



(12) CERERE DE BREVET DE INVENȚIE

(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:
• AȘTILEAN 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, TÂRNAVENI, MS, RO;

• HULEA MIHAI, STR. BISTRIȚEI NR. 7,
CLUJ-NAPOCA, CJ, RO;
• MIRON RADU FLORIN, STR. SLĂNIC
NR.5, AP.11, CLUJ-NAPOCA, CJ, RO;
• LEȚIA TIBERIU ȘTEFAN,
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, JUDEȚUL CLUJ

(54) SISTEM ȘI METODĂ SECURIZATĂ DE COMUNICAȚIE ÎNTRE
DISPOZITIVE FIXE ȘI MOBILE

(57) Rezumat:

Invenția se referă la un sistem și la o metodă securizată de comunicație între dispozitive fixe și mobile, pe baza amprentelor digitale. Sistemul conform invenției este format din unul sau mai multe subsisteme (1) transmițătoare, și un subsistem (2) receptor, care constă dintr-un server de aplicație distribuit, conectat la Internet, transmiterea securizată a informațiilor între aceste subsisteme (1 și 2) fiind bazată pe utilizarea unor tehnologii de comunicație fără fir sau cu fir, fiecare subsistem (1) transmițător având în componența sa: un cititor de amprentă (FPS) prevăzut cu unitate de memorare și procesare, cu posibilități de comunicare prin Bluetooth, Wi-Fi sau GPRS, un dispozitiv (GPS) ce comunică cu cititorul de amprentă (FPS), și 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 comunicație, conform invenției, presupune transmiterea și recepționarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică și durată de viață limitată, cheia simetrică fiind generată folosind informațiile rezultate din citirea amprentei digitale a participanților la o sesiune de comunicație, și pe cele referitoare la pozițiile acestora, iar autentificarea se realizează conform unui protocol care implică, pe lângă amprenta digitală, și poziția utilizatorului, și codurile de identitate ale entităților implicate în procesul de comunicație, precum și numărul sesiunii de comunicație între utilizatorii implicați.

Revendicări: 7
Figuri: 3

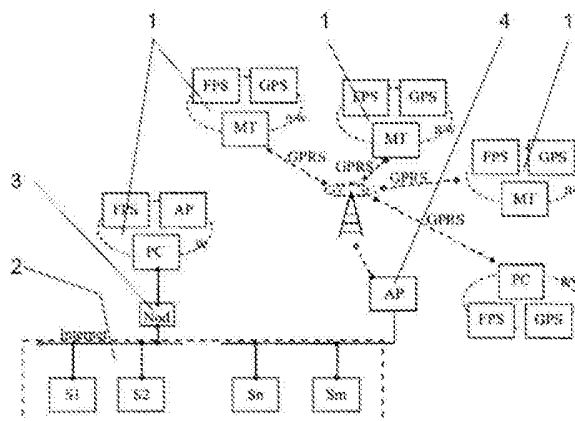
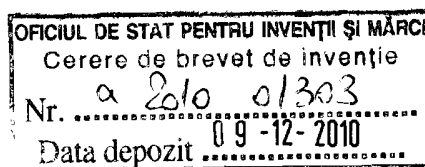


Fig. 1

Cu începere de la data publicării cererii de brevet, cererea asigură, în mod provizoriu, solicitantului, protecția conferită potrivit dispozițiilor art.32 din Legea nr.64/1991, cu excepția cazurilor în care cererea de brevet de invenție a fost respinsă, retrasă sau considerată ca fiind retrasă. Întinderea protecției conferite de cererea de brevet de invenție este determinată de revendicările conținute în cererea publicată în conformitate cu art.23 alin.(1) - (3).





Sistem și metodă securizată de comunicație între dispozitive fixe și mobile

Invenția se referă la un sistem și o metodă securizată de comunicație între dispozitive fixe și 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 și numai în scopul identificării personale, la distanță, a utilizatorilor.

Este cunoscută invenția **KR 20010039815 (A)** care prezintă un sistem și o metodă de criptare utilizate în transmiterea de date. Acestea presupun existența unor mijloace hardware și software atât la emisie, cât și la cea recepție și parcurgerea unor etape precise. Într-o primă fază, care se derulează la partea transmițătoare, se rețin în memoria unui dispozitiv de memorare amprentele persoanelor autorizate să acceseze sistemul, mai precis caracteristicile amprentelor într-o formă criptată. La folosirea sistemului se citește amprenta utilizatorului, se extrag caracteristicile acesteia și se compară cu cele stocate anterior în memoria dispozitivului de memorare. Dacă există o corespondență între amprenta citită și 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 afișate pe un display. În continuare se decriptează caracteristicile amprentelor memorate anterior și criptate cu un algoritm general, se compară cu caracteristicile amprentei examinate și pe baza comparației 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 părții receptoare este format din ID-ul utilizatorului a cărui amprentă a fost citită, din caracteristicile amprente citite criptate cu cheia X și din mesajul propriu-zis introdus de utilizator, criptat cu ajutorul cheii Y.

La partea receptoare mesajul recepționat este prelucrat și analizat după aceeași logică, dar parcursă în sens invers.

Sistemul și metoda descrise în brevetul **KR 20010039815 (A)** prezintă mai multe dezavantaje, unul dintre cele mai importante fiind acela că necesită transportul prealabil al unor informații inițiale de la emisie la recepție, sub formă înregistrată. Sistemul necesită o multitudine de dispozitive hardware și software plasate atât la emițător, cât și la receptor; dispozitivele părții transmițătoare par a fi plasate într-o locație fixă.

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

Problema tehnică pe care o rezolvă invenția este realizarea unei comunicații cu un grad ridicat de securitate între dispozitive fixe și mobile.

Sistemul de acces securizat conform invenției este format din unul sau mai multe subsisteme transmițătoare de mesaje, pe de o parte și un subsistem, de regulă fix, având calitatea de subsistem receptor, pe de altă parte, în care subsistemul receptor constă dintr-un server de aplicație distribuit conectat la Internet, iar transmiterea securizată a informațiilor între entitățile implicate (emițător și receptor) bazându-se pe utilizarea unor tehnologii de comunicație fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.

Metoda securizată de comunicație conform invenției presupune transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică și cu durată de viață limitată. Metoda de generare a cheii simetrice se bazează pe un algoritm de tipul Diffie – Hellman și utilizează informațiile rezultate din citirea amprentei digitale a participanților la sesiunea de comunicație (minuțiile) și pe cele referitoare la pozițiile acestora. Autentificarea se realizează conform unui protocol care implică pe lângă cele două informații enumerate mai sus (amprenta digitală și poziția utilizatorului), codurile de identitate ale entităților implicate în procesul de comunicație, precum și numărul sesiunii de comunicație între utilizatorii implicați. Acesta modifică cele două coduri de identitate conform unui algoritm prestabilit.

Se dă în continuare un exemplu de realizare a invenției, 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 invenției, permite comunicația între dispozitive mobile (subsistem emițător) și dispozitive fixe (subsistem receptor) sau între dispozitive fixe (adică între emițător fix și receptor fix). Un subsistem emițător 1 are în componența sa un cititor de amprentă FPS (Finger Print Sensor) prevăzut cu unitate de memorare și procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth B, Wi-Fi W (la distanță mică) sau GPRS (la distanță mare), un dispozitiv GPS (Global Positioning System) care comunică cu senzorul de amprentă FPS și 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 emițător 1 cu subsistemul receptor 2 se poate realiza într-un punct de acces 4 cu ajutorul tehnologiei de comunicație fără fir sau într-un nod de comunicație 3 prin intermediul unei legături fizice (cu fir). Subsistemul receptor 2 constă într-un server de aplicație distribuit S_x , $x=1,2, \dots, m$ conectat la Internet, serverele componente S_x , $x=1,2, \dots, m$ fiind fixe.

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

Operațiile destinate procesării locale a amprentelor au loc la nivelul dispozitivului FPS și sunt urmate de transmiterea informațiilor esențiale (ampretele, locația și codul de identificare) către un server de aplicație distribuit. Validarea datelor și accesul este posibil numai în locații având poziții predefinite, care pot fi determinate folosind GPS-ul în exteriorul clădirilor, respectiv cu ajutorul tehnologiei Wi-Fi în interiorul clădirilor. Transmiterea securizată a informațiilor între entitățile implicate se poate face utilizând tehnologii de comunicație fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir.

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

Inițializarea sesiunii de comunicație pe canalul securizat și prelucrarea datelor în vederea autorizării accesului la informație se realizează folosind un server de aplicație la nivelul căruia sunt verificate ampretele, locația și codurile de identificare. Acestea sunt stocate într-un sistem distribuit de baze de date.

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

Conform Figurii 2, aplicația software care rulează pe terminalul mobil (calculator sau telefon mobil) conține funcțiile prezentate în continuare, împreună cu rolurile lor:

- FPSFunction* – realizează interfața cu senzorul de amprentare;

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

- BluetoothInterface* - comunicația cu senzorul de amprentare și receptorul GPS se face folosind tehnologia Bluetooth. Această interfață interpretează datele din formatul Bluetooth și le convertește într-un format utilizat mai departe;

- Autentification* - modulul realizează verificarea și identificarea locală a ampretei;

-*Security* - informațiile transmise către / dinspre server sunt criptate / decriptate folosind mai mulți algoritmi de criptare în funcție de nivelul de securitate impus;

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

Terminalele mobile MT sau/și serverul sunt inițializate cu amprente martor ale partenerilor de dialog date de senzorul FPS și pozițiile lor furnizate de receptorul GPS sau determinate prin tehnologia Wi-Fi.

Protocolul de autentificare și asigurare a confidențialității informațiilor transmise între dispozitive fixe și mobile se bazează pe execuția următorului algoritm:

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

1. Autentificarea utilizatorului terminalului prin citirea amprente și compararea ei cu amprenta martor de care trebuie să difere cu mai puțin decât o valoare specificată.
2. Citirea poziției curente a terminalului.
3. Crearea cheii parțiale de criptare K' din amprenta curentă și poziția curentă.
4. Transmiterea cheii K' partenerului de dialog.
5. Recepționarea cheii parțiale de criptare similare, K'' , de la partenerul de dialog.
6. Calculul cheii de criptare K din cheile parțiale K' și K'' .
7. Criptarea cu ajutorul cheii K și transmiterea spre partenerul de dialog a informațiilor cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii.
8. Recepționarea de la partenerul de dialog a unui mesaj criptat cu ajutorul cheii K ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii.
9. Extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta curentă a partenerului de dialog, a poziției sale curente și anterioare.
10. Compararea amprente curente a partenerului de dialog cu cea martor corespunzătoare. Se refuză dialogul dacă diferența dintre amprenta transmisă a partenerului și cea martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziția anterioară nu coincide cu cea stocată în terminalul curent.
11. Actualizarea pozițiilor celor două perechi de terminale mobile.
12. Desfășurarea sesiunii de comunicație în mod criptat.
13. Închiderea sesiunii de lucru.

Generarea cheii unice pe sesiune și transmiterea ei între utilizatorii 1 și 2, conform Figurii 3, se bazează pe algoritmul Diffie-Hellman modificat, noutatea constând în modul în care se generează exponenții cheii secrete. Caracteristicile distinctive ale acestor exponenți se datorează caracteristicilor diferite ale amprente, respectiv minuțiilor, precum și aplicării funcțiilor Hash în scopul prelucrării minuțiilor. Chiar și în cazul aceleiași persoane citirea succesivă a aceleiași amprente prezintă modificări, datorită poziționării diferite a degetului pe cititorul de amprente.

Suplimentar, aplicarea funcțiilor SHA asupra șirului de biți care reprezintă un număr de minuții va conduce la reprezentări binare sensibil diferite pentru fiecare citire de amprentă.

Aceste șiruri de biți vor fi partajate și transmise bidirecțional între cele două terminale (emițător – receptor) pentru a genera cheia secretă.

Cheia privată K, pct. 6 din algoritmul de autentificare și asigurare a confidențialității informațiilor prezentat mai sus, se generează conform invenției, parcurgând următorii pași:

1. Se concatenează șirul de biți care reprezintă minuțiile cu șirul de biți care reprezintă poziția utilizatorului;
2. Se aplică un algoritm de tipul Secure Hash Algorithm (SHA) șirului de biți;
3. Se segmentează șirul de caractere rezultate în urma aplicării funcției SHA, în scopul efectuării operațiilor ulterioare; subșirurile obținute 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 subșiruri);
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 aceleași componente ale cheii secrete K_j :

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

11. Utilizând componentele K_j și o relație de compunere prestabilită, la cele două terminale se calculează aceeași cheie secretă K' ;
12. În scopul obținerii unei chei finale K , de lungime precizată, se aplică o funcție SHA cheii secrete K' .

Metoda de securizare a comunicației între dispozitive fixe și mobile conform invenției prezintă următoarele avantaje:

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

- terminalul mobil (aflat la partea transmițătoare) nu trebuie să dispună de o bază de date care să stocheze informațiile folosite la compararea cu amprenta citită. Această bază de date este stocată la nivelul unui server de aplicație distribuit;
- includerea informației privind poziția actuală și poziția anterioară a utilizatorilor printre informațiile care fac obiectul verificării înaintea autorizării accesului sporește securitatea comunicației.

REVENDICĂRI

1. Sistem securizat de comunicație între dispozitive fixe si mobile format din unul sau mai multe subsisteme (1) transmițătoare de mesaje, pe de o parte și 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 aplicație distribuit conectat la Internet, iar transmiterea securizată a informațiilor între entitățile implicate (1) și (2) bazându-se pe utilizarea unor tehnologii de comunicație fără fir (Wi-Fi, Bluetooth sau GPRS) sau cu fir, **caracterizat prin aceea că**, subsistemul emițător (1) are în componența sa un cititor de amprentă (FPS) prevăzut cu unitate de memorare și procesare, cu posibilitate de comunicare utilizând tehnologiile Bluetooth (B), Wi-Fi (W), la distanță mică, sau GPRS, la distanță mare, un dispozitiv (GPS) care comunică cu senzorul de amprentă (FPS) și 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 comunicație între dispozitive fixe si mobile care presupune transmiterea-receptarea unui mesaj criptat, folosind un algoritm de criptare cu cheie simetrică și cu durată de viață limitată, **caracterizată prin aceea că**, utilizează informațiile rezultate din citirea amprente digitale a participanților la sesiunea de comunicație (minuțiile amprente) și pe cele referitoare la pozițiile participanților, autentificarea realizându-se conform unui protocol care implică pe lângă cele două informații enumerate, amprenta digitală și poziția utilizatorului, codurile de identitate ale entităților implicate în procesul de comunicație, precum și numărul sesiunii de comunicație între utilizatorii implicați, protocolul modificând cele două coduri de identitate conform unui algoritm prestabilit, cheia de criptare fiind unică pentru fiecare sesiune.
3. Metoda securizată de comunicație 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 amprente se citesc amprentecele celor doi utilizatori care comunică;
 - II. se extrag minuțiile amprentelor, cu ajutorul unității de procesare și memorare a senzorului de amprentă FPS;

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

IV. se generează cheia privată K conform invenției parcurgând următorii pași:

- a) se concatenează șirul de biți care reprezintă minuțiile cu șirul de biți care reprezintă poziția utilizatorului;
- b) se aplică un algoritm de tipul Secure Hash Algorithm (SHA) șirului de biți rezultat la pasul a);
- c) se segmentează șirul de caractere rezultate în urma aplicării funcției SHA, în scopul efectuării operațiilor ulterioare; subșirurile obținute 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 subșiruri, 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 aceleași componente ale cheii secrete K_j pe baza formulei

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

- k) utilizând componentele K_j și o relație de compunere prestabilită, cei doi utilizatori calculează aceeași cheie secretă K' ;
- l) în scopul obținerii unei chei finale K, de lungime precizată, se aplică o funcție SHA cheii secrete K' .

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

- i) Autentificarea utilizatorului terminalului prin citirea amprente și compararea ei cu amprenta martor de care trebuie să difere cu mai puțin decât o valoare specificată.
- ii) Citirea poziției curente a terminalului.
- iii) Crearea cheii parțiale de criptare K' din amprenta curentă și poziția curentă.
- iv) Transmiterea cheii K' partenerului de dialog.
- v) Recepționarea cheii parțiale de criptare similare, K'' , de la partenerul de dialog.
- vi) Calculul cheii de criptare K din cheile parțiale K' și K'' .
- vii) Criptarea cu ajutorul cheii K și transmiterea spre partenerul de dialog a informațiilor cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii.
- viii) Recepționarea de la partenerul de dialog a unui mesaj criptat cu ajutorul cheii K ce conține informațiile cuprinse în amprenta curentă, poziția curentă, poziția anterioară și identificatorul sesiunii.
- ix) Extragerea, prin decriptare, din mesajul primit, a informațiilor cuprinse în amprenta curentă a partenerului de dialog, a poziției sale curente și anterioare.

- x) Compararea amprente curente a partenerului de dialog cu cea martor corespunzătoare. Se refuză dialogul dacă diferența dintre amprenta transmisă a partenerului și cea martor corespunzătoare diferă cu mai mult decât o valoare specificată, sau poziția anterioară nu coincide cu cea stocată în terminalul curent.
 - xi) Actualizarea pozițiilor celor două perechi de terminale mobile.
 - xii) Desfășurarea sesiunii de comunicație în mod criptat.
 - xiii) Închiderea sesiunii de lucru.
5. Metoda securizată de comunicație între dispozitive fixe si mobile, conform revendicărilor 1, 2 și 3, **caracterizată prin aceea că**, la nivelul subsistemului emițător (1), cheia de criptare unică pe sesiune se generează de către dispozitivul mobil (FPS) prin intermediul unităților de procesare și memorare cu care acesta este prevăzut.
6. Metoda securizată de comunicație între dispozitive fixe si mobile, conform revendicării 2, **caracterizată prin aceea că**, în cadrul informațiilor de autentificare se include și poziția actuală și poziția anterioară a utilizatorului, poziție în jurul căreia se acceptă schimbul de informații.
7. Metoda securizată de comunicație între dispozitive fixe si mobile, conform revendicării 2, **caracterizată prin aceea că**, la închiderea sesiunii de comunicație, valabilitatea cheii de criptare K expiră.

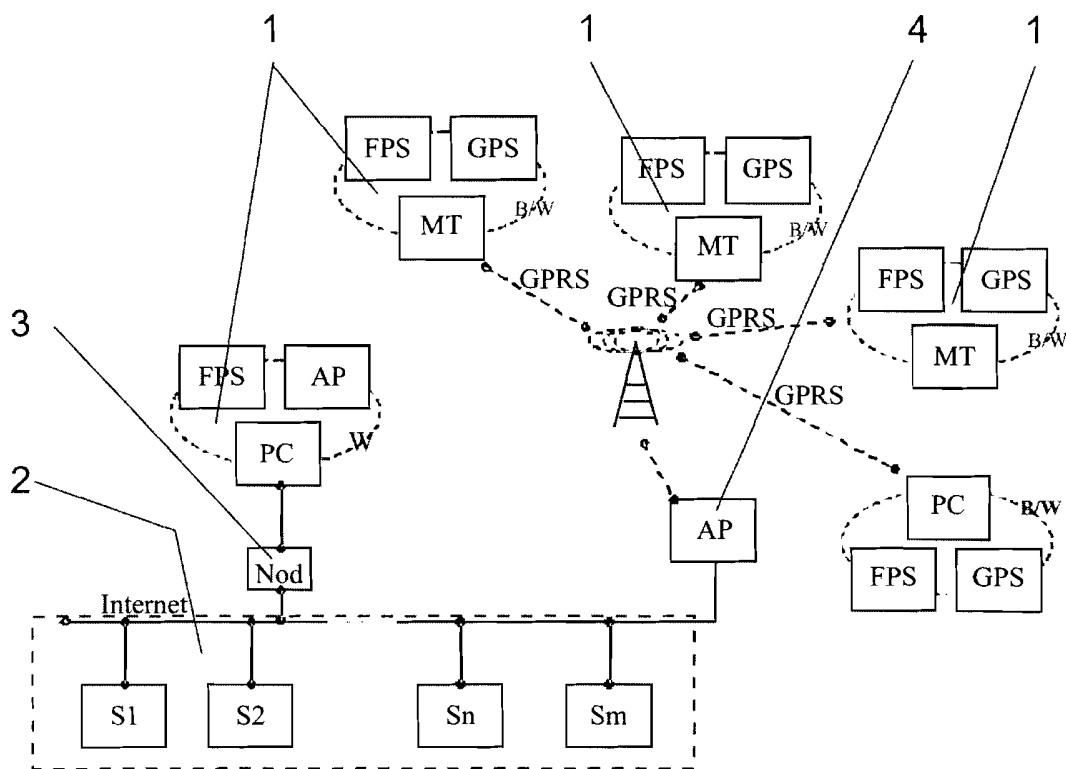


Figura 1

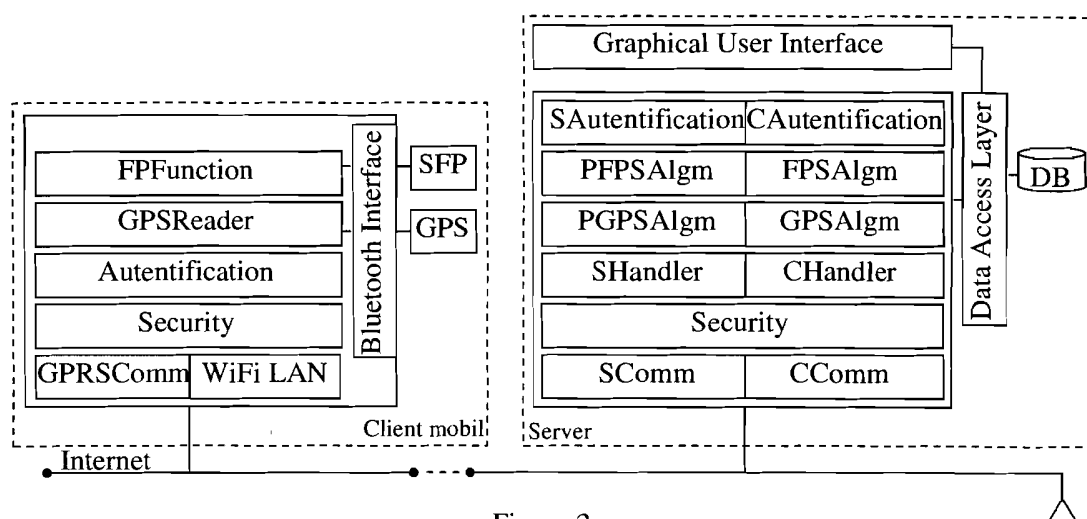


Figura 2

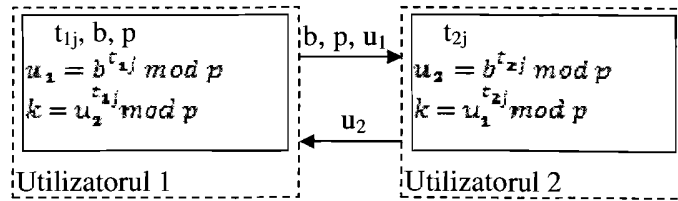


Figura 3