitím maticového násobenia a zakóduje sa.

Tak ako v dieloch tried (1, 3+) a (3+, 1) môžu byť aj v tomto prípade vytvorené jednorozmerné podúrovne. Kontroluje sa, či všetci reprezentanti v bite, ktorý obsahuje viac než jedného reprezentanta, sú v tom istom riadku v **U**, čo znamená, že S-rozmer skolabuje, alebo v tom istom stĺpci v **U**, čo znamená, že D-rozmer skolabuje.

Ďalší opis obsahuje údajové štruktúry, použité v ochrannej stene na reprezentáciu NAT a HP vstupov.

V oboch prípadoch sa používa pár IP adries *saddr* a *daddr*, pár portov *sport* a *dport* a protokol *proto* spracúvaného paketu ako kľúč pri vyhľadávaní. Prvým krokom pri vyhľadávaní je výpočet transformačnej hodnoty. To sa uskutoční s

použitím veľmi jednoduchých a rýchlych inštrukcií, ako sú bitové posuny bitových logických operátorov. S použitím transformačnej hodnoty ako indexu sa 16-bitový smerník získa z veľkého poľa (transformačnej tabuľky).

Smerník je buď 0, čo znamená, že vyhľadávanie zlyhalo (prázdny) alebo odkazuje na koreň Patricia stromu, ktorý je veľmi efektívnou údajovou štruktúrou na reprezentáciu malých súborov kľúčov. Ak smerník odkazuje na Patricia strom, kľúč sa vytvorí spojením bitových obrazcov *saddr*, *daddr*, *sport*, *dport* a *proto*. Tento kľúč sa potom použije pri prehľadávaní Patricia stromu, ako je opísané v nasledujúcej časti.

Patricia strom je binárny strom, ktorý spracúva dopytové kľúče ako bitové polia a používa bitový index v každom vnútornom uzle na riadenie vetvenia. Prehľadávanie sa uskutoční prechádzaním stromom od koreňa po list. Keď sa príde k vnútornému uzlu s bitovým indexom i, preskúma sa bit i dopytového kľúča, aby sa určilo, či sa má pokračovať v hľadaní v ľavom (ak bit je 0) alebo v pravom (ak bit je 1) substrome. Prechádzanie sa zastaví, keď sa príde k listu. Aby sa určilo, či je dopytový kľúč prítomný v tabuľke alebo nie, dopytový kľúč sa porovná s kľúčom, zapamätaným v tomto liste. Ak sú oba kľúče rovnaké, hľadanie bolo úspešné.

Obr. 12 znázorňuje príklad neúspešného hľadania pre dopytový kľúč 001111 v Patricia strome, obsahujúcom šesť kľúčov. Počas prechádzania sa skúmajú bity č. 0, 2 a 3, čo končí v liste s kľúčom 011101. Keď sa porovnáva dopytový kľúč s kľúčom listu, deteguje sa nezhoda v bite č. 1.

S ohľadom na bitové indexy, zapamätané vo vnútorných uzloch, je Patricia strom usporiadaný ako pyramída. To znamená, že akýkoľvek vnútorný uzol s výnimkou koreňa má bitový index väčší, než je bitový index jeho predchodcu. Z toho vyplýva, že všetky kľúče, zapamätané v substrome, ktorého koreňom je uzol s bitovým indexom i, sú identické až po a vrátane bitu i-1.

Vloženie sa vykoná tak, že sa najprv uskutoční neúspešné vyhľadávanie a zaznamená sa index i prvého nezhodujúceho sa bitu pri porovnávaní dopytového kľúča s kľúčom listu. Potom sa vytvoria dva nové uzly, nový vnútorný uzol s indexom i a listový uzol pre dopytový kľúč. V závislosti od toho, či i-ty bit dopytového kľúča je 0 alebo 1, sa list zapamätá ako ľavý alebo pravý substrom vnútorného uzla. S použitím druhého poľa substromu ako spojovacieho poľa sa vnútorný uzol potom

vloží priamo nad uzol s najmenším bitovým indexom väčším než i do dráhy, prechádzanej od koreňa k listu.

Obr. 13 znázorňuje Patricia strom ako výsledok vloženia dopytového kľúča z neúspešného hľadania z predchádzajúceho príkladu na obr. 12. Vytvorí sa nový vnútorný uzol s bitovým indexom 1 a vloží sa medzi uzly s bitovými indexami 0 a 2 v dráhe, prechádzanej od koreňa.

Patricia transformácia, použitá na dierovanie, pracuje presne tak, ako sme opísali vyššie – jednoduché prehľadávanie transformačnej tabuľky, po ktorom nasleduje prehľadávanie Patricia stromu. Vo väčšine prípadov sa list dosiahne priamo, čo znamená, že nie je nevyhnutné vytvárať bitové pole z parametrov – tieto sa porovnávajú priamo so zodpovedajúcimi poľami v štruktúre, obsahujúcej/ reprezentujúcej Patricia list.

Je vytvorená vyhľadávacia funkcia *hp_lookup(iaddr, xaddr, iport, xport, proto)*, ktorá sa používa tak pre I2X-HP, ako aj pre X2I-HP. Jediným rozdielom medzi nimi je poradie, v akom sú zadané parametre. Pre I2X-HP sa funkcia volá ako *hp_lookup(saddr, daddr, sport, dport, proto)* a pre X2I-HP sa volá ako *hp_lookup(daddr, saddr, dport, sport, proto)*.

Vyhľadávacia funkcia vracia odkaz na štruktúru, obsahujúcu kľúč Patricia listu, t. j. *iaddr*, *xaddr*, *iport*, *xport* a *proto*, a rad ďalších polí, ktoré reprezentujú stav spojenia, napríklad TCP sekvenčné čísla.

Patricia transformácia pre NAT je o niečo zložitejšia než pre HP. Dôvodom je to, že na rozdiel od HP, kde sú zahrnuté len dve adresy a porty, sú tu zahrnuté tri rozličné adresy a porty, *iaddr*, *naddr*, *xaddr*, *iport*, *nport*, *xport*. To znamená, že rozdiel medzi I2X a X2I sa stáva o niečo zložitejším než jednoducho presúvanie adries a portov pri vyhľadávaní.

Tento problém je vyriešený tým, že sa nechá vytvoriť zrkadlový obraz najmenej signifikantného bitu transformačnej hodnoty, ak je vyhľadávaním I2X alebo X2I (to je v podstate to isté ako použitie dvoch transformačných tabuliek). Štruktúra, obsahujúca kľúče Patricia listov pre NAT spojenie, je rovnaká pre I2X a X2I a obsahuje všetky tri adresy a porty.

Existujú dve vyhľadávacie funkcie, *nat_i2x_lookup(saddr, daddr, sport, dport, proto)* a *nat_x2i_lookup(saddr, daddr, sport, dport, proto)*. Obe funkcie používajú

argumenty na vypočítanie transformačnej hodnoty, pričom sa najmenej signifikantný bit príslušne nastaví. Ak výsledný smerník odkazuje na Patricia uzol (vnútorný uzol), adresy, porty a protokol sa spoja, aby vytvorili bitové pole, potrebné na prechádzanie cez Patricia strom. Keď sa dosiahne listová štruktúra, adresy, porty a protokol sa porovnajú so zodpovedajúcimi poľami v liste.

Keď sa paket podrobí I2X-NAT:

saddr (paketu) sa porovná s *iaddr* (listovej štruktúry)

daddr sa porovná s *xaddr*

sport sa porovná s *iport*

dport sa porovná s *xport*

proto sa porovná s *proto*.

Ak sa všetky zhodujú, vyhľadávanie je úspešné a zdrojová adresa a port, *saddr* a *sport*, paketu sa nahradia *naddr* a *nport* (listovej štruktúry) predtým, než sa paket odošle ďalej.

Keď sa paket podrobí X2I-NAT:

saddr (paketu) sa porovná s *xaddr* (listovej štruktúry)

daddr sa porovná s *naddr*

sport sa porovná s *xport*

dport sa porovná s *nport*

proto sa porovná s *proto*.

Ak sa všetky zhodujú, vyhľadávanie je úspešné a adresa miesta určenia a port, *daddr* a *dport*, paketu sa nahradia *iaddr* a *iport* (listovej štruktúry) predtým, než sa paket odošle do nasledujúceho kroku spracovania.

Aktualizácie HP a NAT údajových štruktúr uskutoční EffNIX jadro (predtým NetBSD), bežiace na BSP (procesor 1), ale väčšinu vyhľadávaní uskutočňuje odosielajúce jadro, bežiace na AP (procesor 2). Existuje len jeden prípad HP údajovej štruktúry a jeden prípad NAT údajovej štruktúry. Tieto sa nachádzajú v zdieľanej pamäti a oba procesory k nim pristupujú súčasne. To vedie k veľmi zaujímavému problému synchronizácie – jeden zapisovač a jeden čítač. Synchronizácia sa vyrieši tým, že aktualizačné programy sa nechajú, aby urobili štruktúry listov a uzly neplatnými predtým, než sa čokoľvek zmení (zapisovanie). Vyhľadávací program skontroluje, či listy a uzly, ku ktorým sa pristupuje, sú platné

predtým a potom, ako sa k nim uskutočnil prístup, a tiež, či sa nezmenili počas tohto prístupu. Ak dôjde k súbehu a tento sa deteguje (všetky nebezpečné stavy súbehov sa detegujú), vyhľadávanie zlyhá a paket sa odošle do BSP a spracuje sa tam (buď sa uskutoční úspešné hľadanie a následné spracovanie, alebo sa údajové štruktúry aktualizujú).

Malo by byť zrejmé, že tento vynález poskytuje zariadenie ochrannej steny a spôsob riadenia sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami, ktorý úplne vyhovuje cieľom a výhodám, ktoré sme uviedli vyššie.

Hoci bol vynález opísaný v spojitosti s jeho špecifickým uskutočnením, tento vynález sa dá uskutočniť v rozličných formách, pričom treba chápať, že tento opis sa má považovať za uvedenie príkladu princípov vynálezu a nemá obmedzovať vynález na ilustrované špecifické uskutočnenie.

PV2023-2000
09.04.01

PATENTOVÉ NÁROKY

1. Ochranná stena (3) na riadenie sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami (1, 5, 4), zahrnujúca filtračné prostriedky na výber z celého súboru pravidiel v závislosti od obsahu údajových polí údajového paketu, ktorý sa prenáša medzi uvedenými sieťami, pravidla, aplikovateľného na uvedený údajový paket, aby sa uvedený paket zablokoval alebo aby sa uvedený paket odoslal cez ochrannú stenu (3), v y z n a č u j ú c a s a t ý m, že zahrnuje prostriedky (8) na vyhľadávanie v 2-rozmernej tabuľke zdrojových adries a adries miesta určenia paketu v súbore adresových prefixov, pričom každý adresový prefix má podsúbor pravidiel z celého súboru pravidiel, aby sa našiel adresový prefix prostredníctvom jeho reprezentácie, priradený uvedeným zdrojovým adresám a adresám miesta určenia, a prostriedky (10) na hľadanie zhody s pravidlami – na základe obsahu uvedených údajových polí, aby sa našlo pravidlo, aplikovateľné na uvedený údajový paket.

2. Ochranná stena podľa nároku 1, v y z n a č u j ú c a s a t ý m, že uvedené prostriedky (8) na vyhľadávanie v 2-rozmernej tabuľke zahrnujú prostriedky na nájdenie prefixu, priradeného uvedeným zdrojovým adresám a adresám miesta určenia, určením najbližšieho majorantného bodu p v **p** pod normou L_∞, t. j. majorantného bodu $p_i \in \mathbf{p}$ z p, ktorý minimalizuje L_∞-vzdialenosť medzi p_i a p.

3. Ochranná stena podľa nároku 2, v y z n a č u j ú c a s a t ý m, že

zdrojové adresy a adresy miesta určenia sú reprezentované bodom $(s, d) \in \mathbf{U}$, kde **U** je 2-rozmerný adresový priestor, reprezentovaný pármi (s, d) celých čísel, vyhovujúcich podmienke $0 \le s < 2^{32}$, $0 \le d < 2^{32}$,

prefixy $\mathbf{P} = \{P_1, P_2, \ldots P_n\}$ sú oddiely adresového priestoru **U**, a

každý prefix P_i je logickým pravouholníkom R v adresovom priestore **U**, definovaným $[(s_0, d_0),(s_1, d_1)]$, kde $s_1 - s_0 = s_1 - 2^{i_s} * k_s = 2^{i_s}$ a $d_1 - d_0 = = d_1 - 2^{i_d} * k_d = 2^{i_d}$ pre niektoré nezáporné celé čísla i_s, i_d, k_s a k_d,

pričom uvedený logický pravouholník R je podmnožinou **U**, ktorá vyhovuje podmienke: $(s, d) \in R$, ak $s_0 \leq s < s_1$, $d_0 \leq d < d_1$, kde (s_0, d_0), $(s_1, d_1) \in \mathbf{U}$, a pár bodov $[(s_0, d_0),(s_1, d_1)]$ jednoznačne definuje uvedený pravouholník R.

4. Ochranná stena podľa nároku 2 alebo 3, v y z n a č u j ú c a s a t ý m, že pre každý prefix $P = [(s_0, d_0), (s_1, d_1)] \in \mathbf{P}$ je bod $p_0 = (s_0, d_0)$ reprezentantom P a $\mathbf{p} = \{p_1, p_2,\ldots,p_n\} = \{(s_1, d_1), (s_2, d_2),\ldots, (s_n, d_n),\}$ je množina reprezentantov prefixov v **P**, pričom ak je daný bod $(s_d, d_d) \in \mathbf{U}$, pre každý $(s, d) \in \mathbf{U}$ taký, že $s_d \geq s$ a $d_d \geq d$, (s, d) je majorizovaný (s_d, d_d).

5. Ochranná stena podľa nároku 3, v y z n a č u j ú c a s a t ý m, že ak je daný pár bodov (s_1, d_1), $(s_2, d_2) \in \mathbf{U}$, vzdialenosť medzi týmito bodmi pod normou L_∞ je daná výrazom:

$$\lim_{k\to\infty} (|s_1-s_2|^k + |d_1-d_2|^k)^{1/k} = \max(|s_1-s_2|, |d_1-d_2|)$$

6. Ochranná stena podľa ktoréhokoľvek z predchádzajúcich nárokov, v y - z n a č u j ú c a s a t ý m, že zahrnuje fragmentovací stroj (11), zahrnujúci prostriedky na zberanie fragmentov, určené na pozberanie fragmentov paketov z fragmentovaného paketu, kým sa neprijme hlavička fragmentu uvedeného paketu, prostriedky na zapamätanie hlavičky fragmentu na zapamätanie informácie, prítomnej v poli hlavičky fragmentu paketu, vo vstupných prostriedkoch, prostriedky na odoslanie fragmentu na odoslanie paketových fragmentov, vybavených informáciou hlavičky fragmentu, počnúc hlavičkou fragmentu, pričom každý fragment sa spracuje filtračnými prostriedkami ako regulárny nefragmentovaný paket.

7. Ochranná stena podľa ktoréhokoľvek z predchádzajúcich nárokov, v y - z n a č u j ú c a s a t ý m, že zahrnuje prostriedky (12, 14) na prevádzanie sieťových adries, ktoré prevádzajú v závislosti od informácie v prefixe vnútorné zdrojové adresy na vonkajšie zdrojové adresy paketu, prenášaného von cez

ochrannú stenu (3), alebo vonkajšie zdrojové adresy na vnútorné zdrojové adresy paketu, prenášaného dovnútra cez ochrannú stenu (3).

8. Ochranná stena podľa ktoréhokoľvek z nárokov 1 až 6, v y z n a č u j ú c a s a t ý m, že zahrnuje prostriedky (12, 14) na prevádzanie sieťových adries, ktoré prevádzajú v závislosti od informácie v prefixe vnútorné zdrojové adresy na vonkajšie zdrojové adresy paketu, prenášaného z vnútornej siete (1) do vonkajšej siete (4), alebo vonkajšie zdrojové adresy na vnútorné zdrojové adresy paketu, prenášaného z vonkajšej siete (4) do vnútornej siete (1).

9. Ochranná stena podľa ktoréhokoľvek z predchádzajúcich nárokov, v y - z n a č u j ú c a s a t ý m, že zahrnuje dierovacie prostriedky (16, 17) na určenie na základe informácie v prefixe, či uvedený paket podlieha dočasnej výnimke z vonkajšieho-do-vnútorného blokovacieho pravidla pre spojenie, iniciované z vnútornej siete, pričom sa pre pakety, prenášané z vonkajšej siete (4) do vnútornej siete (1), vytvorí spätný kanál cez ochrannú stenu počas trvania spojenia.

10. Ochranná stena (3) na riadenie sieťovej prevádzky údajových paketov medzi vnútornými a vonkajšími sieťami (1, 5, 4), zahrnujúca filtračné prostriedky na výber z celého súboru pravidiel v závislosti od obsahu údajových polí údajového paketu, ktorý sa prenáša medzi uvedenými sieťami, pravidla, aplikovateľného na uvedený údajový paket, aby sa uvedený paket zablokoval alebo aby sa uvedený paket odoslal cez ochrannú stenu (3), v y z n a č u j ú c a s a t ý m, že zahrnuje fragmentovací stroj (11), zahrnujúci prostriedky na zberanie fragmentov z fragmentovaného paketu, kým sa neprijme hlavička fragmentu uvedeného paketu, prostriedky na zapamätanie hlavičky fragmentu na zapamätanie informácie, prítomnej v poli hlavičky fragmentu, vo vstupných prostriedkoch, prostriedky na odoslanie fragmentu na odosielanie paketových fragmentov, vybavených informáciou hlavičky fragmentu, počnúc hlavičkou fragmentu, pričom sa každý fragment spracuje filtračnými prostriedkami ako regulárny nefragmentovaný paket.

11. Spôsob riadenia sieťovej prevádzky údajových paketov medzi vnútornou sieťou (1, 5) a vonkajšou sieťou (4) cez ochrannú stenu (3), zahrnujúci kroky

výberu z celého súboru pravidiel v závislosti od obsahu údajových polí údajového paketu, ktorý sa prenáša medzi uvedenými sieťami, pravidla, aplikovateľného na uvedený údajový paket,

aplikovania uvedeného pravidla na uvedený paket, a

v závislosti od pravidla zablokovania uvedeného paketu alebo odoslania uvedeného paketu cez ochrannú stenu (3),

v y z n a č u j ú c i s a t ý m, že uvedená filtrácia zahrnuje ďalšie kroky:

uskutočnenia vyhľadávania v 2-rozmernej tabuľke zdrojových adries a adries miesta určenia paketu, aby sa našiel prefix prostredníctvom jeho reprezentácie, priradený uvedeným zdrojovým adresám a adresám miesta určenia v množine adresových prefixov, pričom každý prefix má podsúbor pravidiel z celého súboru pravidiel,

a na základe obsahu uvedených údajových polí paketu uskutočnenia hľadania zhody s pravidlami na tomto podsúbore pravidiel, aby sa našlo pravidlo, aplikovateľné na údajový paket.

12. Spôsob podľa nároku 11, v y z n a č u j ú c i s a t ý m, že pred krokom výberu pravidla, aplikovateľného na údajový pakt, zahrnuje ďalšie kroky:

zberania paketových fragmentov z fragmentovaného paketu, kým sa neprijme hlavička fragmentu uvedeného paketu,

zapamätania informácie, prítomnej v poli hlavičky fragmentu paketu, vo vstupných prostriedkoch, a

odoslania paketových fragmentov, vybavených informáciou hlavičky fragmentu, počnúc hlavičkou fragmentu, pričom každý fragment sa spracuje filtračnými prostriedkami ako regulárny nefragmentovaný paket.

13. Spôsob podľa nároku 11 alebo 12, v y z n a č u j ú c i s a t ý m, že pred krokom uskutočnenia vyhľadávania zhody s pravidlami zahrnuje ďalší krok:

v závislosti od informácie v prefixe prevedenia vonkajšej zdrojovej adresy do vnútornej zdrojovej adresy paketu, ktorý sa má preniesť dovnútra cez ochrannú stenu (3).

14. Spôsob podľa ktoréhokoľvek z predchádzajúcich nárokov 11 až 13, v y - z n a č u j ú c i s a t ý m, že pred krokom uskutočnenia vyhľadávania zhody s pravidlami zahrnuje ďalší krok:

v závislosti od informácie v prefixe prevedenia vonkajšej zdrojovej adresy do vnútornej zdrojovej adresy paketu, ktorý sa má preniesť z vonkajšej siete (4) do vnútornej siete (1, 5).

15. Spôsob podľa ktoréhokoľvek z predchádzajúcich nárokov 11 až 14, v y - z n a č u j ú c i s a t ý m, že zahrnuje ďalší krok:

v závislosti od informácie v prefixe prevedenia vnútornej zdrojovej adresy do vonkajšej zdrojovej adresy paketu, ktorý sa má preniesť von cez ochrannú stenu (3).

16. Spôsob podľa ktoréhokoľvek z predchádzajúcich nárokov 11 až 15, v y - z n a č u j ú c i s a t ý m, že zahrnuje ďalší krok:

v závislosti od informácie v prefixe prevedenia vnútornej zdrojovej adresy do vonkajšej zdrojovej adresy paketu, ktorý sa má preniesť z vnútornej siete (4) do vonkajšej siete (1, 5).

17. Spôsob podľa ktoréhokoľvek z predchádzajúcich nárokov 11 až 16, v y - z n a č u j ú c i s a t ý m, že pred krokom uskutočnenia vyhľadávania zhody s pravidlami zahrnuje ďalšie kroky:

na základe informácie v prefixe určenia, či uvedený paket podlieha dočasnej výnimke z vonkajšieho-do-vnútorného blokovacieho pravidla pre spojenie, iniciované z vnútornej siete (1),

ak je to tak, vytvorenia spätného kanála pre pakety, prenášané z vonkajšej siete (4) do vnútornej siete (1) cez ochrannú stenu (3), s dobou trvania, zodpovedajúcou dobe existencie spojenia.

18. Spôsob riadenia sieťovej prevádzky údajových paketov medzi vnútornou a vonkajšou sieťou (1, 5, 4) cez ochrannú stenu (3), zahrnujúci kroky

v závislosti od obsahu údajových polí údajového paketu, ktorý sa prenáša medzi uvedenými sieťami, výberu z celého súboru pravidiel pravidla, aplikovateľného na uvedený údajový paket,

aplikovania uvedeného pravidla na uvedený paket,

a v závislosti od tohto pravidla buď zablokovania uvedeného paketu alebo odoslania uvedeného paketu cez ochrannú stenu (3),

v y z n a č u j ú c i s a t ý m, že pred krokom výberu pravidla, aplikovateľného pre údajový pakt, zahrnuje ďalšie kroky:

zberania paketových fragmentov z fragmentovaného paketu, kým sa neprijme hlavička fragmentu uvedeného paketu,

zapamätania informácie, prítomnej v poli hlavičky fragmentu paketu, vo vstupných prostriedkoch, a

odoslania paketových fragmentov, vybavených informáciou hlavičky fragmentu, počnúc hlavičkou fragmentu, pričom každý fragment sa spracuje filtračnými prostriedkami ako regulárny nefragmentovaný paket.

19. Spôsob podľa ktoréhokoľvek z predchádzajúcich nárokov 11 až 18, v y - z n a č u j ú c i s a t ý m, že krok uskutočnenia 2-rozmerného vyhľadávania zdrojových adries a adries miesta určenia paketu zahrnuje ďalší krok:

nájdenia najbližšieho majorantného bodu p v **p** pod normou L_∞, t. j. majorantného bodu $p_i \in \mathbf{p}$ z p, ktorý minimalizuje L_∞-vzdialenosť medzi p_i a p.

20. Ochranná stena podľa nároku 19, v y z n a č u j ú c a s a t ý m, že

zdrojové adresy a adresy miesta určenia sú reprezentované bodom (s, d) $\in$ **U**, kde **U** je 2-rozmerný adresový priestor, reprezentovaný pármi (s, d) celých čísel, vyhovujúcich podmienke $0 \le s < 2^{32}$, $0 \le d < 2^{32}$,

súbor prefixov $\mathbf{P} = \{P_1, P_2, \ldots P_n\}$ je oddielom adresového priestoru **U**, a

každý prefix P_i je logickým pravouholníkom R v adresovom priestore **U**, definovaným $[(s_0, d_0),(s_1, d_1)]$, kde $s_1 - s_0 = s_1 - 2^{i_s} * k_s = 2^{i_s}$ a

$d_1 - d_0 = = d_1 - 2^{i_d} * k_d = 2^{i_d}$ pre niektoré nezáporné celé čísla i_s, i_d, k_s a k_d, pričom uvedený logický pravouholník R je podmnožinou **U**, ktorá vyhovuje podmienke: (s, d) $\in$ R, ak $s_0 \leq s < s_1$, $d_0 \leq d < d_1$, kde (s_0, d_0), $(s_1, d_1) \in$ **U**, a pár bodov $[(s_0, d_0),(s_1, d_1)]$ jednoznačne definuje uvedený pravouholník R,

pre každý prefix $P = [(s_0, d_0), (s_1, d_1)] \in$ **P** je bod $p_0 = (s_0, d_0)$ reprezentantom P a **p** = $\{p_1, p_2,\ldots,p_n\} = \{(s_1, d_1), (s_2, d_2),\ldots, (s_n, d_n),\}$ je množina reprezentantov prefixov v **P**, pričom ak je daný bod $(s_d, d_d) \in$ **U**, pre každý (s, d) $\in$ **U** taký, že $s_d \geq s$ a $d_d \geq d$, (s, d) je majorizovaný bodom (s_d, d_d), a

ak je daný pár bodov (s_1, d_1), $(s_2, d_2) \in$ **U**, vzdialenosť medzi týmito bodmi pod normou L_∞ je daná výrazom:

$$\lim_{k\to\infty} (|s_1-s_2|^k + |d_1-d_2|^{k'})^{1/k} = \max(|s_1-s_2|, |d_1-d_2|)$$

PV2023-2000
09-04-01

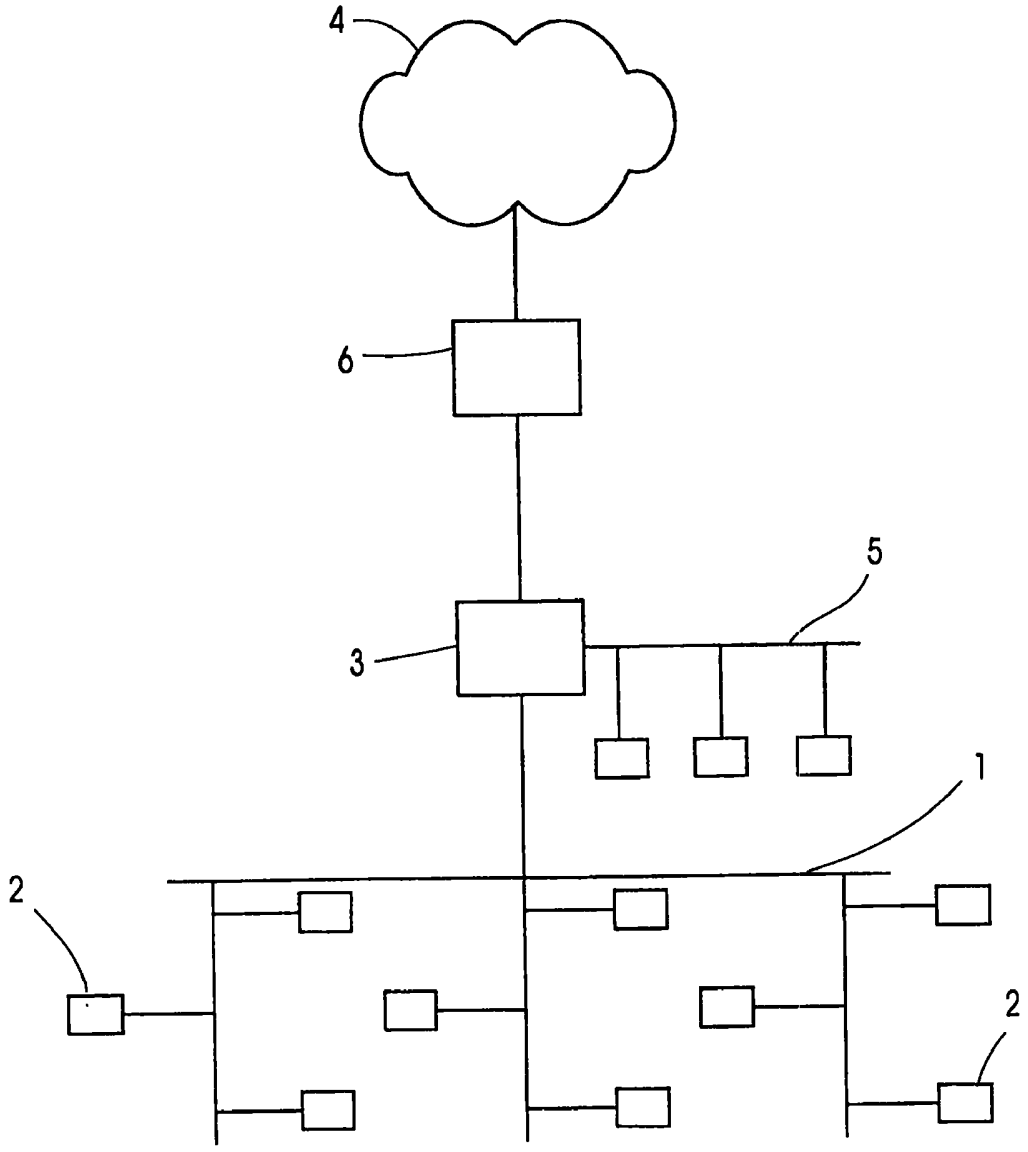


FIG. 1

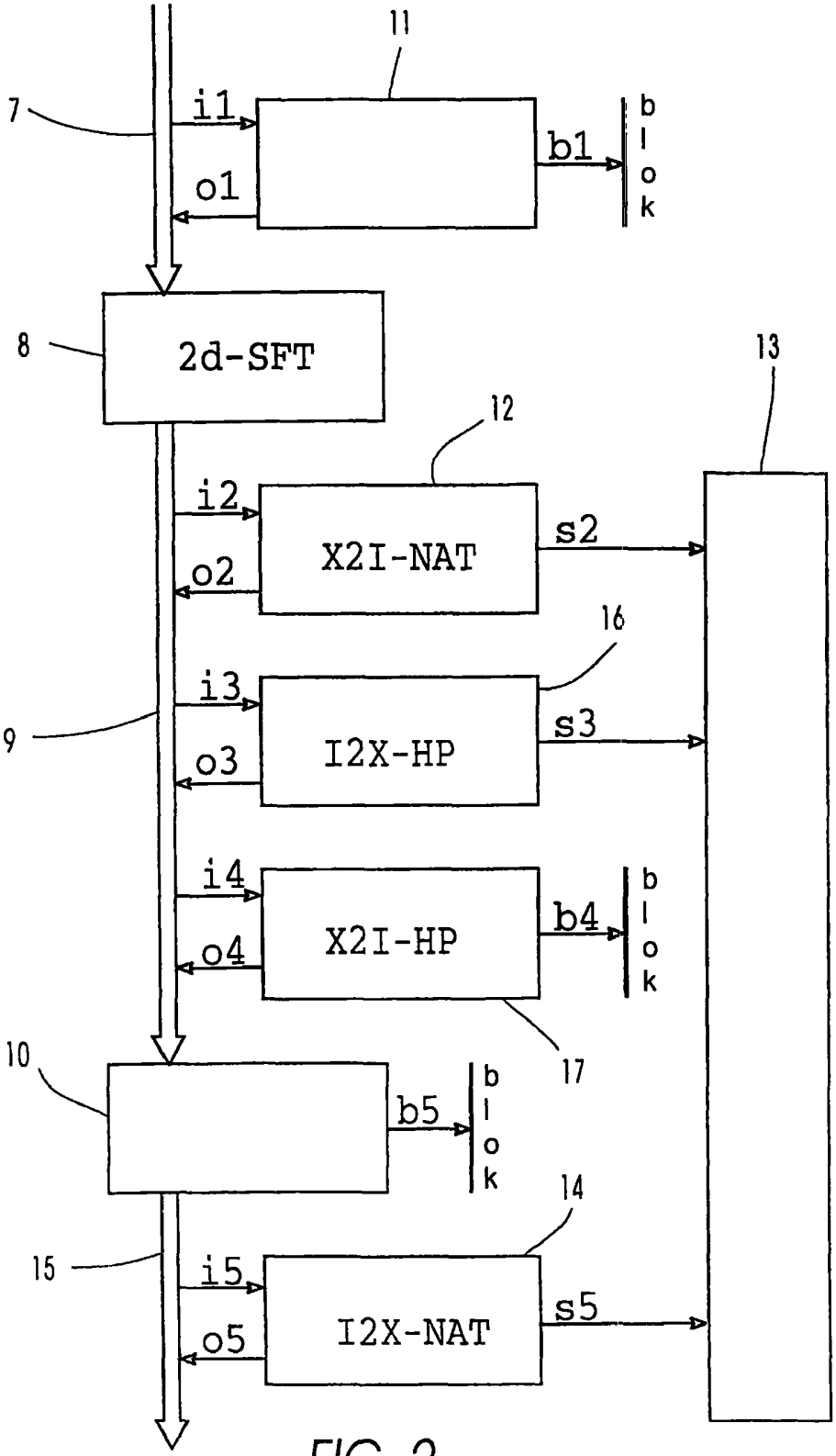

11
7
i1
o1
b1
b
l
o
k
8
2d-SFT
13
12
i2
o2
X2I-NAT
s2
16
i3
9
o3
I2X-HP
s3
i4
o4
X2I-HP
b4
b
l
o
k
17
10
b5
b
l
o
k
14
15
i5
o5
I2X-NAT
s5

FIG. 2

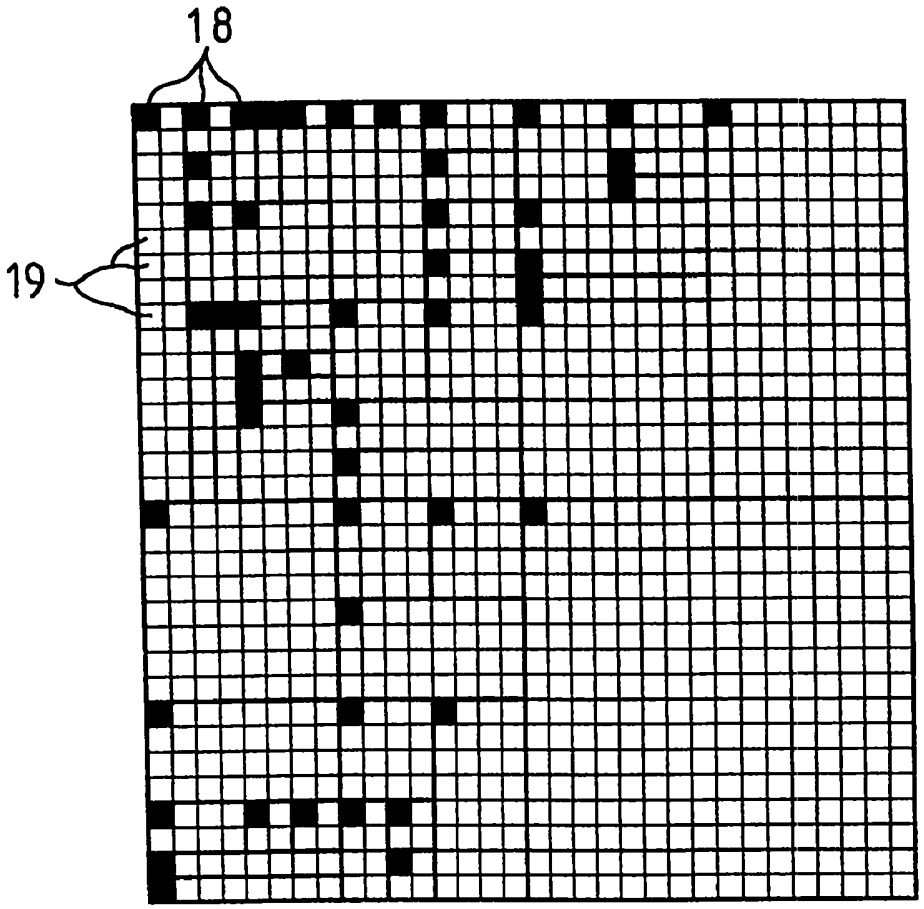


FIG. 3

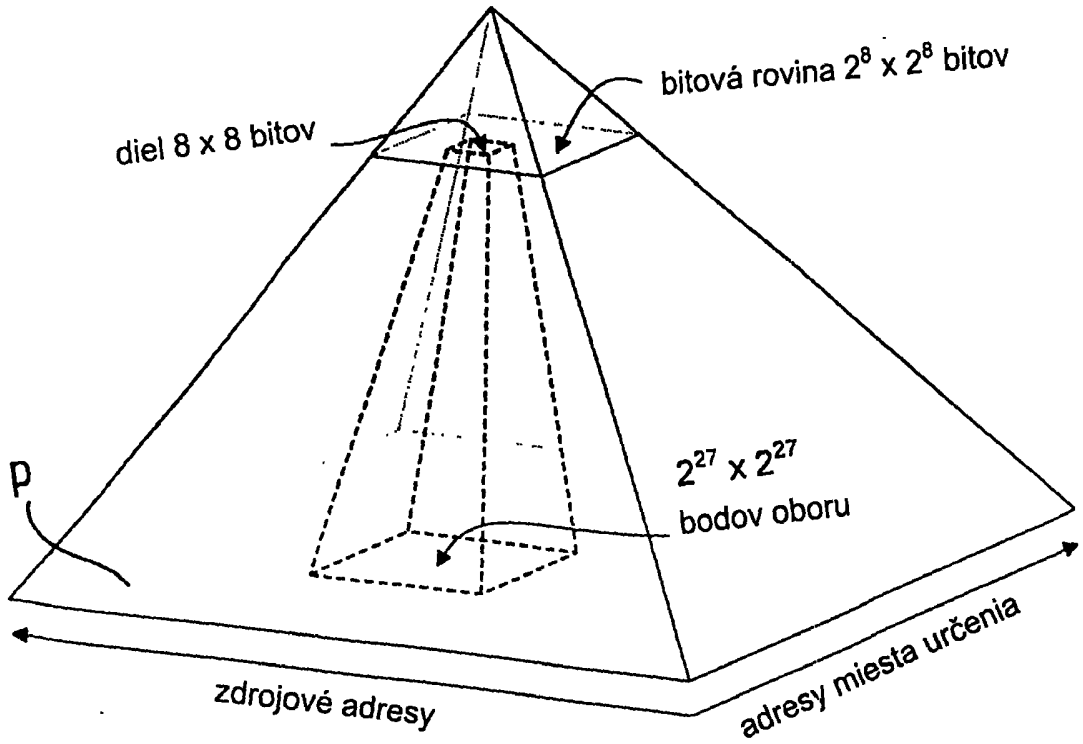

bitová rovina 2^8 x 2^8 bitov
diel 8 x 8 bitov
P
2^{27} x 2^{27}
bodov oboru
zdrojové adresy
adresy miesta určenia

FIG. 4

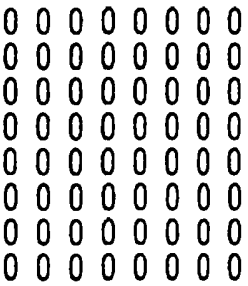


FIG. 5

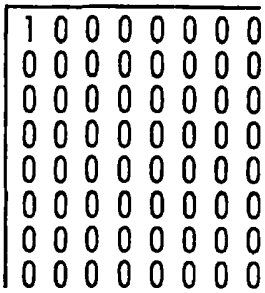


FIG. 6

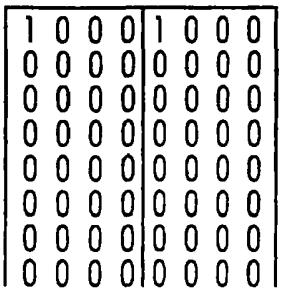


FIG. 7

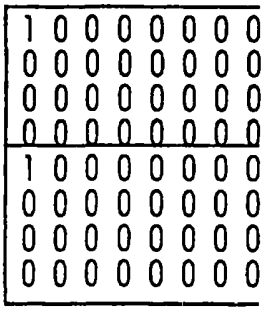


FIG. 8

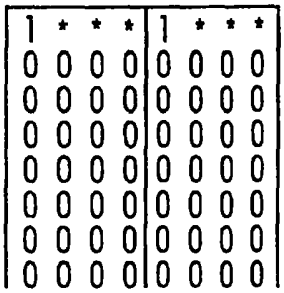


FIG. 9

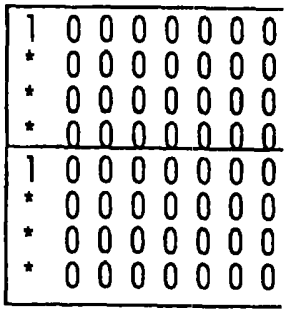


FIG. 10

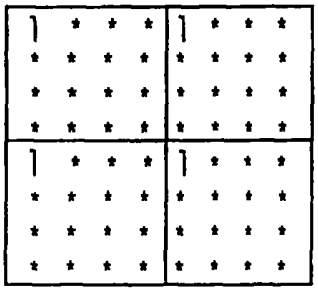


FIG. 11

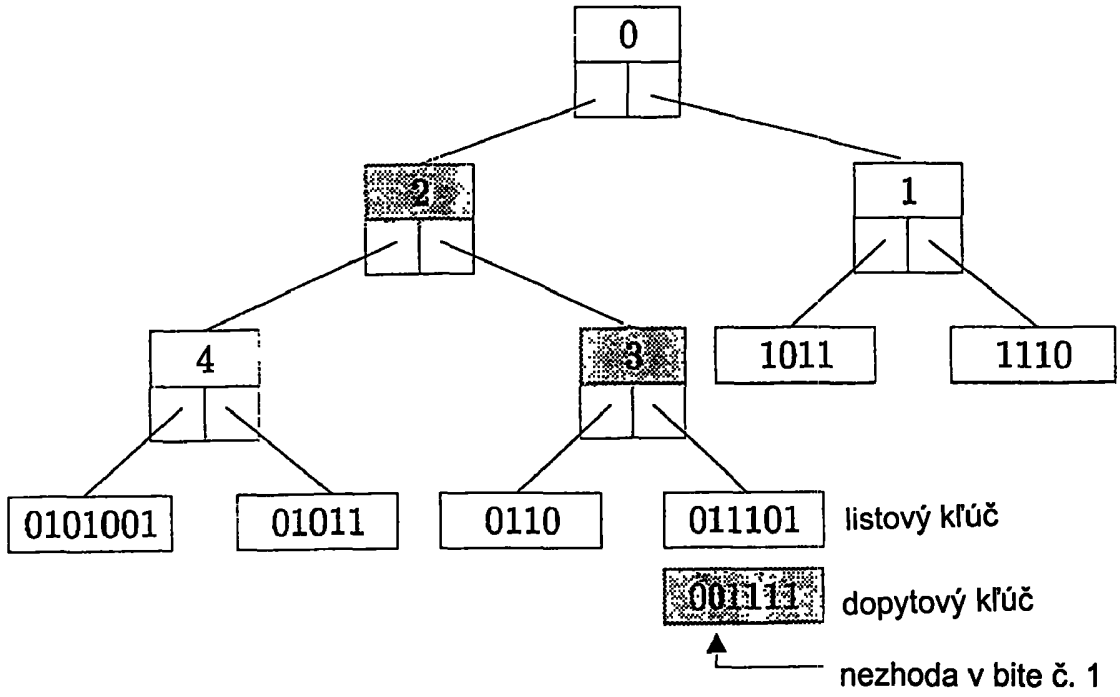

0
2
1
4
3
1011
1110
0101001
01011
0110
011101
listový kľúč
001111
dopytový kľúč
nezhoda v bite č. 1

FIG. 12

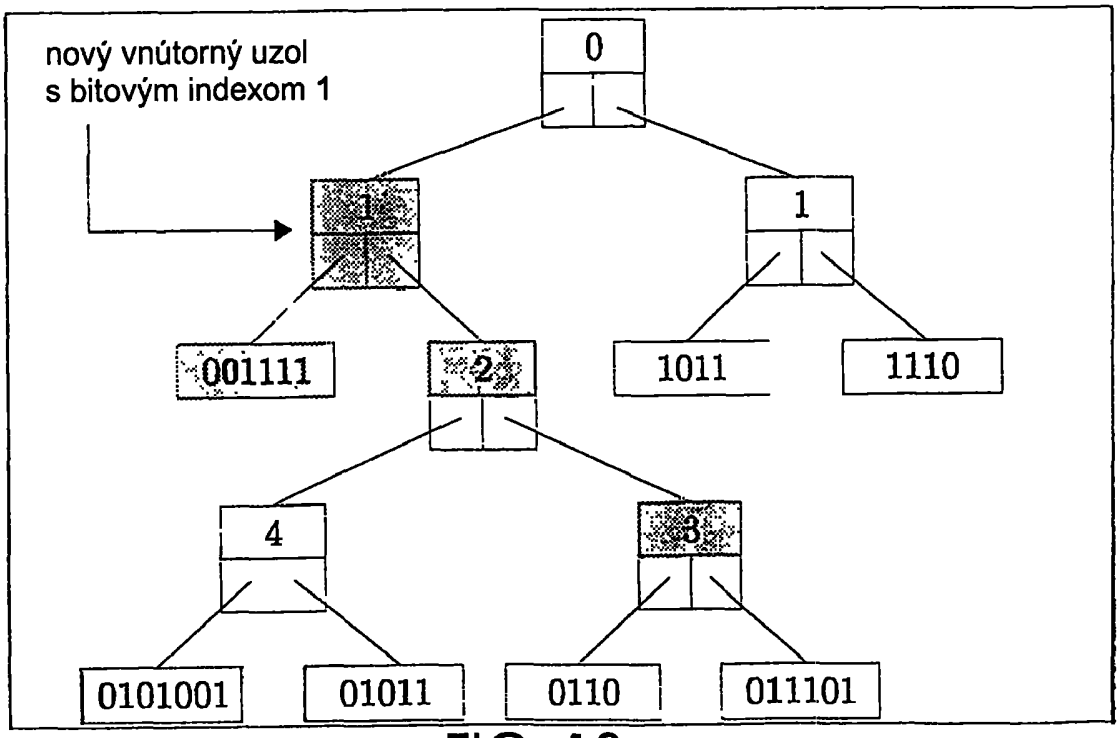

nový vnútorný uzol
s bitovým indexom 1
0
1
1
001111
2
1011
1110
4
3
0101001
01011
0110
011101

FIG. 13