ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 130142 A2**

(51) Int.Cl.
H04W 24/06 (2009.01);
H04W 12/04 (2009.01);
H04L 9/08 (2006.01);

(12) **CERERE DE BREVET DE INVENŢIE**

(21) Nr. cerere: **a 2013 00647**

(22) Data de depozit: **28.08.2013**

(41) Data publicării cererii:
30.03.2015 BOPI nr. **3/2015**

(71) Solicitant:
• **IXIA**, *A CALIFORNIA CORPORATION, 26601 WEST AGOURA ROAD, CALABASAS, CA, US*

(72) Inventatori:
• **CIPU ANDREI**, *STR.SAIDAC GH., NR.7, BL.27, SC.A, AP.8, BUCUREŞTI, B, RO;*
• **BADEA ALEXANDRU R.**, *CALEA CRÂNGAŞI NR.30, BL.50, SC.B, AP.39, BUCUREŞTI, B, RO;*
• **CIOBANU DAN GEORGE**, *STR.BERZELOR NR.47, VASLUI, VS, RO*

(74) Mandatar:
RATZA ŞI RATZA SRL, *B-DUL A.I. CUZA, NR. 52-54, SECTOR 1, BUCUREŞTI*

(54) METODE, SISTEME ŞI SUPORT CARE POATE FI CITIT PE CALCULATOR PENTRU UTILIZAREA CHEILOR DE CRIPTARE PREDETERMINATE ÎNTR-UN MEDIU DE SIMULARE A TESTĂRII

(57) **Rezumat:**

Invenţia se referă la metode, sisteme şi suport citibil pe calculator, pentru efectuarea simulărilor de trafic pachete de date într-un mediu de simulare a testării. Metoda pentru utilizarea datelor de schimbare a cheilor de criptare prestabilite constă în generarea, înainte de iniţierea unei sesiuni de testare pe Internet, prin protocolul de securitate (**IPsec**), a unei chei private şi a unei chei publice la un dispozitiv de imitare trafic, în stocarea cheii private şi a cheii publice într-o unitate de stocare locală, asociată cu dispozitivul de imitare trafic, în preluarea, de la unitatea de stocare locală, a cheii private şi a cheii publice, la iniţierea sesiunii de testare prin protocolul de securitate (**IPsec**) între dispozitivul de imitare trafic şi un dispozitiv supus testării (**DUT**), şi în generarea unei chei secrete partajată, utilizând cheia privată preluată şi o cheie publică recepţionată de la dispozitivul supus testării (**DUT**). Sistemul pentru utilizarea datelor de chei de criptare prestabilite într-un mediu de simulare a testării conţine un dispozitiv supus testării (**DUT**), configurat pentru a genera o cheie publică şi pentru a fi supus unei sesiuni de testare pe Internet, sub protocolul de securitate (**IPsec**), un dispozitiv de imitare trafic, configurat pentru a genera o cheie privată şi o cheie publică, pentru a stoca aceste chei într-o unitate locală de stocare, pentru a prelua aceste chei de la unitatea locală de stocare, şi pentru a genera o cheie secretă partajată, utilizând cheia privată preluată şi o cheie publică, recepţionate de la dispozitivul supus testării (**DUT**).

Revendicări: 23
Figuri: 3

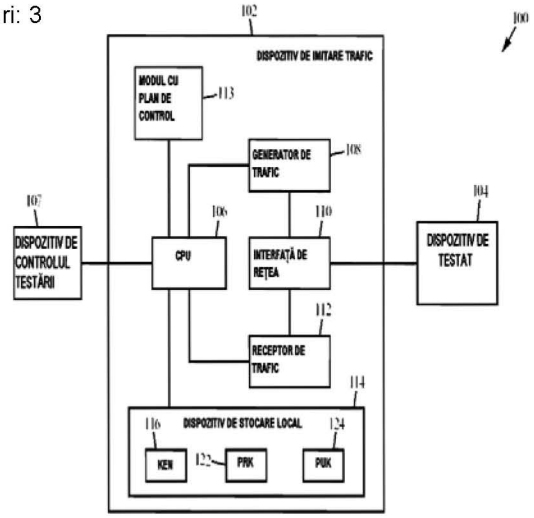

Fig. 1

RO 130142 A2

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2013 00647
Data depozit 28.08.2013

Metode, sisteme şi suport citibil pe calculator pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării

DOMENIUL TEHNIC

Prezenta invenţie se referă la efectuarea simulărilor de trafic pachete de date într-un mediu de simularea testării. Mai precis, prezenta invenţie se referă la metode, sisteme şi suport care poate fi citit pe calculator pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării.

STADIUL ANTERIOR AL TEHNICII

Metoda Diffie-Hellman de schimbarea cheii de criptare este o parte integrantă a procesului de stabilire a canalului de comunicaţie prin protocolul de securitate Internet (IPSec). Cu toate acestea, acest proces de schimbarea cheilor de criptare se contorizează, pentru o cantitate considerabilă de timp de procesare necesară pentru a stabili o cale de comunicaţie prin protocolul IPsec. Concret, este extrem de greu de calculat generarea unei chei private, a unei chei publice şi a unei chei secrete partajată asociată. În ciuda acestui neajuns important, ar trebui să se stabilească, cât mai curând posibil, un număr mare de canale comunicaţie prin protocolul IPsec, într-un mediu de simularea testării. Astfel, orice reducere a timpului asociată cu stabilirea de chei de criptare poate fi extrem de benefică pentru creşterea eficienţei testării. Astfel, există o nevoie de metode, sisteme şi suport care poate fi citit pe calculator pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării.

EXPUNEREA INVENTIEI

Sunt descrise metode, sisteme şi suport care poate fi citit pe calculator pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării. Conform unui exemplu de realizare, o metodă constă în, generarea, înainte de iniţierea unei sesiuni de teste pe Internet sub protocolul de securitate (IPsec), a unei chei private şi a unei chei publice de la un dispozitiv de imitare trafic şi stocarea cheii private şi a cheii publice într-o unitate de stocare locală asociată cu dispozitivul de imitare trafic.

Metoda mai constă în preluarea, de la unitatea de stocare locală, a cheii private şi a cheii publice, la iniţierea sesiunii de testare prin protocolul Ipsec, între dispozitivul de imitare trafic

a-2013-00647
28 -08- 2013

şi un dispozitiv supus testării (DUT) şi în generarea unei chei secrete partajată utilizând cheia privată preluată şi o cheie publică DUT recepţionată de la DUT.

Obiectul prezentei invenţii pentru utilizarea de chei de criptare prestabilite poate fi pus în aplicare în hardware, software, firmware, sau în orice combinaţie a acestora. Ca atare, termenii "funcţie", "modul", "unitate", sau "nod", aşa cum sunt utilizaţi aici, se referă la hardware, care poate include, de asemenea, componentele software şi/sau firmware necesare pentru punerea în aplicare a caracteristicilor ce vor fi descrise în continuare. Conform exemplului de realizare, obiectul prezentei invenţii poate fi implementat folosind un suport citibil de calculator ce are stocate instrucţiuni executabile pe calculator care atunci când sunt executate de procesorul unui calculator comandă realizarea etapelor. Suportul care poate fi citit de calculator adecvat pentru punerea în aplicare a prezentei invenţii include suportul non–tranzitoriu citibil de calculator, cum ar fi dispozitive cu discuri de memorie, dispozitive cu cip de memorie, dispozitive logice programabile şi circuite integrate cu aplicaţii specifice. În plus, un suport care poate fi citit de calculator care implementează prezenta invenţie poate fi dispus pe un singur dispozitiv sau platformă de calcul sau poate fi distribuit în mai multe dispozitive sau platforme de calcul.

DESCRIEREA PE SCURT A DESENELOR EXPLICATIVE

Se vor descrie în continuare exemplele de realizarea prezentei invenţii în legătură cu figurile însoţitoare, în care numerele de referinţă se reprezintă ca părţi, figuri care reprezintă:

Figura 1 prezintă o schemă bloc a unui exemplu de sistem pentru utilizarea chei de criptare prestabilite într- un mediu de simularea testării, în conformitate cu un exemplu de realizarea prezentei invenţii;

Figurile 2A şi 2B prezintă o diagramă de semnalizare care descrie transmiterea de semnale pentru utilizarea cheilor de criptare prestabilite într- un mediu de testare, în conformitate cu un exemplu de realizarea prezentei invenţii; şi

Figurile 3A şi 3B prezintă o organigramă a unei metode pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării, în conformitate cu un exemplu de realizarea prezentei invenţii;

DESCRIEREA DETALIATĂ

Sunt prezentate metode, sisteme şi suport care poate fi citit pe calculator pentru utilizarea cheilor de criptare prestabilite. Conform unui exemplu de realizare, prezenta invenţie implică

a-2013-00647-
28 -08- 2013

calculul, la un dispozitiv de imitare trafic, a unei chei de criptare privată şi a unei chei de criptare publică, care sunt utilizate la o metodă Diffie-Hellman de schimbarea cheii de criptare, înainte de a efectua orice sesiuni de simularea testării (de exemplu, înainte de stabilirea oricărui canal de comunicaţie real prin protocolul IPsec). Cheile de criptare calculate sunt apoi mai târziu preluate la iniţierea unei sau a mai multor sesiuni de testare. Astfel, calculul cheilor de criptare este efectuat o singură dată, pentru a fi utilizate într-o simulare de test care implică o multitudine de canale de comunicaţii prin protocolul Ipsec stabilite. În special, conform prezentei invenţii, se reduce şi se minimizează timpul petrecut pentru calculul cheilor de criptare mari consumatoare de resurse. Astfel, un număr mare de canale de comunicaţii prin protocolul Ipsec poate fi stabilit într-un mediu de simularea testării prin reutilizarea chei de criptare stocate.

Figura 1 este o schemă bloc care prezintă o arhitectură pentru un sistem **100** de simularea testării, conform unui exemplu de realizare a prezentei invenţii. Conform Figurii 1, sistemul **100** include un dispozitiv **102** de imitare trafic care este, din punct de vedere al comutaţiei, conectat la un dispozitiv **101** de controlul testării şi un dispozitiv **104** de testat (DUT). Conform unor exemple de realizare, DUT **104** poate include o poartă de acces de servire (SGW), o poartă de acces reţea de pachete de date (PGW), un dispozitiv de protecţie de tip firewall, un router, sau orice dispozitiv sau sistem care ar putea beneficia de teste de simulare trafic cu randament ridicat. Conform unui exemplu de realizare, DUT **104** poate fi conectat din punct de vedere al comunicaţiei la dispozitivul **102** de imitare trafic printr-o conexiune prin cablu fără fir, care facilitează transferul traficului de pachete de date criptate.

Conform unor exemple de realizare, dispozitivul **102** de imitare trafic poate include un dispozitiv sau un echipament hardware care este configurat pentru a genera şi transmite traficul de pachete de date la DUT **104** în scopuri de testare propuse. Conform unui exemplu de realizare, dispozitivul **102** de imitare trafic poate include un procesor **106**, o unitate generator de trafic **108**, o unitate interfaţă de reţea **110**, o unitate receptor de trafic **112**, un modul cu plan de control **113** şi unitatea de stocare locală **114**. Procesorul **106** poate include o unitate centrală de procesare (CPU), un microcontroler, sau orice altă unitate de procesare bazată pe hardware care configurată pentru a gestiona şi a executa modulele **108-114** în dispozitivul **102** de imitare trafic. Procesorul **106** poate, de asemenea, include o unitate de memorie şi diferite unităţi specializate, circuite, software şi interfeţe pentru furnizarea funcţionalităţilor şi caracteristicilor descrise îm prezenta invenţie. Conform unor alte exemple

a-2013-00647
28 -08- 2013

de realizare, dispozitivul **102** de imitare trafic poate funcţiona fie ca o entitate client fie ca o entitate server.

Conform unor exemple de realizare, unitatea generator de trafic **108** poate include un modul voce, care poate fi configurat pentru a genera date de trafic audio, şi un modul video, care poate fi configurat pentru a genera date de trafic video. Într- unul dintre exemple, modulul voce poate include un modul pe bază de software (executat de procesorul **106** al unui hardware), care este configurat pentru a genera date tip voce pe baza traficului simulat pe un anumit protocol L4-L7. De exemplu, unitatea **108** generator de trafic poate fi configurată să genereze date prin protocolul de transport în timp real (real-time transport protocol RTP), date care sunt în cele din urmă transmise la DUT **104**. În plus, unitatea **108** generator de trafic poate fi configurată pentru a cripta traficul de pachete generat, aşa cum ar fi prin utilizarea protocolului de securitate IPsec. Traficul de pachete generat şi criptat prin unitatea **108** generator de trafic poate fi transmis la reţea unitatea **110** interfaţă de reţea.

Conform unelor exemple de realizare, unitatea **110** de interfaţă de reţea poate converti traficul de pachete test de ieşire de la unitatea **108** generator de trafic într-un format de semnal electric, optic, sau wireless de semnal care este necesar pentru a transmite traficul de testare la DUT **104** prin intermediul unei conexiuni prin cablu, fibră optică, wireless, sau un alte conexiuni de comunicaţie similare. De asemenea, unitatea **110** de interfaţă de reţea poate recepţiona semnale electrice, optice sau wireless de la DUT **104** şi pot fi configurată pentru a converti semnalele primite în interiorul traficului de testare de intrare într-un format utilizabil (de exemplu, pachete de date) prin dispozitivul **102** de imitare trafic. Pachetele recepţionate pot fi transmise prin unitatea **110** de interfaţă de reţea la unitatea **112** receptor de trafic.

Conform unelor exemple de realizare, unitatea **112** receptor de trafic poate recepţiona traficul test de intrare de la unitatea **110** de interfaţă de reţea. Unitatea **112** receptor de trafic poate fi configurată să determine dacă fiecare pachet de date recepţionat este un element al unul flux de date specific, şi poate acumula statisticile de testare pentru fiecare flux, în conformitate cu instrucţiunile de testare oferite de procesorul **106**. Statisticile de testare acumulate pot include, de exemplu, numărul total de pachete recepţionate, numărul de pachete recepţionate în afara secvenţei, numărul de pachete de date recepţionate cu erori, întârzierea de propagare maximă, medie şi minimă, şi alte statistici pentru fiecare flux. Unitarea **112** receptor de trafic poate oferi, de asemenea, statistici de testare şi/sau pachetele capturate de la procesorul **106** pentru analize suplimentare, în timpul sau după sesiunea test. Conform unor exemple de realizare,

unitatea **112** receptor de trafic poate fi de asemenea configurată pentru a decripta traficul de pachete recepţionat de la DUT **104**.

Conform exemplului de realizare, modulul **113** cu plan de control poate include un modul cu plan de control prin protocolul de comunicaţie (GTP) pentru serviciul general de pachete de date radio (GPRS) care este configurat pentru a efectua negocierea asociată cu stabilirea canalelor de comunicaţie prin protocolul IPSec, într-o sesiune test. Conform unor exemple de realizare, sesiunea test prin protocolul IPsec se desfăşoară între un dispozitiv de imitare trafic şi un DUT, la un strat de reţea. De exemplu, modulul **113** cu plan de control poate comunica cu DUT **104** pentru a stabili o multitudine de sesiuni prin protocolul Ipsec, care pot fi utilizate pentru a comunica trafic de date media criptat.

Conform unor exemple de realizare, procesorul **106** poate fi configurat să comunice cu dispozitivul **101** de control testare. Dispozitivul **101** de control testare poate fi un dispozitiv de calcul conţinute în, sau extern la, dispozitivul **102** de imitare trafic. Dispozitivul **101** de control testare poate furniza procesorului **106** instrucţiunile şi datele utilizate de dispozitivul **102** de imitare trafic, pentru realizarea testării de către DUT **104**. Instrucţiunile şi datele primite de dispozitivul **102** de imitare trafic de la dispozitivul **101** de control testare pot include, de exemplu, definiţiile fluxurilor de pachete de date pentru a fi generate de dispozitivul **102** de imitare trafic şi definiţiile statisticilor de performanţă care pot fi acumulate şi raportate de dispozitivul **102** de imitare trafic. Conform unui exemplu de realizare, dispozitivul **101** de control testare poate fi utilizat de un operator de reţea, un administrator de simulare testare sau orice alt utilizator, pentru a iniţia şi/sau a stabilii parametrii de simulare testare trafic care implică dispozitivul **102** de imitare trafic şi DUT **104**.

Conform unor exemple de realizare, unitatea de stocare locală **114** poate include o memorie, o unitate de stocare bazată pe hardware, o bază de date sau orice altă unitate locală, care este capabilă de stocare electronică de informaţii. De exemplu, unitatea de stocare locală **114** poate fi amplasată în dispozitivul **102** de imitare trafic. Aşa cum se arată în figura 1, unitatea de stocare locală **114** poate fi utilizată pentru a stoca una sau mai multe chei private **122**, una sau mai multe chei publice **124**, unul sau mai multe numere **116** de schimbarare de chei de criptare, şi altele asemenea.

Conform unor exemple de realizare, dispozitivul **101** de control testare poate fi utilizat de către un operator de testare reţea pentru a oferi numere de schimbare cheii de criptare la dispozitivul **102** de imitare trafic. Ca răspuns, dispozitivul **102** de imitare trafic poate fi

configurat să utilizeze numerele de schimbarea cheii de criptare recepţionate pentru a calcula cheile private şi/sau publice. În special, determinarea de chei publice şi private este realizată înainte de a stabili o sesiune de testare cu DUT **104**. Dispozitivul **102** de imitare trafic poate astfel stoca ulterior cheile publice şi private calculate în unitatea de stocare **114** locală pentru o utilizare ulterioară, la stabilirea unei sesiuni de testare cu DUT **104**. Dispozitivul **102** de imitare trafic poate fi configurat pentru a stoca numerele de schimbarea cheii înainte sau după calcularea cheilor publice şi private.

La iniţierea unei sesiuni de teste cu DUT **104**, dispozitivul **102** de imitare trafic poate fi configurat pentru a prelua cheile publice şi private calculate anterior, care sunt stocate în unitatea de stocare **114** locală. Prin preluarea cheilor publice şi private, dispozitivul **102** de imitare trafic este capabil de a conserva resursele de procesare valoroase, care sunt de obicei necesare pentru a determina cheile de criptare, la momentul constituirii unui canal de comunicaţie prin protocolul IPsec asociat cu o sesiune de testare.

După ce un canal de comunicaţie prin IPSec este negociat şi stabilit prin unitatea **113** cu plan de control, dispozitivul **102** de imitare trafic poate fi configurat să genereze trafic criptat de pachete de date (de exemplu, un flux de pachete de date). De exemplu, datele de trafic criptate pot include date de trafic RTP criptate prin IPsec. Conform unui exemplu de realizare, unitatea **108** generator de trafic poate fi determinată de dispozitivul **101** de control testare să înceapă generarea datelor de trafic necesare pentru sesiunea de testare.

După ce dispozitivul **102** de imitare trafic stabileşte canal de comunicaţie prin IPsec pentru comunicarea de date de tip fascicul media la DUT **104**, dispozitivul **102** de imitare trafic poate cripta datele din traficul de pachete şi datele din traficul de pachete criptate sunt transmise de unitatea **110** de interfaţă reţea. Unitatea **110** de interfaţă reţea transmite ulterior traficul de pachete criptat la DUT **104** prin intermediul canalului de comunicaţie IPsec stabilit. Conform exemplului de realizare, datele de trafic simulat sunt criptate şi pachetizate înainte de a fi trimise pe canalul de comunicaţie stabilit, la DUT **104**.

O prezentare cu privire la modul în care aceste chei de criptare prestabilite sunt utilizate este redată în Figurile 2A şi 2B. În special, Figurile 2A şi 2B prezintă o diagramă de semnalizare care descrie transmiterea de semnale pentru utilizarea cheilor de criptare prestabilite într-un mediu de testare, în conformitate cu un exemplu de realizarea prezentei invenţii. În linia 1, dispozitivul **102** de imitare trafic stabileşte sau determină numerele de schimbarea cheii de criptare (de exemplu, "p" şi "g"), care pot fi eventual utilizate în simularea de testare cu DUT **104**. Conform exemplului de realizare, numărul "g" de schimbarea cheii poate avea o valoare

prestabilită (de exemplu, g = 2), care este cunoscută şi utilizată atât de dispozitivul **102** de imitare trafic cat şi de DUT **104**. Alternativ, dispozitivul **101** de control al traficului poate fi folosit pentru a atribui o valoare numărului de schimbarea cheii "g". Similar, dispozitivul **101** de controlul testării poate fi de asemenea utilizat pentru a selecta unul sau mai multe numere de schimbarea cheii de criptare "p_1-p_n" care sunt susceptibile de a fi compatibile cu, şi suportate de DUT **104**. Conform unor exemple de realizare, unul sau mai multe numere de schimbarea cheii potenţiale pot fi stocate ca şi numere de schimbarea cheii **116** stocate în uitatea **114** de stocare locală.

În linia 2, dispozitivul **102** de imitare trafic generează o cheie privată. Într-un anumit caz, dispozitivul **102** de imitare trafic poate genera o cheie privată "a" înainte de iniţierea unei sesiuni de testare.

În linia 3, dispozitivul **102** de imitare trafic generează o cheie publică. Într-unul din cazuri, dispozitivul **102** de imitare trafic poate genera o cheie publică "A" înainte de iniţierea unei sesiuni de testare.

În linia 4, dispozitivul **102** de imitare trafic stochează cheia privată şi cheia publică. Într-un exemplu de realizare, dispozitivul **102** de imitare trafic stochează cheia privată "a" şi cheia publică "A" în unitatea de stocare locală, cum ar fi memoria, sau într-o bază de date locală, înainte de iniţierea unei sesiuni de testare.

În linia 5, dispozitivul **102** de imitare trafic iniţiază o sesiune de testare cu DUT **104**. În acest moment, DUT **104** poate genera, de asemenea, o cheie privată "b".

În linia 6, dispozitivul **102** de imitare trafic preia cheia privată şi cheia publică pentru a fi utilizate în sesiunea de testare iniţiată. Într-un exemplu de realizare, dispozitivul **102** de imitare trafic preia cheia privată "a" şi cheia publică "A" de la unitatea de stocare **114**.

În linia 7, dispozitivul **102** de imitare trafic transmite cheia publica "A" şi unul sau mai multe numere de schimbarea cheii de criptare (de exemplu, numerele de schimbarea cheii de criptare "p_1-p_5") la DUT **104**. În acest exemplu, numărul p_1 de schimbarea cheii este asociat cu (şi a fost folosit pentru a genera) cheia de schimbarea cheii publice "A".

În linia 8, DUT **104** utilizează unul dintre numerele de schimbarea cheii recepţionate (de exemplu, "p_1") pentru a genera o cheie publică "B". Într-um exemplu de realizare, DUT **104** determină dacă "p_1" este compatibilă cu şi susţinută de DUT **104,** în scopul testării. Dacă "p_1" nu este acceptată sau utilizabilă de către DUT **104**, atunci DUT **104** poate selecta oricare unul dintre numerele de schimbarea cheii recepţionate (de exemplu, p_2-p_5). Dacă nici unul dintre numerele "p" transmise de dispozitivul **102** de imitare trafic nu este utilizabil de către DUT

a-2013-00647-
28 -08- 2013

104, DUT **104** poate contacta dispozitivul **102** de imitare trafic pentru a solicita un alt număr "p" de schimbare cheii de criptare.

În linia 8, DUT **104** generează o cheie publică "B". Concret, odată ce DUT **104** determină o valoare "p" acceptabilă (de exemplu, p_1), DUT **104** poate genera o cheie publică "B" folosind numere de schimbarea cheii de criptare, cum ar fi valorile "p_1" şi "g".

În linia 9, DUT **104** furnizează cheia publică B dispozitivului **102** de imitare trafic. În linia 10, atât dispozitivul **102** de imitare trafic cat şi DUT **104** sunt configurate pentru a genera o cheie secretă partajată. De exemplu dispozitivul **102** de imitare trafic poate utiliza cheia publică "B" primită pentru a calcula cheia secretă partajată "s_{TE}", unde $s_{TE} = B^a \bmod p$, unde mod este o operaţie matematică de modul. De asemenea, DUT **104** poate utiliza cheia publică "A" repţionată pentru a calcula cheia secretă "s_{DUT}" partajată, unde $s_{DUT} = A^b \bmod p$. În special, s_{TE} este egală cu s_{DUT}.

În linia 11, este stabilit un canal de comunicaţie securizat prin protocolul IPSec. Conform unui exemplu de realizare, dispozitivul **102** de imitare trafic şi DUT **104** utilizează cheia secretă partajată pentru cererea de comunicaţie de schimb şi pentru mesaje de răspuns comunicaţie pentru a stabili o primă comunicaţie prin IPsec între dispozitivul **102** de imitare trafic şi DUT **104**.

În linia 12, dispozitivul **102** de imitare trafic iniţiază o nouă sesiune prin protocolul Ipsec (de exemplu, a doua sesiune IPsec) cu DUT **104**. Conform unor exemple de realizare, dispozitivul **102** de imitare trafic preia cheia privată prestabilită “a” şi cheia publică "A" din memoria locală. În unele exemple de realizare, recuperarea cheii private stocate şi a cheii publice se poate baza pe momentul în care aceleaşi numere de schimbarea cheii vor fi utilizate pentru a stabili canalele de comunicaţie IPsec ulterioare în simularea testării. Similar, un DUT poate fi configurat pentru a genera o noua cheie publică şi o nouă cheie privată, în cazul în care o nouă sesiune IPsec este iniţiată. De exemplu, DUT **104** poate genera o nouă cheie privată "b2" şi o nouă cheie publică "B2".

În liniile 13 şi 14, cheile publice sunt schimbate între dispozitivul **102** de imitare trafic şi DUT **104**. Mai precis, dispozitivul **102** de imitare trafic transmite cheia publică prestabilită "A" la DUT **104** şi DUT **104** transmite o nouă cheie publică "B2" la dispozitivul **102** de imitare trafic.

În linia 15, atât dispozitivul **102** de imitare trafic cat şi DUT **104** sunt fiecare configurate să genereze o cheie secretă partajată. De exemplu, dispozitivul **102** de imitare trafic poate utiliza cheia publică "B" recepţionată pentru a calcula cheia secretă partajată "s_{TE}", unde $s_{TE} = B^a$

mod p. Similar, DUT **104** poate utiliza cheia publică "A" recepţionată pentru a calcula cheia secretă "s_{DUT}" partajată, unde $s_{DUT} = A^b$ mod p. Aşa cum este indicat mai sus, s_{TE} trebuie să fie egală s_{DUT}.

În linia 16, este stabilit un al doilea canal de comunicaţie securizat IPSec. Conform unui exemplu de realizare, dispozitivul **102** de imitare trafic şi DUT **104** utilizează cheile secrete partajate pentru cereri de schimbarea canalului de comunicaţie şi mesaje de răspuns canal de comunicaţie pentru a stabilii un al doilea canal de comunicaţie securizat prin IPsec între dispozitivul **102** de imitare trafic şi DUT **104**.

Figurile 3A şi 3B prezintă o organigramă a unei metode pentru utilizarea cheilor de criptare prestabilite într-un mediu de simularea testării, în conformitate cu un exemplu de realizarea prezentei invenţii. În etapa **302**, sunt stabilite numere de schimbarea cheii de criptare. Conform unor exemple de realizare, dispozitivul de imitare trafic poate determina o multitudine de diferite numere de schimbare cheie care pot fi, eventual, utilizate într-un test de simulare trafic. În special, această etapă se efectuează înainte ca orice sesiuni de testare să fie iniţiate sau stabilite. În unele exemple de realizare, un număr de schimbare cheie de criptare "g" poate fi setat la o valoare numerică care este cunoscut de către toate DUT-urile, cum ar fi g = 2. În ceea ce priveşte numărul "p" de schimbare cheie, dispozitivul de imitare trafic poate furniza unităţii de stocare locală (de exemplu, memoria locală sau o bază de date locală) o multitudine de valori "p". În special, unitatea de stocare locală poate conţine orice număr de valori "p", fiecare dintre ele este mapată la o cheie privată corespunzătoare şi la o cheie publică corespunzătoare, chei care au fost prestabilite şi/sau precalculate.

În etapa **304**, este generată cel puţin o cheie privată prin dispozitivul de imitare trafic. În unele exemple de realizare, dispozitivul de imitare trafic poate genera propria cheie privată "a", care este cunoscută doar de dispozitivul de imitare trafic.

În etapa **306**, este generată cel puţin o cheie publică de dispozitivul de imitare trafic. În unele exemple de realizare, dispozitivul de imitare trafic generează o cheie publică folosind unul sau mai multe numere de schimbare cheie (de exemplu, "p" şi "g") şi o cheie privată generată anterior de dispozitivul de imitare trafic (vezi etapa **304**). De exemplu, dispozitivul de imitare trafic poate genera o cheie publică "A", unde A este egală cu produsul dintre g^a şi mod p, unde mod este o operaţie matematică de modul (de exemplu, $A=g^a$ mod p). Conform unor exemple de realizare, dispozitivul de imitare trafic poate fi prevăzut cu o pluralitate de valori cunoscute "p", care pot fi utilizate în cursul unui test de simulare trafic. În astfel de cazuri,

a-2013-00647
28 -08- 2013

dispozitivul de imitare trafic, poate genera o cheie publică unică pentru fiecare din multitudinea de valori cunoscute "p".

În etapa **308** sunt stocate cel puţin o cheie privată şi cel puţin o cheie publică. În unele exemple de realizare, dispozitivul de imitare trafic stochează cheia(cheile) privată(e) şi cheia(cheile) publică(e) în unitatea de stocare locală în dispozitivul de imitare trafic. De exemplu, dispozitivul de imitare trafic poate fi configurat să stocheze fiecare dintre cheile publice şi private asociate, împreună cu o valoare corespunzătoare "p" într-o bază de date locală în dispozitivul de imitare trafic.

În etapa **310**, se face o determinare pentru a stabili dacă să se iniţieze o sesiune de testare. În unele exemple de realizare, această decizie poate fi făcută de un operator de reţea folosind un dispozitiv de controlul testării (de exemplu, dispozitivul de control testare **101** în figura1). În cazul în care o sesiune de teste IPSec este iniţiată şi realizată între dispozitivul de imitare trafic şi DUT, metoda **300** continuă la etapa **312**. Altfel, metoda **300** se termină.

In etapa **312**, cheia privată stocată şi cheia publică sunt preluate unitatea de stocare locală. Conform unui exemplu de realizare, dispozitivul de imitare trafic obţine cheia privată stocată a clientului şi cheia publică a serverului din memoria locală de pe dispozitivul de imitare trafic.

În etapa **314**, cheia publică şi cel puţin un număr de schimbarea cheii de criptare sunt furnizate la DUT. În unele exemple de realizare, dispozitivul de imitare trafic poate transmite la DUT, un mesaj care conţine o multitudine de valori p, împreună cu o cheie publică care corespunde cu cel puţin cu una dintre valorile p. De exemplu, dispozitivul de imitare trafic poate transmite valorile p_1, p_2, p_3, p_4 şi p_5 posibile împreună cu cheia publică A_1 (care este asociat cu p_1). La primirea mesajului care conţine valorile posibile p, DUT face o determinare dacă p_1 poate fi utilizat pentru simularea testării. Dacă p_1 poate fi utilizat de către DUT, atunci acesta utilizează p_1 şi valoarea g cunoscută anterior pentru a genera o cheie publică B. Într-un exemplu de realizare, cheia publică B este egală cu g^b mod p, unde b este egal cu o cheie privată generată de DUT.

Dacă p_1 nu poate fi utilizat (de exemplu, incompatibil) prin DUT, atunci DUT determină dacă unul dintre p_2, p_3, p_4, p_5 pot fi folosite în simularea de testare. În cazul în care se determină că unul dintre unul dintre p_2, p_3, p_4 şi p_5 pot fi folosite, atunci DUT transmite un mesaj la dispozitivul de imitare trafic care indică o valoare p selectată de DUT. În unele exemple de realizare, DUT poate transmite, de asemenea, o valoare B a cheii publice asociată cu valoarea p selectată în mesajul către dispozitivul de imitare trafic. Dacă se constată că nici unul dintre

a-2013-00647-
28-08-2013

p_1, p_2, p_3, p_4, p_5 nu poate fi folosit de DUT, atunci DUT transmite un mesaj la dispozitivul de imitare trafic, mesaj care indică faptul că toate valorile p furnizate anterior sunt incompatibile.

În etapa **316**, o cheie publică este recepţionată de la DUT. După cum se indică mai sus, DUT poate utiliza o cheie privată, valoarea p_1 primită de la dispozitivul de imitare trafic şi valoarea g cunoscută anterior pentru a genera o cheia publică B. La generarea cheii publice B, DUT o poate transmite dispozitivului de imitare trafic.

În etapa **318**, se generează o cheie secretă partajată. În unele exemple de realizare, dispozitivul de imitare trafic utilizează cheia sa privată (de exemplu, cheia privată "a") şi cheia publică DUT recepţionată (de exemplu, cheia publică "B"), pentru a determina o cheie secretă partajată "s", în cazul în care s este egală cu produsul dintre B^a şi mod p. Similar, DUT poate utiliza propria cheie privată şi cheia publică recepţionată de la dispozitivul de imitare trafic pentru a determina, de asemenea, cheia secretă partajată s, unde s în acest caz este determinat prin produsul dintre A^b şi mod p. În special, cheia secretă s partajată generată atât de dispozitivul de imitare trafic cat şi de DUT este respectiv egală cu B^a mod p şi A^b mod p.

În etapa **320**, este stabilit canalul de comunicaţie prin protocolul IPsec. Într-un exemplu de realizare, fiecare dispozitiv de imitare trafic şi DUT utilizează cheia sa partajată secretă pentru a finaliza negocierile de stabilirea sesiunii de comunicaţii prin IPsec.

În etapa **322**, se face o determinare pentru a stabili dacă o altă sesiune de testare urmează să fie iniţiată. De exemplu, dispozitivul de imitare trafic determină dacă un canal de comunicaţie IPsec ulterioar urmează să fie stabilit între dispozitivul de imitare trafic şi DUT. Dacă este aşa, atunci metoda **300** se întoarce la etapa **312**. Altfel, metoda **300** se termină.

Se va înţelege că diferite detalii ale prezentei invenţii dezvăluite în descrierea de mai sus pot fi schimbate fără a se îndepărta de la scopul protecţiei. În plus, descrierea de mai sus este numai în scopul de a ilustra şi nu în scopul limitării.

a-2013-00647
28 -08- 2013

61

REVENDICĂRI

Ceea ce se revendică este:

1. Metodă pentru utilizarea datelor de schimbarea cheilor de criptare prestabilite într-un mediu de simularea testării care constă în:

generarea, înainte de iniţierea unei sesiuni de testare pe Internet prin protocolul de securitate (IPsec), a unei cheie private şi a unei chei publice la un dispozitiv de imitare trafic;

stocarea cheii private şi cheii publice într-o unitate de stocare locală asociată cu dispozitivul de imitare trafic; şi

preluarea, de la unitatea de stocare locală, a cheii private şi a cheii publice, la iniţierea sesiunii de testare prin protocolul IPsec între dispozitivul de imitare trafic şi un dispozitiv supus testării (DUT);

generarea unei chei secrete partajată utilizând cheia privată preluată şi o cheie publică DUT recepţionată de la DUT.

2. Metodă, conform revendicării 1, caracterizată prin aceea că determinarea, înainte de generarea cheii publice, a cel puţin un număr de schimbare cheie de criptare.

3. Metoda conform revendicării 2, caracterizată prin aceea că generarea de cheie publică include regăsirea cheii publice folosind cel puţin un număr de schimbare cheie de criptare.

4. Metodă, conform revendicării 3, caracterizată prin aceea că mai constă în transmiterea cheii publice şi a cel puţin un număr de schimbare cheie de criptare la DUT.

5. Metodă, conform revendicării 1, caracterizată prin aceea că mai constă în recepţionarea unei chei publice DUT de la dispozitivul DUT, la iniţierea sesiunii de testare prin protocolul IPsec.

6. Metodă, conform revendicării 1, caracterizată prin aceea că sesiunea de testare IPsec se efectuează între dispozitivul de imitare trafic şi DUT, la un strat de reţea.

7. Metodă, conform revendicării 1, caracterizată prin aceea că dispozitivul de imitare trafic funcţionează fie ca o entitate client fie ca o entitate server.

8. Metodă, conform revendicării 1, caracterizată prin aceea că menţionata cheie publică este generată folosind cheia privată şi cel puţin un număr de schimbarea cheii de criptare.

a-2013-00647
28 -08- 2013

9. Metodă, conform revendicării 1, caracterizată prin aceea că, fiecare dintre cheile privată, publică şi secretă partajată este generată folosind o metodă Diffie-Hellman.

10. Metodă, conform revendicării 1, caracterizată prin aceea că DUT include cel puţin unul dintre: un dispozitiv de protecţie de tip firewall, un router, o poartă de acces de servire (SGW) şi o poarta de acces reţea de pachete de date (PGW).

11. Metodă, conform revendicării 1, caracterizată prin aceea că mai constă în preluarea, la dispozitivul de imitare trafic, a cheii private şi a cheii publice, din memoria locală la iniţierea unei a doua sesiuni de testare prin protocolul Ipsec, între dispozitivul de imitare trafic şi DUT, şi generarea unei a doua chei secretă partajată folosind cheia privată preluată şi o a doua cheie publică DUT recepţionată de la dispozitivul DUT.

12. Sistem pentru utilizarea datelor de chei de criptare prestabilite într-un mediu de simularea testării, care conţine:

un dispozitiv de testat (DUT) configurat pentru a genera o cheie publică DUT şi pentru a fi supus unei sesiuni de testare pe Internet sub protocolul de securitate (IPsec); şi

un dispozitiv de imitare trafic configurat pentru a genera, înainte de iniţierea sesiunii de testare prin IPsec cu DUT, o cheie privată şi o cheie publică, pentru a stoca cheia privată şi cheia publică într-o unitate locală de stocare, pentru a prelua cheia privată şi cheia publică de la unitatea locală de stocare la iniţierea sesiunii de testare IPsec, şi pentru a genera o cheie secretă partajată utilizând cheia privată preluată şi o cheie publică DUT recepţionate de la DUT.

13. Sistem, conform revendicării 12, caracterizat prin aceea că dispozitivul de imitare trafic este în plus configurat pentru a determina, înainte de generarea cheii publice, a cel puţin un număr de schimbarea cheii de criptare.

14. Sistem, conform revendicării 13, caracterizat prin aceea că dispozitivul de imitare trafic este în plus configurat pentru a obţine cheia publică utilizand cel puţin un număr de schimbarea cheii de criptare.

15. Sistem, conform revendicării 14, caracterizat prin aceea că dispozitivul de imitare trafic este în plus configurat pentru a transmite cheia publică şi cel puţin un număr de schimbarea cheii de criptare la DUT.

16. Sistem, conform revendicării 12, caracterizat prin aceea că dispozitivul de imitare trafic este în plus configurat pentru a recepţiona o cheie publică DUT de la DUT, la iniţierea sesiunii de testare IPsec.

17. Sistem, conform revendicării 12, caracterizat prin aceea că sesiunea de testare IPsec se desfăşoară între dispozitivul de imitare trafic şi DUT la un strat de reţea.

18. Sistem, conform revendicării 12, caracterizat prin aceea că dispozitivul de imitare trafic funcţionează fie ca o entitate client fie ca o entitate server.

19. Sistem, conform revendicării 12, caracterizat prin aceea că menţionata cheie publică este generată prin utilizarea cheii private şi a cel puţin un număr de schimbare cheie de criptare.

20. Sistem, conform revendicării 12, caracterizat prin aceea că fiecare dintre cheile privată, publică şi secretă partajată este generată folosind o metodă Diffie-Hellman.

21. Sistem, conform revendicării 12, caracterizat prin aceea că DUT include cel puţin unul dintre: un dispozitiv de protecţie de tip firewall, un router, o poartă de acces de servire (SGW) şi o poarta de acces reţea de pachete de date (PGW).

22. Sistem, conform revendicării 12, caracterizat prin aceea că dispozitivul de imitare traficul este în plus configurat pentru a prelua cheia privată şi cheia publică din memoria locală la iniţierea unei a doua sesiuni de testare prin protocolul Ipsec, între dispozitivul de imitare trafic şi DUT, şi pentru a genera o a doua cheie secretă partajată folosind cheia privată şi o a doua cheie publică DUT recepţionate de la dispozitivul DUT.

23. Suport non-tranzitoriu care poate fi citit de calculator ce are stocate instrucţiuni executabile pe calculator care atunci când sunt executate de procesorul unui calculator comandă realizarea etapelor care constau în:

generarea, înainte de iniţierea unei sesiuni de testare pe Internet sub protocolul de securitate (IPsec), a unei chei private şi a unei chei publice la un dispozitiv de imitare trafic;

stocarea cheii private şi cheii publice într-o unitate de stocare locală asociată cu dispozitivul de imitare trafic; şi

preluarea, de la unitatea de stocare locală, a cheii private şi a cheii publice, la iniţierea sesiunii de testare prin protocolul IPsec între dispozitivul de imitare trafic şi un dispozitiv supus testării (DUT);

generarea unei chei secrete partajată utilizând cheia privată preluată şi o cheie publică DUT recepţionată de la DUT.

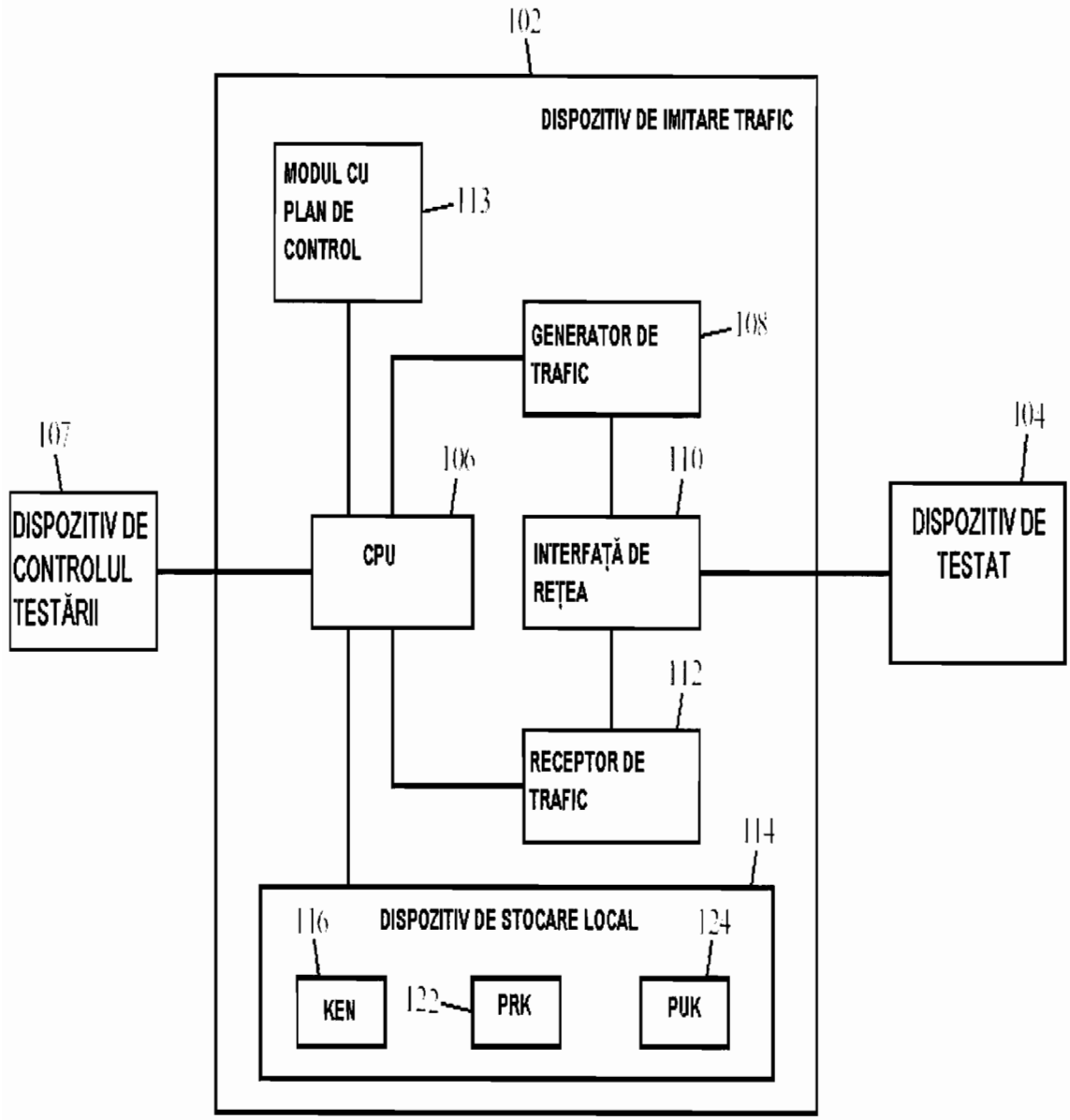
102
100
DISPOZITIV DE IMITARE TRAFIC
MODUL CU PLAN DE CONTROL
113
GENERATOR DE TRAFIC
108
104
107
106
110
DISPOZITIV DE CONTROLUL TESTĂRII
CPU
INTERFAȚĂ DE REȚEA
DISPOZITIV DE TESTAT
112
RECEPTOR DE TRAFIC
114
116
DISPOZITIV DE STOCARE LOCAL
124
KEN
122
PRK
PUK

FIG. 1

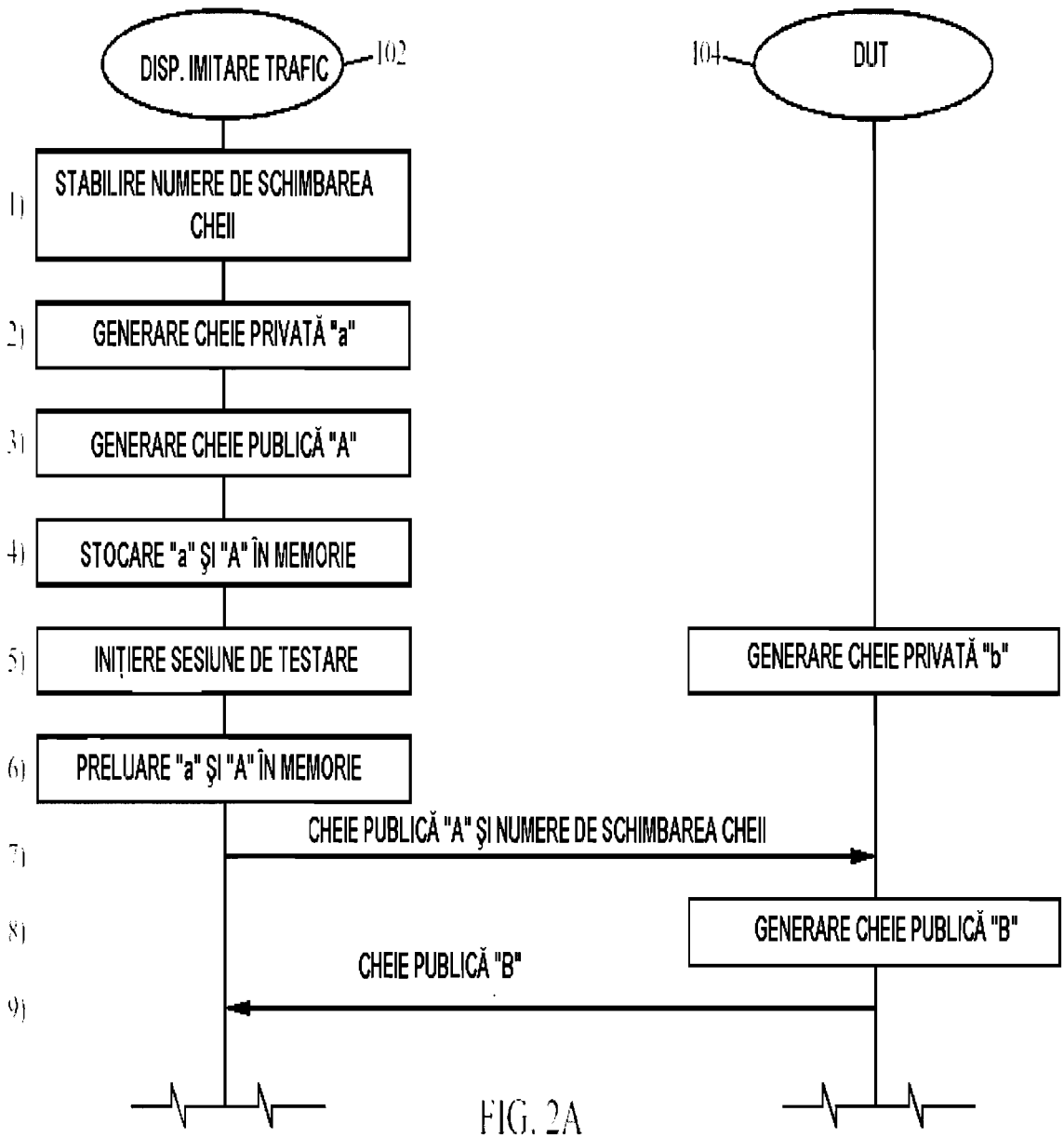
DISP. IMITARE TRAFIC
102
DUT
104
STABILIRE NUMERE DE SCHIMBAREA CHEII
1)
GENERARE CHEIE PRIVATĂ "a"
2)
GENERARE CHEIE PUBLICĂ "A"
3)
STOCARE "a" ŞI "A" ÎN MEMORIE
4)
INIŢIERE SESIUNE DE TESTARE
5)
GENERARE CHEIE PRIVATĂ "b"
PRELUARE "a" ŞI "A" ÎN MEMORIE
6)
CHEIE PUBLICĂ "A" ŞI NUMERE DE SCHIMBAREA CHEII
7)
GENERARE CHEIE PUBLICĂ "B"
8)
CHEIE PUBLICĂ "B"
9)

FIG. 2A

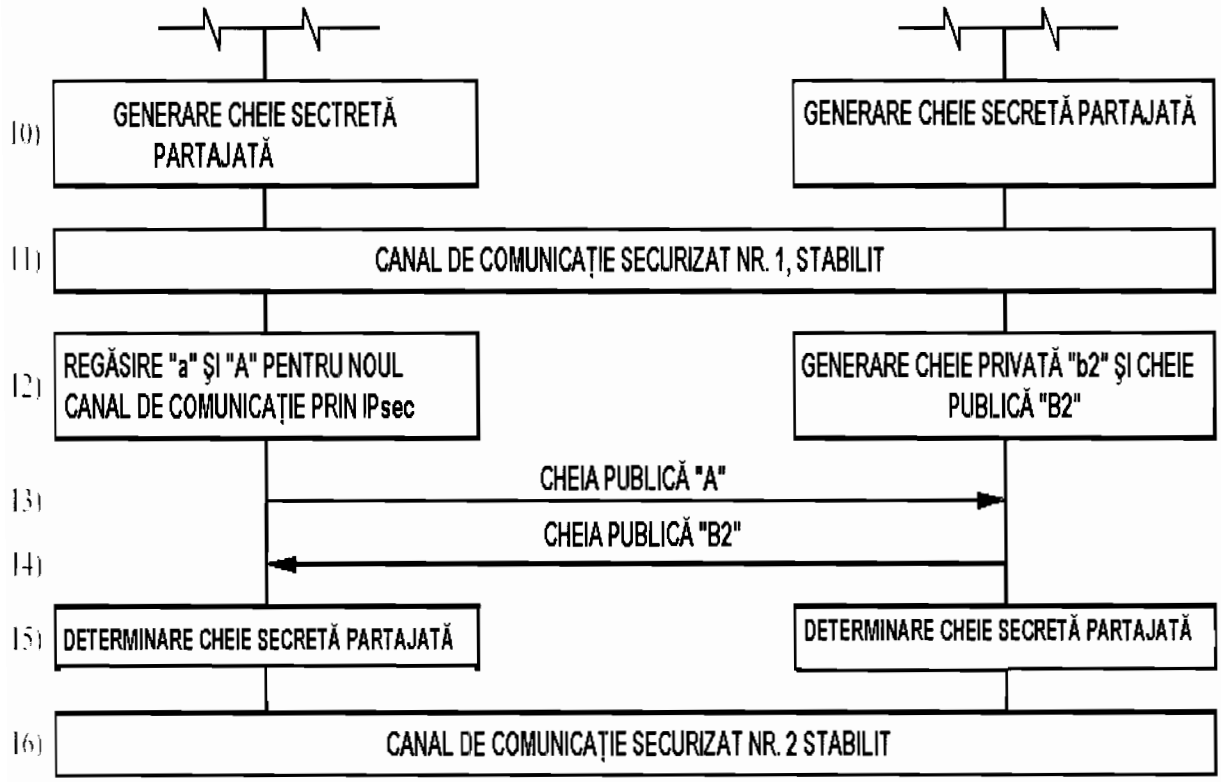
10)
GENERARE CHEIE SECTRETĂ PARTAJATĂ
GENERARE CHEIE SECRETĂ PARTAJATĂ
11)
CANAL DE COMUNICAȚIE SECURIZAT NR. 1, STABILIT
12)
REGĂSIRE "a" ŞI "A" PENTRU NOUL CANAL DE COMUNICAȚIE PRIN IPsec
GENERARE CHEIE PRIVATĂ "b2" ŞI CHEIE PUBLICĂ "B2"
13)
CHEIA PUBLICĂ "A"
14)
CHEIA PUBLICĂ "B2"
15)
DETERMINARE CHEIE SECRETĂ PARTAJATĂ
DETERMINARE CHEIE SECRETĂ PARTAJATĂ
16)
CANAL DE COMUNICAȚIE SECURIZAT NR. 2 STABILIT

FIG. 2B

a-2013-00647
28-08-2013

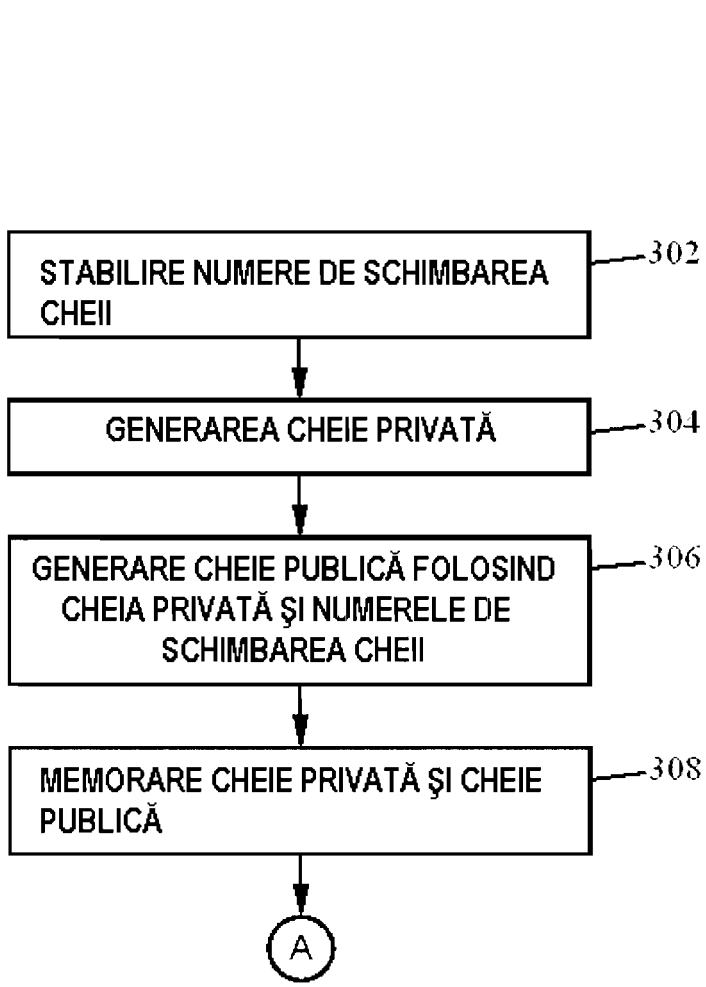

FIG. 3A

a-2013-00647-
28-08-2013

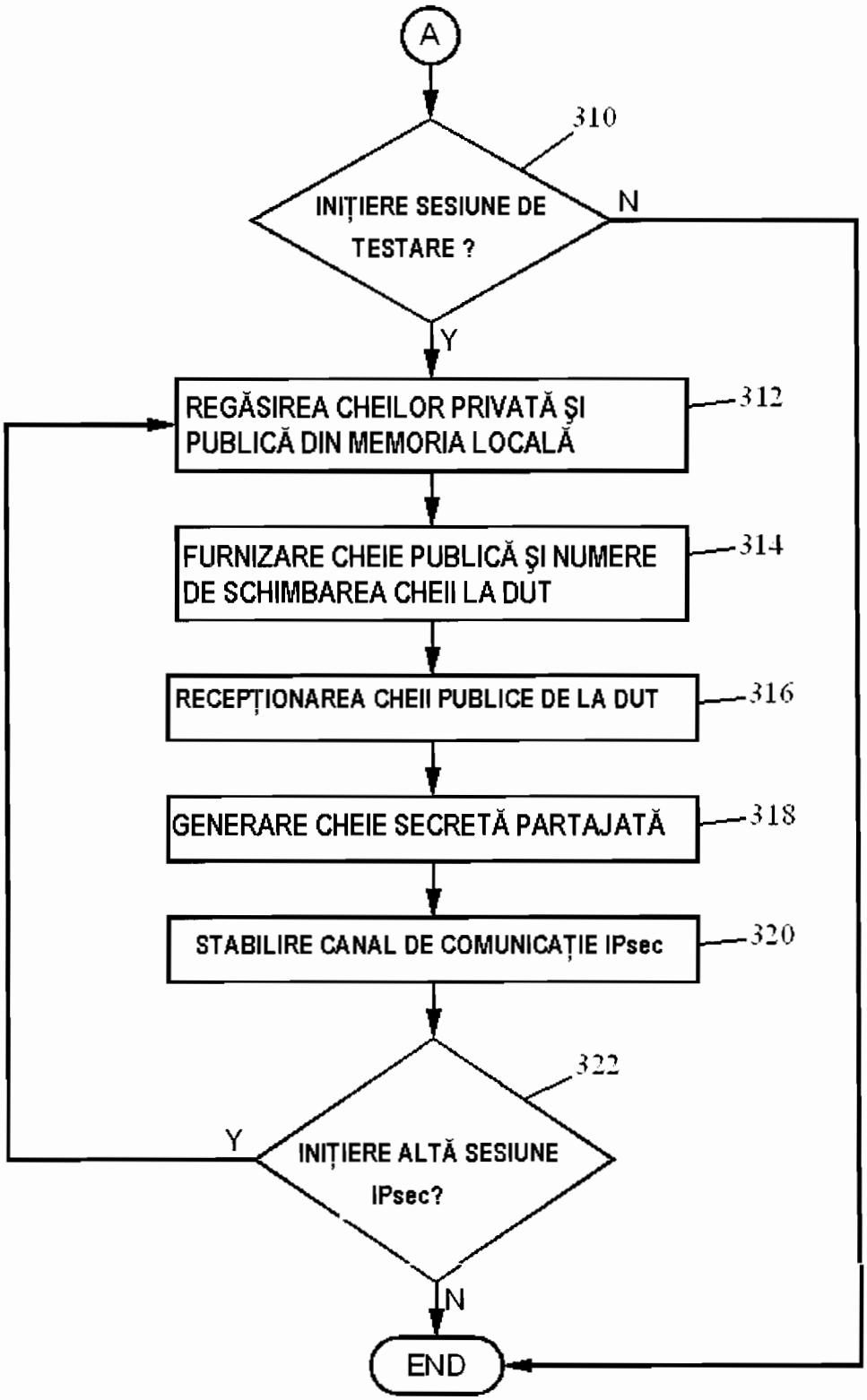

FIG. 3B