ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) RO 127706 A2

(51) Int.Cl.
H04L 9/12 (2006.01);
H04L 9/32 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2010 01303**

(22) Data de depozit: **09.12.2010**

(41) Data publicării cererii:
30.07.2012 BOPI nr. **7/2012**

(71) Solicitant:
• **UNIVERSITATEA TEHNICĂ DIN CLUJ-NAPOCA**, *STR. MEMORANDUMULUI NR.28, CLUJ NAPOCA, CJ, RO*

(72) Inventatori:
• **AŞTILEAN ADINA**, *ALEEA CIOPLEA NR. 9 BL. S9, SC. 2, ET. 2, AP. 26, CLUJ-NAPOCA, CJ, RO;*
• **FOLEA SILVIU**, *STR. METEOR NR. 6, BL. OZ2, SC. 2, ET. 3, AP. 21, CLUJ-NAPOCA, CJ, RO;*
• **AVRAM CAMELIA**, *STR. REPUBLICII NR. 74/E, AP. 7, TÂRNĂVENI, MS, RO;*
• **HULEA MIHAI**, *STR. BISTRIŢEI NR. 7, CLUJ-NAPOCA, CJ, RO;*
• **MIRON RADU FLORIN**, *STR. SLĂNIC NR.5, AP.11, CLUJ-NAPOCA, CJ, RO;*
• **LEŢIA TIBERIU ŞTEFAN**, *STR.MESTECENILOR NR.8, AP.19, CLUJ-NAPOCA, CJ, RO;*
• **CIUPAN EMILIA**, *STR.MESTECENILOR NR.6, AP.2, CLUJ-NAPOCA, CJ, RO*

(74) Mandatar:
CABINET DE PROPRIETATE INDUSTRIALĂ CIUPAN CORNEL, *STR. MESTECENILOR NR. 6, BL. 9E, AP. 2, CLUJ NAPOCA, JUDEŢUL CLUJ*

(54) # SISTEM ŞI METODĂ SECURIZATĂ DE COMUNICAŢIE ÎNTRE DISPOZITIVE FIXE ŞI MOBILE

(57) **Rezumat:**

Invenţia se referă la un sistem şi la o metodă securizată de comunicaţie între dispozitive fixe şi mobile, pe baza amprentelor digitale. Sistemul conform invenţiei este format din unul sau mai multe subsisteme (**1**) transmiţătoare, şi un subsistem (**2**) receptor, care constă dintr-un server de aplicaţie distribuit, conectat la Internet, transmiterea securizată informaţiilor între aceste subsisteme (**1** şi **2**) fiind bazată pe utilizarea unor tehnologii de comunicaţie fără fir sau cu fir, fiecare subsistem (**1**) transmiţător având în componenţa sa: un cititor de amprentă (**FPS**) prevăzut cu unitate de memorare şi procesare, cu posibilităţi de comunicare prin Bluetooth, Wi-Fi sau GPRS, un dispozitiv (**GPS**) ce comunică cu cititorul de amprentă (**FPS**), şi un terminal mobil (**MT**), ce are înglobată tehnologie GPRS, sau un computer (**PC**), prin intermediul terminalului mobil (**MT**) sau computerului (**PC**) realizându-se conectarea la subsistemul (**2**) receptor. Metoda securizată de comunicaţie, conform invenţiei, presupune transmiterea şi recepţionarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică şi durată de viaţă limitată, cheia simetrică fiind generată folosind informaţiile rezultate din citirea amprentei digitale a participanţilor la o sesiune de comunicaţii, şi pe cele referitoare la poziţiile acestora, iar autentificarea se realizează conform unui protocol care implică, pe lângă amprenta digitală, şi poziţia utilizatorului, şi codurile de identitate ale entităţilor implicate în procesul de comunicaţie, precum şi numărul sesiunii de comunicaţii între utilizatorii implicaţi.

Revendicări: 7
Figuri: 3

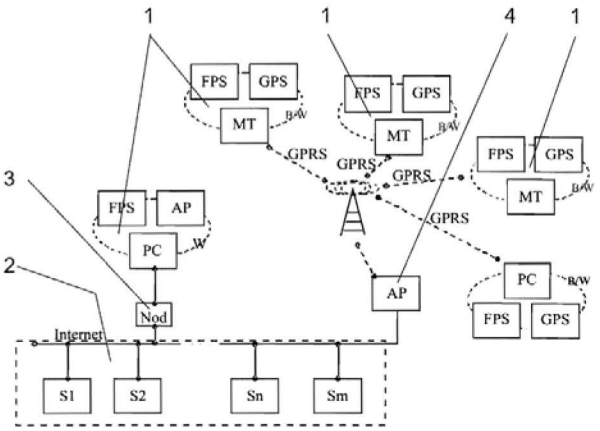

Fig. 1

RO 127706 A2

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2010 01303
Data depozit 09-12-2010

36

Sistem şi metodă securizată de comunicaţie între dispozitive fixe si mobile

Invenţia se referă la un sistem şi o metodă securizată de comunicaţie între dispozitive fixe şi mobile pe baza amprentelor digitale, în vederea accesului la "Internet Banking", ATM, într-o zonă cu acces limitat, sau la o componentă software. De asemenea, metoda poate fi utilizată şi numai în scopul identificării personale, la distanţă, a utilizatorilor.

Este cunoscută invenţia **KR 20010039815 (A)** care prezintă un sistem şi o metodă de criptare utilizate în transmiterea de date. Acestea presupun existenţa unor mijloace hardware şi software atât la emisie, cât şi la cea recepţie şi parcurgerea unor etape precise. Într-o primă fază, care se derulează la partea transmiţătoare, se reţin în memoria unui dispozitiv de memorare amprentele persoanelor autorizate să acceseze sistemul, mai precis caracteristicile amprentelor într-o formă criptată. La folosirea sistemului se citeşte amprenta utilizatorului, se extrag caracteristicile acesteia şi se compară cu cele stocate anterior în memoria dispozitivului de memorare. Dacă există o corespondenţă între amprenta citită si una dintre amprentele memorate anterior, atunci se generează o cheie de criptare Y care va servi la criptarea unui mesaj introdus de utilizator de la o tastatură sau selectat dintr-o listă de mesaje afişate pe un display. În continuare se decriptează caracteristicile amprentelor memorate anterior şi criptate cu un algoritm general, se compară cu caracteristicile amprentei examinate şi pe baza comparaţiei de determină un scor care este apoi folosit la generarea unei a doua chei de criptare X. Cheia X este folosită în continuare la criptarea caracteristicilor amprentei examinate. Mesajul transmis părţii receptoare este format din ID-ul utilizatorului a cărui amprentă a fost citită, din caracteristicile amprentei citite criptate cu cheia X şi din mesajul propriu-zis introdus de utilizator, criptat cu ajutorul cheii Y.

La partea receptoare mesajul recepţionat este prelucrat şi analizat după aceeaşi logică, dar parcursă în sens invers.

Sistemul şi metoda descrise în brevetul KR 20010039815 (A) prezintă mai multe dezavantaje, unul dintre cele mai importante fiind acela că necesită transportul prealabil al unor informaţii iniţiale de la emisie la recepţie, sub formă înregistrată. Sistemul necesită o multitudine de dispozitive hardware şi software plasate atât la emiţător, cât şi la receptor; dispozitivele părţii transmiţătoare par a fi plasate într-o locaţie fixă.

De asemenea, metoda descrisă în brevetul KR 20010039815 (A) nu beneficiază de o fundamentare matematică corespunzătoare, probabilitatea de a genera aceeaşi cheie de două ori nefiind suficient studiată.

Problema tehnică pe care o rezolvă invenţia este realizarea unei comunicaţii cu un grad ridicat de securitate între dispozitive fixe şi mobile.

Sistemul de acces securizat conform invenţiei este format din unul sau mai multe subsisteme transmiţătoare de mesaje, pe de o parte şi un subsistem, de regulă fix, având calitatea de subsistem receptor, pe de altă parte, în care subsistemul receptor constă dintr-un server de aplicaţie distribuit conectat la Internet, iar transmiterea securizată a informaţiilor între entităţile implicate (emiţător şi receptor) bazându-se pe utilizarea unor tehnologii de comunicaţie fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.

Metoda securizată de comunicaţie conform invenţiei presupune transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică şi cu durată de viaţă limitată. Metoda de generare a cheii simetrice se bazează pe un algoritm de tipul Diffie – Hellman şi utilizează informaţiile rezultate din citirea amprentei digitale a participanţilor la sesiunea de comunicaţie (minuţiile) şi pe cele referitoare la poziţiile acestora. Autentificarea se realizează conform unui protocol care implică pe lângă cele două informaţii enumerate mai sus (amprenta digitală şi poziţia utilizatorului), codurile de identitate ale entităţilor implicate în procesul de comunicaţie, precum şi numărul sesiunii de comunicaţie între utilizatorii implicaţi. Acesta modifică cele două coduri de identitate conform unui algoritm prestabilit.

Se dă în continuare un exemplu de realizare a invenţiei, în legătură cu figurile 1-3 care reprezintă:

- fig. 1, arhitectura hardware a sistemului de acces securizat;
- fig. 2, arhitectura software a sistemului de acces securizat;
- fig. 3, schema de generare a cheii unice pe sesiune.

Sistemul de acces securizat, conform invenţiei, permite comunicaţia între dispozitive mobile (subsistem emiţător) şi dispozitive fixe (subsistem receptor) sau între dispozitive fixe (adică între emiţător fix şi receptor fix). Un subsistem emiţător 1 are în componenţa sa un cititor de amprentă FPS (Finger Print Sensor) prevăzut cu unitate de memorare şi procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth B, Wi-Fi W (la distanţă mică) sau GPRS (la distanţă mare), un dispozitiv GPS (Global Positioning System) care comunică cu senzorul de amprentă FPS şi un terminal mobil MT (de exemplu, un telefon mobil sau un PDA) care are înglobată tehnologie GPRS-sau un PC, prin intermediul acestui ultim dispozitiv (MT sau PC) realizându-se, de regulă, conectarea la subsistemul receptor 2. Conectarea unui

subsistem emiţător 1 cu subsistemul receptor 2 se poate realiza într-un punct de acces 4 cu ajutorul tehnologiei de comunicaţie fără fir sau într-un nod de comunicaţie 3 prin intermediul unei legături fizice (cu fir). Subsistemul receptor 2 constă într-un server de aplicaţie distribuit Sx, x=1,2, ..., m conectat la Internet, serverele componente Sx, x=1,2, ..., m fiind fixe.

Metoda de securizare conform invenţiei este implementată pe un dispozitiv hardware mobil FPS special realizat, prevăzut cu o unitate de procesare şi capacitate de memorie. Dispozitivul FPS este prevăzut cu posibilităţi de comunicaţie radio bazate pe tehnologii larg răspândite (Wi-Fi, BT, GPRS). Nu este necesară în mod obligatoriu existenţa suplimentară a unui PC sau a unui telefon mobil, dispozitivul putând funcţiona şi independent.

Operaţiile destinate procesării locale a amprentelor au loc la nivelul dispozitivului FPS şi sunt urmate de transmiterea informaţiilor esenţiale (amprentele, locaţia şi codul de identificare) către un server de aplicaţie distribuit. Validarea datelor şi accesul este posibil numai în locaţii având poziţii predefinite, care pot fi determinate folosind GPS-ul în exteriorul clădirilor, respectiv cu ajutorul tehnologiei Wi-Fi în interiorul clădirilor. Transmiterea securizată a informaţiilor între entităţile implicate se poate face utilizând tehnologii de comunicaţie fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.

În cazul subsistemului emiţător 1, cheia de criptare unică pe sesiune se generează la nivelul dispozitivului FPS, fără a necesita, sub nici o formă, transportul prealabil şi riscant al unor date înregistrate.

Iniţializarea sesiunii de comunicaţie pe canalul securizat şi prelucrarea datelor în vederea autorizării accesului la informaţie se realizează folosind un server de aplicaţie la nivelul căruia sunt verificate amprentele, locaţia şi codurile de identificare. Acestea sunt stocate într-un sistem distribuit de baze de date.

Comunicaţia cu fir este utilizată doar între PC–uri, prin intermediul unor noduri de comunicaţie. Terminalele mobile MT şi calculatoarele PC comunică cu senzorul de amprentă FPS şi cu receptorul GPS folosind tehnologie Bluetooth B sau Wi-Fi (W).

Conform Figurii 2, aplicaţia software care rulează pe terminalul mobil (calculator sau telefon mobil) conţine funcţiile prezentate in continuare, împreună cu rolurile lor:

-*FPSFunction* – realizează interfaţa cu senzorul de amprentare;

-*GPSReader* – citeşte periodic datele de la receptorul GPS;

-*BluetoothInterface* - comunicaţia cu senzorul de amprentare şi receptorul GPS se face folosind tehnologia Bluetooth. Această interfaţă interpretează datele din formatul Bluetooth şi le converteşte într-un format utilizat mai departe;

-*Autentification* - modulul realizează verificarea şi identificarea locală a amprentei;

-*Security* - informaţiile transmise către / dinspre server sunt criptate / decriptate folosind mai mulţi algoritmi de criptare în funcţie de nivelul de securitate impus;

-*GPRSComm / WiFiLAN* – în funcţie de tipul de acces la Internet informaţia este structurată pe pachete de date (GSM sau LAN).

Terminalele mobile MT sau/şi serverul sunt iniţializate cu amprentele martor ale partenerilor de dialog date de senzorul FPS şi poziţiile lor furnizate de receptorul GPS sau determinate prin tehnologia Wi-Fi.

Protocolul de autentificare şi asigurare a confidenţialităţii informaţiilor transmise între dispozitive fixe si mobile se bazează pe execuţia următorului algoritm:

Algoritmul de pe un terminal mobil MT sau de pe server execută:

1. Autentificarea utilizatorului terminalului prin citirea amprentei şi compararea ei cu amprenta martor de care trebuie să difere cu mai puţin decât o valoare specificată.
2. Citirea poziţiei curente a terminalului.
3. Crearea cheii parţiale de criptare K' din amprenta curentă şi poziţia curentă.
4. Transmiterea cheii K' partenerului de dialog.
5. Recepţionarea cheii parţiale de criptare similare, K", de la partenerul de dialog.
6. Calculul cheii de criptare K din cheile parţiale K' şi K".
7. Criptarea cu ajutorul cheii K şi transmiterea spre partenerul de dialog a informaţiilor cuprinse în amprenta curentă, poziţia curentă, poziţia anterioară şi identificatorul sesiunii.
8. Recepţionarea de la partenerul de dialog a unui mesaj criptat cu ajutorul cheii K ce conţine informaţiile cuprinse în amprenta curentă, poziţia curentă, poziţia anterioară şi identificatorul sesiunii.
9. Extragerea, prin decriptare, din mesajul primit, a informaţiilor cuprinse în amprenta curentă a partenerului de dialog, a poziţiei sale curente şi anterioare.
10. Compararea amprentei curente a partenerului de dialog cu cea martor corespunzătoare. Se refuză dialogul dacă diferenţa dintre amprenta transmisă a partenerului şi cea martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziţia anterioară nu coincide cu cea stocată în terminalul curent.
11. Actualizarea poziţiilor celor două perechi de terminale mobile.
12. Desfăşurarea sesiunii de comunicaţie în mod criptat.
13. Închiderea sesiunii de lucru.

Generarea cheii unice pe sesiune şi transmiterea ei între utilizatorii 1 şi 2, conform Figurii 3, se bazează pe algoritmul Diffie-Hellman modificat, noutatea constând în modul în care se generează exponenţii cheii secrete. Caracteristicile distinctive ale acestor exponenţi se datorează caracteristicilor diferite ale amprentei, respectiv minuţiilor, precum şi aplicării funcţiilor Hash în scopul prelucrării minuţiilor. Chiar şi în cazul aceleiaşi persoane citirea succesivă a aceleiaşi amprente prezintă modificări, datorită poziţionării diferite a degetului pe cititorul de amprente.

Suplimentar, aplicarea funcţiilor SHA asupra şirului de biţi care reprezintă un număr de minuţii va conduce la reprezentări binare sensibil diferite pentru fiecare citire de amprentă.

Aceste şiruri de biţi vor fi partajate şi transmise bidirecţional între cele două terminale (emiţător – receptor) pentru a genera cheia secretă.

Cheia privată K, pct. 6 din algoritmul de autentificare şi asigurare a confidenţialităţii informaţiilor prezentat mai sus, se generează conform invenţiei, parcurgând următorii paşi:

1. Se concatenează şirul de biţi care reprezintă minuţiile cu şirul de biţi care reprezintă poziţia utilizatorului;
2. Se aplică un algoritm de tipul Secure Hash Algorithm (SHA) şirului de biţi;
3. Se segmentează şirul de caractere rezultate în urma aplicării funcţiei SHA, în scopul efectuării operaţiilor ulterioare; subşirurile obţinute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subşiruri);
4. Se alege un număr prim (notat cu b în Figura 3);
5. Se alege un număr prim suficient de mare, p;
6. Terminalul 1 calculează valorile, $u_1 = b^{t_{1j}} \bmod p$;
7. Terminalul 1 transmite utilizatorului 2 valorile b, p, u_1;
8. Terminalul 2 calculează valorile, $u_2 = b^{t_{2j}} \bmod p$;
9. Terminalul 2 transmite utilizatorului 1 valorile u_2;
10. Ambii utilizatori calculează aceleaşi componente ale cheii secrete K_j :

$$K_j = b^{t_{1j} * t_{2j}} \bmod p, \text{ pentru } j = 1,2,...n;$$

11. Utilizând componentele K_j şi o relaţie de compunere prestabilită, la cele două terminale se calculează aceeaşi cheie secretă K';
12. In scopul obţinerii unei chei finale K, de lungime precizată, se aplică o funcţie SHA cheii secrete K'.

Metoda de securizare a comunicaţiei între dispozitive fixe şi mobile conform invenţiei prezintă următoarele avantaje:

- generarea automată a unei chei unice pe sesiune, aceeaşi la emisie şi recepţie, fără a necesita, sub nici o formă, transportul prealabil şi riscant al unor date înregistrate. Volumul necesar de date memorate este mic;
- metoda se bazează pe o combinaţie formată nu numai din elemente de unicitate caracteristice persoanei (amprenta), ci şi din elemente de unicitate generate prin aplicarea unor funcţii cunoscute (SHA), ale căror proprietăţi au fost riguros stabilite;
- pentru realizarea comunicaţiei nu este neapărat necesar ca utilizatorul să dispună de un calculator sau de un telefon mobil, fiind suficient un dispozitiv hardware mobil, special realizat şi prevăzut cu o unitate de procesare şi capacitate de memorie. Dispozitivul se caracterizează prin costuri, dimensiuni şi consum de putere reduse şi este prevăzut cu posibilităţi de comunicaţie radio bazate pe tehnologii larg răspândite (Wi-Fi, BT, GPRS);
- dispozitivul hardware utilizat la citirea amprentei, generarea cheii de criptare şi criptarea informaţiilor de transmis este mobil, cu precizarea că utilizarea lui trebuie să se facă în perimetrul unor locaţii prestabilite;

- terminalul mobil (aflat la partea transmiţătoare) nu trebuie să dispună de o bază de date care să stocheze informaţiile folosite la compararea cu amprenta citită. Această bază de date este stocată la nivelul unui server de aplicaţie distribuit;
- includerea informaţiei privind poziţia actuală şi poziţia anterioară a utilizatorilor printre informaţiile care fac obiectul verificării înaintea autorizării accesului sporeşte securitatea comunicaţiei.

a-2010-01303--
09-12-2010 30 29

REVENDICĂRI

1. Sistem securizat de comunicaţie între dispozitive fixe si mobile format din unul sau mai multe subsisteme (1) transmiţătoare de mesaje, pe de o parte şi un subsistem (2), de regulă fix, având calitatea de subsistem receptor, pe de altă parte, în care subsistemul receptor (2) constă dintr-un server de aplicaţie distribuit conectat la Internet, iar transmiterea securizată a informaţiilor între entităţile implicate (1) şi (2) bazându-se pe utilizarea unor tehnologii de comunicaţie fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir, **caracterizat prin aceea că**, subsistemul emiţător (1) are în componenţa sa un cititor de amprentă (FPS) prevăzut cu unitate de memorare şi procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth (B), Wi-Fi (W), la distanţă mică, sau GPRS, la distanţă mare, un dispozitiv (GPS) care comunică cu senzorul de amprentă (FPS) şi un terminal mobil (MT) care poate fi un telefon mobil sau un dispozitiv PDA care are înglobată tehnologie GPRS, sau un (PC), prin intermediul acestui ultim dispozitiv, (MT) sau (PC), realizându-se conectarea la subsistemul receptor (2).

2. Metoda securizată de comunicaţie între dispozitive fixe si mobile care presupune transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică şi cu durată de viaţă limitată, **caracterizată prin aceea că**, utilizează informaţiile rezultate din citirea amprentei digitale a participanţilor la sesiunea de comunicaţie (minuţiile amprentei) şi pe cele referitoare la poziţiile participanţilor, autentificarea realizându-se conform unui protocol care implică pe lângă cele două informaţii enumerate, amprenta digitală şi poziţia utilizatorului, codurile de identitate ale entităţilor implicate în procesul de comunicaţie, precum şi numărul sesiunii de comunicaţie între utilizatorii implicaţi, protocolul modificând cele două coduri de identitate conform unui algoritm prestabilit, cheia de criptare fiind unică pentru fiecare sesiune.

3. Metoda securizată de comunicaţie între dispozitive fixe si mobile conform revendicării 2, **caracterizată prin aceea că**, generarea cheii secrete de criptare unice pe sesiune presupune parcurgerea următoarelor etape:
   I. cu dispozitivul mobil FPS de citire a amprentei se citesc amprentele celor doi utilizatori care comunică;
   II. se extrag minuţiile amprentelor, cu ajutorul unităţii de procesare şi memorare a senzorului de amprentă FPS;

III. se citesc coordonatele GPS sau, în locaţii interioare, se utilizează tehnologia Wi-Fi, pentru precizarea poziţiilor utilizatorilor;

IV. se generează cheia privată K conform invenţiei parcurgând următorii paşi:

a) se concatenează şirul de biţi care reprezintă minuţiile cu şirul de biţi care reprezintă poziţia utilizatorului;

b) se aplică un algoritm de tipul Secure Hash Algorithm (SHA) şirului de biţi rezultat la pasul a);

c) se segmentează şirul de caractere rezultate în urma aplicării funcţiei SHA, în scopul efectuării operaţiilor ulterioare; subşirurile obţinute la cele două terminale sunt notate cu t_{ij} (unde i reprezintă numărul terminalului, iar j ia valori de la 1 până la valoarea corespunzătoare numărului de subşiruri, n);

d) se alege un număr prim, notat cu b în Figura 3;

e) se alege un număr prim suficient de mare, notat cu p;

f) utilizatorul 1 calculează valorile, $u_1 = b^{t_{1j}} \bmod p$;

g) utilizatorul 1 transmite utilizatorului 2 valorile b, p, u_1;

h) utilizatorul 2 calculează valorile, $u_2 = b^{t_{2j}} \bmod p$;

i) utilizatorul 2 transmite utilizatorului 1 valorile u_2;

j) ambii utilizatori calculează aceleaşi componente ale cheii secrete K_j pe baza formulei

$$K_j = b^{t_{1j} * t_{2j}} \bmod p, \quad \text{pentru} \quad j = 1,2,\ldots,n;$$

k) utilizând componentele K_j şi o relaţie de compunere prestabilită, cei doi utilizatori calculează aceeaşi cheie secretă K' ;

l) în scopul obţinerii unei chei finale K, de lungime precizată, se aplică o funcţie SHA cheii secrete K' .

4. Metoda securizată de comunicaţie între dispozitive fixe si mobile conform revendicărilor 2 şi 3, caracterizată prin aceea că, utilizează un protocol de autentificare şi asigurare a confidenţialităţii informaţiilor transmise între dispozitive fixe şi mobile care se bazează pe un algoritm ce se execută pe un terminal mobil (MT) sau pe server şi care este descris prin paşii i-xiii după cum urmează:

i) Autentificarea utilizatorului terminalului prin citirea amprentei şi compararea ei cu amprenta martor de care trebuie să difere cu mai puţin decât o valoare specificată.

ii) Citirea poziţiei curente a terminalului.

iii) Crearea cheii parţiale de criptare K' din amprenta curentă şi poziţia curentă.

iv) Transmiterea cheii K' partenerului de dialog.

v) Recepţionarea cheii parţiale de criptare similare, K", de la partenerul de dialog.

vi) Calculul cheii de criptare K din cheile parţiale K' şi K".

vii) Criptarea cu ajutorul cheii K şi transmiterea spre partenerul de dialog a informaţiilor cuprinse în amprenta curentă, poziţia curentă, poziţia anterioară şi identificatorul sesiunii.

viii) Recepţionarea de la partenerul de dialog a unui mesaj criptat cu ajutorul cheii K ce conţine informaţiile cuprinse în amprenta curentă, poziţia curentă, poziţia anterioară şi identificatorul sesiunii.

ix) Extragerea, prin decriptare, din mesajul primit, a informaţiilor cuprinse în amprenta curentă a partenerului de dialog, a poziţiei sale curente şi anterioare.

x) Compararea amprentei curente a partenerului de dialog cu cea martor corespunzătoare. Se refuză dialogul dacă diferenţa dintre amprenta transmisă a partenerului şi cea martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziţia anterioară nu coincide cu cea stocată în terminalul curent.
xi) Actualizarea poziţiilor celor două perechi de terminale mobile.
xii) Desfăşurarea sesiunii de comunicaţie în mod criptat.
xiii) Închiderea sesiunii de lucru.

5. Metoda securizată de comunicaţie între dispozitive fixe si mobile, conform revendicărilor 1, 2 şi 3, **caracterizată prin aceea că**, la nivelul subsistemului emiţător (1), cheia de criptare unică pe sesiune se generează de către dispozitivul mobil (FPS) prin intermediul unităţilor de procesare şi memorare cu care acesta este prevăzut.

6. Metoda securizată de comunicaţie între dispozitive fixe si mobile, conform revendicării 2, **caracterizată prin aceea că**, în cadrul informaţiilor de autentificare se include şi poziţia actuală şi poziţia anterioara a utilizatorului, poziţie în jurul căreia se acceptă schimbul de informaţii.

7. Metoda securizată de comunicaţie între dispozitive fixe si mobile, conform revendicării 2, **caracterizată prin aceea că**, la închiderea sesiunii de comunicaţie, valabilitatea cheii de criptare K expiră.

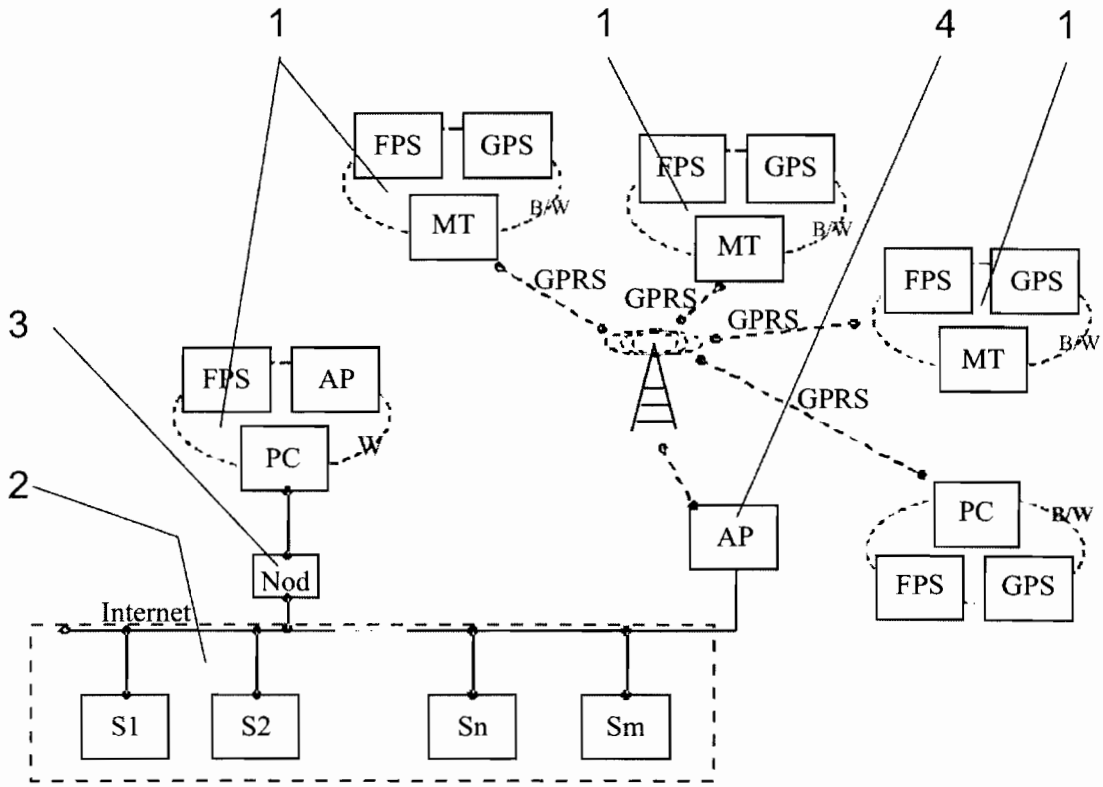

Figura 1

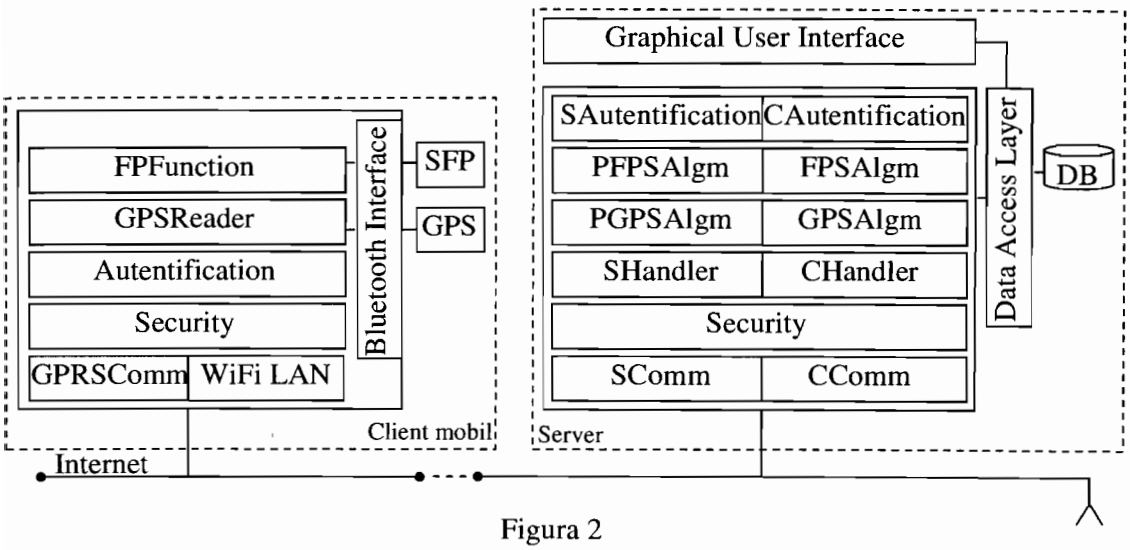

Figura 2

a-2010-01303--
09-12-2010

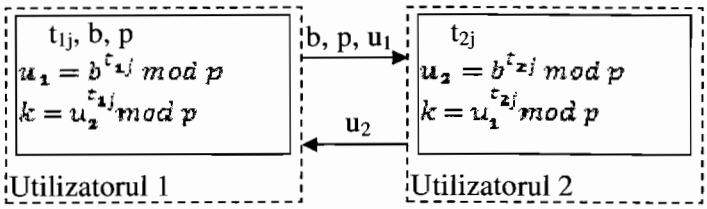

Figura 3