(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 131251 A0
(51) Int.Cl.
H04L 9/08 (2006.01),
H04L 9/14 (2006.01)

(12) # CERERE DE BREVET DE INVENȚIE

(21) Nr. cerere: **a 2015 00663**

(22) Data de depozit: **15/09/2015**

(41) Data publicării cererii:
30/06/2016 BOPI nr. **6/2016**

(71) Solicitant:
• **HDJ WIRELESS ENTERPRISE L.L.C ATLANTA S.U.A. SUCURSALA BUCUREŞTI**, *STR. BUCUR NR. 4-6, OFFICE NR. 1, SECTOR 4, BUCUREŞTI, B, RO*

(72) Inventatori:
• **TICUŞ ION**, *STR. ANASTASIE PANU NR. 20, BL. C15, SC.3, ET. 6, AP. 91, SECTOR 3, BUCUREŞTI, B, RO*

(54) # OPTIMIZAREA PROCESULUI DE ACCEPTARE ÎN MOD SECURIZAT ÎNTR-O REȚEA 802.15.4e

(57) **Rezumat:**

Invenția se referă la o metodă de optimizare a procesului de acceptare în mod securizat într-o rețea de dispozitive cu comunicare în radiofrecvență, conformă cu standardul "802.15.4e", ce rezolvă problema înregistrării lente la admisia în rețea, în cadrul protocoalelor PANA şi EAP-TLS, şi problema nivelului redus de securitate la acceptarea în rețea, în cadrul standardului "IEEE 802.15.4e". Metoda de optimizare, conform invenției, cuprinde un procedeu de admisie rapidă, atunci când o altă admisie completă a fost făcută în aceeaşi rețea, cu respectarea normelor de securitate ale protocoalelor PANA/ EAP-TLS, completat cu un procedeu de administrare a cheilor pe durata de viață, conform căruia un dispozitiv cu comunicare în radiofrecvență va avea la dispoziție tot timpul două chei, ale căror durate de viață se suprapun parțial, astfel încât să fie asigurate premisele unei comunicații securizate continue, şi ale propagării cheilor.

Revendicări: 3
Figuri: 5

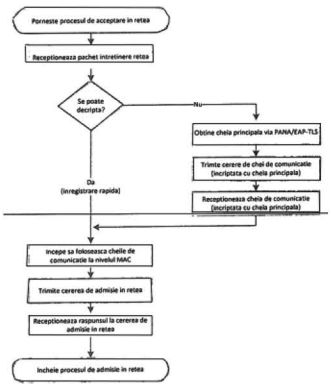

Fig. 2

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).

RO 131251 A0

OFICIUL DE STAT PENTRU INVENŢII ŞI MĂRCI
Cerere de brevet de invenţie
Nr. a 2015 00663
Data depozit 15 -09- 2015

63

Optimizarea procesului de acceptare în mod securizat într-o reţea „802.15.4e"

Invenţia se referă la o metodă de optimizare a procesului de acceptare în mod securizat într-o reţea conformă cu standardul „802.15.4e".

Invenţia este o soluţie de îmbunătăţire a domeniului Internet of Things (Internetul Obiectelor) referit în continuare prin acronimul IoT. Termenul „Internet of Things" a fost inventat de către un englez vizionar, pe numele său Kevin Ashton, în anul 1999 şi a devenit subiect de interes major abia 15 ani mai târziu. Ashton a prezis o lume a viitorului în care dispozitive inteligente se interconectează şi comunică unele cu altele contribuind astfel la apariţia de case, birouri, străzi sau oraşe inteligente care aduc societăţii o economie de timp şi de bani.
IoT reprezintă o infrastructură de reţea care leagă informaţia virtuală de obiecte tangibile (aparate) folosind captarea datelor şi comunicarea fără fir. Există numeroase domenii de aplicabilitate a IoT, de la contoare inteligente, iluminat, sisteme de transport, fabrici şi platforme industriale, până la sănătate şi monitorizarea mediului. În istoria recentă se poate observa o dezvoltare fără precedent a noilor tehnologii care dau tonul pieţei.

Stadiul de dezvoltare tehnică a IoT depinde de standardele oficiale stabilite în domeniul comunicării wireless. Pentru a putea atinge atât ţintele de cost pentru producţia de masă, cât şi interoperabilitatea între componente provenite de la producători diferiţi (dispozitive de radio frecvenţă, modemuri, routere etc.), au fost stabilite câteva standarde şi protocoale în IoT.
Cele relevante pentru stadiul actual al tehnicii pot fi găsite la următoarele surse publice:

- Standardul IEEE 802.15.4e
  - http://standards.ieee.org/findstds/index.html
  - http://standards.ieee.org/getieee802/download/802.15.4e-2012.pdf
- Protocolul de Transfer al Autentificării pentru Accesul in Reţea (Protocol for Carrying Authentication for Network Access – PANA)
  - https://tools.ietf.org/html/rfc5191
- Protocolul pentru Nivelul de Transport Securizat (Transport Layer Security – TLS)
  - https://tools.ietf.org/html/rfc5246
- Protocolul de Autentificare EAP-TLS
  - http://www.ietf.org/rfc/rfc5216.txt
- Protocolul Extensibil de Autentificare (Extensible Authentication Protocol – EAP)
  - https://tools.ietf.org/html/rfc3748.

62

IEEE 802.15.4 este un standard care specifică nivelul fizic şi controlul de acces media (MAC – Media Access Control) pentru reţelele personale de trafic redus (LR-WPANs). Standardul este întreţinut de grupul IEEE 802.15 care l-a definit în 2003. Versiunea „IEEE 802.15.4e", relevantă pentru acest standard, a fost definită în anul 2012. Standardul IEEE 802.15.4e a fost lansat pentru a defini un amendament referitor la substratul MAC (substrat al stratului 2 – Data Link Layer) al standardului deja existent 802.15.4-2006, care foloseşte strategia de schimbare a canalelor pentru a oferi mai mult sprijin pieţelor industriale şi pentru a creşte robusteţea împotriva interferenţelor externe şi a diminuării persistente a semnalelor venite pe căi multiple. Pe 6 februarie 2012, Colegiul Director al Asociaţiei pentru Standarde IEEE a aprobat standardul IEEE 802.15.4e, ceea ce a încheiat eforturile grupului 4e.

Standardul IEEE intenţionează să ofere nivelurile de bază pentru un anumit tip de reţea personală bazată pe comunicaţie fără fir (WPAN), niveluri care se axează pe o comunicare omniprezentă între dispozitive radio, cu cost scăzut şi viteză redusă. Comunicarea descrisă în standard se bazează pe tehnologia RF (radio-frecvenţă) şi poate fi aplicată în industria metrologică, pentru utilităţi, control la distanţă, IoT etc.

Protocolul de Transfer al Autentificării pentru Accesul în Reţea (Protocol for Carrying Authentication for Network Access – PANA) este un protocol bazat pe IP (Internet Protocol) care permite unui dispozitiv radio să se autentifice în reţea pentru a primi acces. PANA nu defineşte niciunul dintre protocoalele de autentificare, de distribuire a cheilor, de concordanţă a cheilor sau de derivare a lor. În acest scop se va folosi EAP (Extensible Authentication Protocol), iar PANA va prelua segmentul/componenta de date EAP.

Protocolul Extensibil de Autentificare şi Transport la Nivel de Securitate (The Extensible Authentication Protocol Transport Layer Security - EAP-TLS) oferă un mecanism standard pentru acceptarea diverselor metode de autentificare în reţele cu şi fără fir.

Referitor la schimbarea cheilor de securitate la acceptarea în reţea, din motive de management al securităţii, pentru a proteja segmentul/componenta de date transferată de la un dispozitiv radio la altul şi pentru a-l restricţiona la un grup de dispozitive radio, standardul IEEE 802.15.4e oferă soluţia cheilor preconfigurate, însă fără a defini contextul şi fluxul de comunicare. Dispozitivele radio pot fi preconfigurate cu una sau cu mai multe chei de comunicaţie. Din moment ce, teoretic, un dispozitiv radio poate comunica cu oricare altul, acelaşi set de chei preconfigurate trebuie să fie programat pe toate dispozitivele, înainte ca

acestea să se alăture reţelei. Dezavantajul acestei soluţii se relevă în situaţia în care cheile preconfigurate ale unui dispozitiv radio sunt compromise, fapt ce atrage după sine compromiterea tuturor dispozitivelor radio din acea reţea. Este posibil ca reconfigurarea cheilor preconfigurate pe toate dispozitivele radio să nu fie o soluţie validă deoarece este una foarte costisitoare.

În cazul altor standarde cum ar fi, de exemplu, PANA/EAP-TLS, sunt prezentate mecanismele pentru asigurarea unui nivel optim de securitate la admiterea în reţea. Dezavantajele aplicării în practică a acestor principii constau într-un consum mare al benzii de radio-frecvenţă şi un proces lent de înregistrare.

Problemele tehnice pe care le rezolvă invenţia rezidă în înregistrarea lentă la admisia în reţea în cadrul protocoalelor PANA şi EAP-TLS şi în nivelul redus de securitate la acceptarea în reţea în cadrul standardului „IEEE 802.15.4e".

În ceea ce priveşte nivelul de securitate la acceptarea în reţea, standardul „IEEE 802.15.4 e" doar nominalizează soluţia cheilor preconfigurate. Conform standardului, există un singur set de chei preconfigurate folosite permanent pentru reţea. Prin implementarea metodei prevăzute de acest standard, reţeaua este foarte expusă la atacuri externe şi la scurgeri de informaţii privind segmentul de date. De asemenea, standardul „IEEE 802.15.4e" nu defineşte modul de configurare a cheilor şi nici administrarea cheilor de comunicaţie.

Soluţia la problema tehnică constă în dezvoltarea unei metode aplicabile într-o reţea 802.15.4e constând într-un procedeu de admisie rapidă **atunci când o altă admisie completă a fost făcută în aceeaşi reţea**, cu respectarea normelor de securitate ale protocoalelor PANA/EAP-TLS, completat de un procedeu de schimbare a cheilor de comunicaţie la acceptarea în reţea şi un procedeu de administrare a cheilor pe durata de viaţă, conform cărora un dispozitiv cu comunicare în radio-frecvenţă 802.15.4e va avea la dispoziţie tot timpul două chei ale căror durate de viaţă se suprapun parţial, astfel încât să fie asigurate premisele unei comunicaţii securizate continue şi ale propagării cheilor.

Invenţia de faţă introduce o noutate tehnologică cu plajă largă de utilizare. Aceasta prezintă caracteristici tehnice aplicabile în sisteme mai mari de dispozitive radio (până la zeci de mii de dispozitive) numite „obiecte inteligente" (eng. Smart Objects). Ele detectează şi comunică cu diferite tehnologii, oferind astfel o varietate de soluţii utilizatorilor. Integrarea echipamentelor

şi cea a datelor sunt două procese interdependente deoarece se bazează pe tehnologia sistemelor de calcul integrat în obiecte, care le manevrează şi le monitorizează după cum urmează:

- Le interoghează şi le determină să strângă informaţii; ca atare, sunt folosite ca metode de comunicare;
- Le schimbă starea şi informaţia care le este asociată, forţându-le să execute comenzi;
- Se asigură că dispozitivele radio vor capta interacţiunile dintre stările interne ale componentelor infrastructurii şi mediul extern.

În continuare se prezintă, pe scurt, câteva domenii de aplicare a obiectului invenţiei, selectate în funcţie de gradul de importanţă şi anume:

1. Sisteme automate de citire a contoarelor

   Reprezintă o tehnologie care colectează automat date despre consum, diagnostic şi stare din contoarele de apă sau energie (electricitate, gaze) şi le transferă către baza de date centrală unde pot fi folosite în activitatea de facturare a serviciilor sau în cea de analiză şi depanare a sistemului.

   Beneficiile pe care le aduc astfel de sisteme sunt:

   - scutirea companiei furnizoare de cheltuielile deplasărilor periodice la locul unde este instalat contoarul pentru a-l citi
   - facturarea se poate face pe baza unui consum măsurat aproape în timp real în schimbul unei estimări pe baza unor consumuri înregistrate anterior
   - companiile furnizoare, pe de o parte, pot controla mai bine producţia de energie electrică, gaze sau apă, iar clienţii, pe de altă parte, pot gestiona mai bine consumul acestora.

2. Sisteme inteligente de iluminat stradal

   Cunoscute şi sub numele de iluminat stradal adaptativ, aceste sisteme reacţionează la mişcarea pietonilor, cicliştilor sau a maşinilor făcând ca intensitatea luminii să scadă atunci când nu este detectată nicio mişcare şi respectiv, să crească atunci când apare mişcare.

   Printre beneficiile a astfel de sisteme se numără economia de energie, costurile de mentenanţă reduse şi nivelurile de emisii de CO_2 mai mici.

3. Automatizare industrială şi reţele de senzori fără fir

Asigură măsurători de mentenanţă, diagnosticarea proceselor, optimizare şi control. De exemplu, pot fi menţionate aici numeroase aplicaţii pentru macarale, vehicule cu pilot automat, precum şi control la distanţă al diferitelor dispozitive şi maşini.

Beneficiile acestor aplicaţii sunt:

- reducerea costurilor generate de utilizarea cablurilor
- asigurarea unui flux îmbunătăţit al informaţiei în fabrici - datele despre fabrică şi procesele din interiorul ei sunt disponibile oriunde datorită senzorilor fără fir; de asemenea, îmbunătăţeşte calitatea datelor
- îmbunătăţirea productivităţii, a managementului activelor şi a distribuirii controlului
- mobilitate - elimină nevoia de a avea panouri de control fixe, care pot fi amplasate în locuri cu acces dificil sau în locuri unde costul pentru a trage fire nu este justificat
- scalabilitate - odată instalaţi, senzorii fără fir sunt scalabili. Noi senzori pot fi adăugaţi cu costuri reduse
- interoperabilitate - ajuta la interconectarea fabricilor şi a platformelor industriale
- pot fi folosiţi atât în interior, cât şi în exterior, chiar şi în condiţii meteorologice extreme.

4. Sisteme fără fir pentru automatizarea clădirilor

Numite şi sisteme de management al clădirii sau sisteme de automatizare a clădirii, aceste sisteme asigură controlul automatizat şi centralizat al încălzirii, al ventilaţiei, al aerului condiţionat, al luminii etc., dintr-o clădire.

Principalele avantaje ale acestor sisteme sunt: nivel mai mare de confort pentru ocupanţii clădirii, operarea mai eficientă a sistemelor clădirii şi reducerea costurilor cu energia şi a celor de operare.

5. Reţea inteligentă

Este o reţea modernizată de energie electrică care foloseşte tehnologia informaţiei şi a comunicaţiilor pentru a strânge şi pentru a analiza date despre producţia şi distribuţia electricităţii.

Avantajele acestor reţele inteligente se constituie în îmbunătăţirea eficienţei, a fiabilităţii, reducerea costurilor, precum şi durabilitatea sistemului de furnizare a energiei electrice si adaptarea lui la nevoile consumatorilor.

Se dă în continuare un exemplu de realizare a invenţiei în legătură cu figurile 1 - 5 care reprezintă:

- Figura 1 – exemplu de reţea standard „802.15.4e"
- Figura 2 – schema logică a unui proces standard de acceptare într-o reţea securizată de tipul „802.15.4e"
- Figura 3 – schema logică a procesului de schimbare a cheilor de comunicaţie la acceptarea în reţea
- Figura 4 – exemplu de administrare a cheilor de securitate de-a lungul duratei lor de viaţă
- Figura 5 - utilizarea cheilor de securitate în timpul perioadelor consecutive.

Obiectului invenţiei de faţă se utilizează în cadrul reţelelor securizate conforme cu standardul "802.15.4e", cu căi formate din mai multe segmente (multi-hop), pentru admiterea în reţea în condiţii de securitate şi viteză sporite, inclusiv schimbul şi managementul cheilor de securitate. Nivelul MAC (Media Access Control) conform cu standardul "802.15.4e" efectuează autentificare şi criptare bazată pe chei de comunicaţie. Modalitatea în care cheile sunt schimbate şi menţinute este în afara scopului standardului "802.15.4e". Invenţia noastră oferă soluţii de configurare şi menţinere în condiţii optime a cheilor de comunicaţie.

Componentele unei reţele care respectă standardul "802.15.4 e", care sunt folosite în cadrul invenţiei, sunt prezentate mai jos:

- Un dispozitiv cu comunicare în radio-frecvenţă „802.15.4e" este un dispozitiv de tip RF (radio-frecvenţă) care respectă protocolul "802.15.4e". Acesta va fi denumit în continuare „dispozitiv radio", „dispozitiv RF" sau simplu, „dispozitiv".
- Un router "802.15.4e" de tip RF este un dispozitiv radio "802.15.4e" care poate ruta pachete "802.15.4 e" de la un dispozitiv radio "802.15.4e" la alt dispozitiv "802.15.4e" . Acesta va fi denumit în continuare „router RF".
- Un administrator de reţea „802.15.4e" este un dispozitiv care controlează întreaga reţea "802.15.4e", o reţea "802.15.4e" putând să aibă unul sau mai multe dispozitive radio structurate pe unul sau mai multe canale. Această componentă va fi denumită in continuare „coordonator reţea".

Schema unei reţele „802.15.4e", cu comunicaţie prin radio-frecvenţă, este exemplificată în figura 1. O reţea ce respectă standardul "802.15.4e" este compusă dintr-un număr de dispozitive (care poate varia de la unul până la câteva mii) şi un coordonator reţea. Comunicaţia

dintre dispozitive se realizează prin tehnica de RF (radio-frecvenţă) şi este în conformitate cu formatele reglementate prin standardul „802.15.4e" şi cu modalitatea de utilizare a benzilor RF. Reţeaua are topologie distribuită care permite dispozitivelor să comunice cu alte dispozitive prin unul sau mai multe canale. Coordonatorul reţea permite mesajelor conforme cu standardul „802.15.4e" să fie rutate în cadrul reţelei „802.15.4e" sau către alte reţele externe.

În momentul în care un dispozitiv încearcă să se înregistreze într-o reţea, acesta va căuta toate reţelele active din apropierea sa şi va încerca să prindă un pachet periodic pentru întreţinere reţea, îmbunătăţit. Acest pachet periodic pentru întreţinere reţea conţine „Secţiunea pachetului cu elementele de informaţii", inclusiv informaţii de bază cu privire la configuraţia reţelei, ca de exemplu: prioritatea înregistrării în reţea, schimbarea canalelor, setările cuantelor de timp, timpul curent din numărul cuantei de timp şi setul de cuante de bază, precum şi legăturile folosite în timpul procesului de înregistrare. Odată ce pachetul periodic pentru întreţinere reţea îmbunătăţit este recepţionat, admiterea în reţea poate fi iniţiată. Dispozitivul are o aplicaţie de administrare responsabilă cu configurarea de tip „802.15.4e".

Un proces complet de înregistrare "802.15.4e" se realizează prin parcurgerea paşilor d1) - d11) ai metodei prezentate în continuare, conform figurii 2:

d1) Un dispozitiv aşteaptă un pachet periodic pentru întreţinere reţea îmbunătăţit;

d2) Dispozitivul primeşte pachetul periodic pentru întreţinere reţea îmbunătăţit de la un router RF;

d3) Dispozitivul configurează setările reţelei conform elementelor de informaţie cuprinse în pachetul periodic pentru întreţinere reţea îmbunătăţit;

d4) Dispozitivul iniţiază o sesiune PANA/EAP-TLS cu routerul RF. Router-ul RF se comportă ca un releu PANA/EAP-TLS cu un server PANA al coordonatorului reţea;

d5) Dispozitivul primeşte cheia principală la sfârşitul sesiunii PANA/EAP-TLS;

d6) Dispozitivul trimite comanda „ia cheia de comunicaţie" criptată şi autentificată cu cheia principală;

d7) Dispozitivul primeşte răspunsul cheii de comunicaţie criptat şi autentificat cu cheia principală;

d8) Dispozitivul începe să folosească noile configurări ale nivelului de securitate;

d9) Dispozitivul trimite o comandă de tipul „cerere înregistrare" către coordonatorul reţea;

d10) Dispozitivul primeşte răspunsul de înregistrare;

d11) Dispozitivul începe să utilizeze configurările de rețea folosite în răspunsul de înregistrare.

Optimizarea obținută prin aplicarea metodei de mai sus, obiect al invenției noastre, sporește și îmbunătățește posibilitățile standardului „IEEE 802.15.4e" și ale protocoalelor PANA/EAP-TLS. În cazul în care o rețea este configurată fără aceste caracteristici inovative, unul din evenimentele de mai jos va avea loc:

- Dacă dispozitivul este configurat în așa fel încât să nu folosească PANA/EAP-TLS, pașii d4) și d5) sunt omiși, iar dispozitivul va folosi o cheie principală preconfigurată în timpul fazei de configurare inițială a schimburilor de chei pentru comunicarea pachetelor de date. Consecința va fi o securizare slabă a rețelei.
- Daca dispozitivul este configurat în așa fel încât să nu folosească schimbul cheilor de comunicație, atunci pașii d4), d5), d6) și d7) sunt omiși, iar dispozitivele folosesc configurările nivelului de securitate preconfigurate în timpul fazei de configurare inițială. Consecința va fi o securizare slabă a rețelei.

În general, când un dispozitiv detectează o rețea validă, inițiază procesul de acceptare în rețea. Acest proces, descris în detaliu prin pașii d1) – d11), poate fi redat sintetic prin gruparea acestora în secvența de pași a1) – a4) astfel :

a1) Căutarea rețelei – pașii d1) – d3);

a2) Negocierea cheii principale – pașii d4) și d5);

a3) Schimbarea cheilor de comunicație – pașii d6) – d8);

a4) Înregistrarea – pașii d9) – d11).

La *pasul a1)*, dispozitivul nu este încă înregistrat, așadar începe să caute o rețea și așteaptă să recepționeze un pachet periodic pentru întreținere rețea.

La *pasul a2)*, negocierea cheii principale se realizează în conformitate cu protocoalele PANA/EAP-TLS și poate fi configurată ca și:

- algoritm simetric al cheilor– folosind chei pre-configurate;
- algoritm asimetric al cheilor – folosind certificate.

La sfârșitul acestui pas, valoarea aceleiași chei principale este cunoscută de către ambele părți (dispozitiv și coordonator rețea).

La *pasul a3)*, dispozitivul trimite un mesaj de tipul „cerere de cheie de comunicaţie" criptat şi autentificat cu cheia principală obţinută la pasul a2).
Coordonatorul reţea decriptează mesajul şi trimite înapoi valoarea cheii de comunicaţie criptată şi autentificată cu cheia principală obţinută la pasul a2). La finalul pasului a3), dispozitivul este capabil să cripteze şi să decripteze orice mesaj de la reţeaua din care face parte.

La *pasul a4)*, folosind configurările nivelului de securitate (cheile de comunicaţie şi nivelul de criptare) primite la pasul a3), dispozitivul trimite cererea de înregistrare „802.15.4e" către coordonatorul reţea. Acesta trimite înapoi răspunsul de înregistrare, iar acceptarea în reţea este finalizată.

Odată ce dispozitivul primeşte cheile de comunicaţie, stochează aceste chei în asociere cu identificatorul reţelei din care face parte. Dacă un dispozitiv anulează înregistrarea din reţea şi are nevoie ulterior să se reînregistreze, atunci va putea sări paşii a2) şi a3) şi va realiza direct pasul a4) folosind configurările nivelului de securitate. Procesul de a sări peste paşii a2) şi a3) este denumit „Detectarea înregistrării rapide şi în condiţii de securitate" şi are loc atunci când dispozitivul a parcurs anterior un proces complet de înregistrare "802.15.4e" în reţea şi, în consecinţă, sunt îndeplinite simultan condiţiile c1) – c3) de mai jos:

c1) Configurările nivelului de securitate pentru reţeaua curentă sunt deja stocate de către dispozitiv;

c2) Cheia cu identificatorul cheii folosit de reţeaua curentă este inclusă în datele de autentificare stocate;

c3) Dispozitivul este capabil să valideze cu succes semnătura de securitate a pachetului periodic pentru întreţinere reţea primit.

Dacă cel puţin una dintre aceste condiţii nu este adevărată, atunci configurările nivelului de securitate asociate cu reţeaua curentă sunt înlăturate şi întregul proces de înregistrare în condiţii de securitate este reînceput.

În continuare se descrie procesul de schimbare a cheilor de comunicaţie la acceptarea în reţea, în conformitate cu schema logică prezentată în figura 3.
Răspunsul la cererea de chei de comunicaţie conţine:

- nivelul "802.15.4e" de securitate;
- cheia de comunicaţie curentă;
- următoarea cheie de comunicaţie.

Dispozitivul păstrează una sau mai multe chei pentru reţeaua curentă. Fiecare cheie are:

- un identificator unic – acelaşi folosit în "802.15.4e" MAC security header;
- un moment de start – timp universal coordonat (UTC - Coordinated Universal Time)
- sfârşitul duratei de viaţă - timp universal coordonat
- o valoare a cheii – de 128 biţi.

Când durata de viaţă a unei chei a expirat, aceasta va fi ştearsă în mod automat de către dispozitiv.

În timpul procesului de criptare, nivelul MAC de securitate "802.15.4e" foloseşte ultima cheie validă (condiţie de validitate: momentul de start să fie mai mic faţă de momentul curent UTC). În timpul criptării, nivelul MAC de securitate caută cheia setată ca şi cheie identificator în depozitul de chei.

Când dispozitivul de administrare chei rămâne cu o singură cheie, în mod automat lansează o nouă cerere până când primeşte noul set de chei.

În vederea asigurării unei comunicaţii securizate continue, cheile consecutive trebuie să se suprapună o perioadă pentru a permite propagarea cheilor.

Exemplul administrării cheilor pe parcursul duratei lor de viaţă este prezentat în figura 4, iar modul în care se suprapun paşii prezentaţi până acum este explicat mai jos.

Asignarea cheilor şi suprapunerea lor are următoarea structură:

- Cheia 1 are data de start T şi data de sfârşit T+40 zile;
- Cheia 2 are data de start T+30 şi data de sfârşit T+70 zile;
- Cheia 3 are data de start T+60 şi data de sfârşit T+100 zile;
- Cheia 4 are data de start T+90 şi data de sfârşit T+130 zile;
- Şi aşa mai departe, în mod continuu în ciclul vieţii cheilor de comunicaţie.

Utilizarea cheilor în timpul perioadelor consecutive este arătată în tabelul din figura 5.

Momentul de timp T este momentul formării reţelei, când sunt disponibile două chei, Cheia 1 şi Cheia 2. La momentul T+30, Cheia 2 devine cheie principală ceea ce înseamnă că va fi folosită pentru criptare. Pentru decriptare, dispozitivul poate folosi Cheia 1 sau Cheia 2 (in funcţie de cheia identificator din începutul mesajului 802.15.4e). La momentul (T+40) durata de viaţă a Cheii 1 expiră, iar un mesaj de tip „cerere cheie" este trimis pentru a primi Cheia 3. Cu scopul de a-şi menţine posibilitatea de comunicare, Cheia 3 trebuie să fie acceptată până la

momentul (T+60). Acest ciclu este repetat continuu cât timp dispozitivul este parte din reţeaua RF.

Se prezintă în continuare utilitatea şi beneficiile pentru piaţă şi pentru utilizatorii săi finali ale metodei de optimizare a procesului de acceptare în mod securizat într-o reţea „802.15.4e", obiect al invenţiei noastre.

Tehnologia bazată pe radio-frecvenţă şi reţelele de senzori wireless au un impact covârşitor asupra industriilor globale şi un rol în transformarea lor. De-a lungul ultimilor ani, aceste pieţe au avut o creştere semnificativă dublându-şi dimensiunile, cu perspective de evoluţie mult mai accentuate în viitor, pe măsură ce dezvoltatorii creează noi tehnologii. Aşa cum s-a arătat anterior, la momentul prezentării domeniilor de aplicare a invenţiei, exista o nevoie presantă pentru reţele mari, cu mii de dispozitive poziţionate în mod omniprezent. Abilitatea lor de a recepţiona şi de a interpreta date joaca un rol semnificativ în automatizări şi în IoT. Noua direcţie este orientată către teleoperare şi teleprezenţă, pentru dobândirea abilităţii de a monitoriza şi de a controla aceste dispozitive de la distanţă. Aşadar, exista o schimbare in cercetare în sensul integrării conceptelor de securitate inteligentă şi viteză crescută a operării în structuri mari de reţele.

Companiile de electronice şi de reţele, ca şi noi de altfel, au investit semnificativ în activităţile de cercetare-dezvoltare, proiecte ce contribuie la creşterea pieţei IoT. Ne aşteptăm să înregistrăm creşteri importante în venituri, cu livrări în masă în următorii 5, 6 ani.

Am testat invenţia noastră în reţele mari simulate în laboratoarele performante ale companiei. Am înregistrat rezultate pozitive după efectuarea de scenarii de testare complexe. Astfel, tehnologia inovativă dezvoltată de compania noastră a trecut toate criteriile de acceptanţă, printre care menţionăm:

- Crearea unei combinaţii unice între viteză şi securitate la înregistrarea dispozitivelor în reţea, cu rezultate directe în economisirea timpului şi a banilor clienţilor;
- De 200% de ori înregistrare mai rapidă relativ la implementarea stadiului tehnic actual.

Aceste caracteristici inovative au un efect tehnic suplimentar asupra componentelor tangibile din reţea: ele sporesc viteza cu care dispozitivele, router-ul RF şi coordonatorul reţea funcţionează. Creăm astfel condiţiile ca reţelele mari să devina fezabile în contextul unei securităţi robuste, chiar dacă sunt formate din mii de dispozitive.

Invenţia noastră produce rezultate concrete şi utile nu doar pentru compania noastră, ci şi pentru o gamă largă de părţi interesate: furnizori de materii prime şi echipamente de producţie, furnizori de soluţii OEM (producători de echipamente originale), distribuitori şi vânzători cu amănuntul, organizaţii de cercetare, forumuri, asociaţii.

Se prezintă, în cele ce urmează, avantajele invenţiei de faţă în raport cu stadiul actual al tehnicii.

Indicaţiile oferite în standardele şi protocoalele existente (IEEE 802.15.4e, PANA, EAP, TLS) limitează foarte mult flexibilitatea în construirea reţelelor mari şi au un nivel scăzut de securitate. Totuşi, standardele nu sunt exhaustive şi permit inovaţii în limitele recomandate. Aceste probleme de securitate şi flexibilitate pot fi rezolvate cu soluţii inventive. În urma unui efort considerabil de cercetare şi dezvoltare în domeniul tehnologiei fără fir, compania noastră a obţinut rezultate cu aplicabilitate practică, care rezolvă limitările standardelor şi le îmbunătăţesc cu soluţii inovative. Compania caută în mod constant proiecte care împing tehnologia fără fir la limită, fiind prima din piaţă care a oferit soluţii pentru următoarele probleme tehnice:

- Standardul IEEE 802.15.4e are un nivel de securitate scăzut şi nu schimbă în mod dinamic setul de chei pentru admisia în reţea;
- Atunci când sunt implementate, protocoalele PANA/EAP/TLS scad viteza înregistrării din cauza consumului ridicat de bandă de radio-frecvenţă.

a-2015--00663-
15-09-2015

REVENDICĂRI

1. Metodă de detectare a înregistrării rapide şi în condiţii de securitate a unui dispozitiv RF într-o reţea conformă cu standardul „802.15.4e" în care un proces de admisie completă în reţea a unui dispozitiv RF se realizează prin parcurgerea paşilor d1) – d11) în care următoarele acţiuni au loc

   d1) Un dispozitiv aşteaptă un pachet periodic pentru întreţinere reţea îmbunătăţit;

   d2) Dispozitivul primeşte pachetul periodic pentru întreţinere reţea îmbunătăţit de la un router RF;

   d3) Dispozitivul configurează setările reţelei conform elementelor de informaţie cuprinse în pachetul periodic pentru întreţinere reţea îmbunătăţit;

   d4) Dispozitivul iniţiază o sesiune PANA/EAP-TLS cu routerul RF. Router-ul RF se comportă ca un releu PANA/EAP-TLS cu un server PANA al coordonatorului reţea;

   d5) Dispozitivul primeşte cheia principală la sfârşitul sesiunii PANA/EAP-TLS;

   d6) Dispozitivul trimite comanda „ia cheia de comunicaţie" criptată şi autentificată cu cheia principală;

   d7) Dispozitivul primeşte răspunsul cheii de comunicaţie criptat şi autentificat cu cheia principală;

   d8) Dispozitivul începe să folosească noile configurări ale nivelului de securitate;

   d9) Dispozitivul trimite o comandă de tipul „cerere înregistrare" către coordonatorul reţea;

   d10) Dispozitivul primeşte răspunsul de înregistrare;

   d11) Dispozitivul începe să utilizeze configurările de reţea folosite în răspunsul de înregistrare,

   caracterizată prin aceea că etapele de negociere a cheii principale - paşii d4) şi d5) - şi de schimbare a cheilor de comunicaţie - paşii d4), d5) şi d6) - pot fi omise atunci când o altă admisie completă în reţea a aceluiaşi dispozitiv a avut loc anterior.

2. Metodă de autentificare a unui dispozitiv RF într-o reţea „802.15.4e", conform revendicării 1, **caracterizată prin aceea că**, schimbul de chei de comunicaţie se realizează printr-un proces repetitiv în care dispozitivul RF şterge în mod automat o cheie a cărei durată de viaţă a expirat, în care nivelul MAC de securitate foloseşte în timpul procesului de criptare ultima cheie validă, în care nivelul MAC de securitate caută cheia setată ca şi cheie identificator în

depozitul de chei, în care dispozitivul de administrare chei, atunci când rămâne cu o singură cheie, lansează în mod automat o nouă cerere până când primeşte noul set de chei şi în care cheile consecutive se suprapun o perioadă pentru a permite propagarea cheilor, proces descris prin paşii k1) – k11) după cum urmează:

k1) Se încearcă poziţionarea pe prima cheie din depozitul de chei al dispozitivului de administrare chei.

k2) Se verifică dacă există cheie.

Dacă răspunsul este DA, atunci se continuă cu pasul k3.

Dacă răspunsul este NU, atunci se continuă cu pasul k9.

k3) Se verifică dacă cheia citită din depozitul de chei este expirată.

Dacă răspunsul este DA, atunci se continuă cu pasul k4.

Dacă răspunsul este NU, atunci se continuă cu pasul k5.

k4) Se şterge cheia expirată şi se face salt la pasul k6.

k5) Se verifică dacă timpul de start al cheii citite este valid.

Dacă răspunsul este DA, atunci se face salt la pasul k7.

Dacă răspunsul este NU, atunci se continuă cu pasul k6.

k6) Se încearcă poziţionarea pe următoarea cheie din depozitul de chei al dispozitivului de administrare chei şi apoi se face salt la pasul k2.

k7) Se verifică dacă cheia are cel mai apropiat timp de start faţă de timpul curent.

Dacă răspunsul este DA, atunci se continuă cu pasul k8.

Dacă răspunsul este NU, atunci se face salt la pasul k6.

k8) Se setează cheia citită ca şi cheie curentă „802.15.4" şi apoi se face salt la k6.

k9) Se verifică dacă dispozitivul are toate cheile necesare.

Dacă răspunsul este DA, atunci se face salt la k11.

Dacă răspunsul este NU, atunci continuă cu pasul k10.

k10) Dispozitivul trimite către coordonatorul reţea un mesaj de tipul „cerere de cheie de comunicaţie" până când primeşte un nou set de chei.

k11) Încheiere proces de verificare administrare chei.

3. Metodă de administrare a cheilor pe parcursul duratei lor de viaţă, utilizată într-o metodă de autentificare a unui dispozitiv RF într-o reţea „802.15.4e", conform revendicării 2, **caracterizată prin aceea că**, atribuirea cheilor şi suprapunerea lor se face după regula

conform căreia *Cheia n* are data de start $T\cdot(n-1)\cdot \Delta_{start}$ şi data de sfârşit $T\cdot(n-1)\cdot \Delta_{start}+ \Delta_{viata}$, unde T este momentul formării reţelei, *n* e număr natural şi n ≥1, Δ_{viata} şi Δ_{start} sunt două constante pozitive reprezentând durata de viaţă a unei chei şi respectiv, întârzierea datei de start a unei chei faţă de data de start a cheii precedente, $0 < \Delta_{start} < \Delta_{viata}$, regulă care asigură suprapunerea a oricăror două chei consecutive *Cheia n* şi *Cheia (n+1)*, pe parcursul unui interval de timp $\Delta_{viata} - \Delta_{start}$ care încheie ciclul de viaţă al primeia dintre cele două chei, iar utilizarea cheilor în timpul perioadelor consecutive se face după regulile u1) – u7) descrise în continuare:

u1) La momentul de timp *T* al formării reţelei sunt disponibile două chei, Cheia 1 si Cheia 2;

u2) În intervalul $[T, T+ \Delta_{start}]$ Cheia 1 este folosită atât pentru criptare, cât şi pentru decriptare;

u3) La momentul $(T+ \Delta_{start})$, Cheia 2 devine cheie principală;

u4) În intervalul $[T+ \Delta_{start}, T+ \Delta_{viata}]$ Cheia 2 va fi folosita pentru criptare, iar pentru decriptare dispozitivul poate folosi Cheia 1 sau Cheia 2, în funcţie de cheia identificator din începutul mesajului 802.15.4e;

u5) La momentul $(T+ \Delta_{viata})$, durata de viaţă a Cheii 1 expiră, iar un mesaj de tipul „cerere cheie" este trimis pentru a primi Cheia 3;

u6) În intervalul $[T+ \Delta_{viata}, T+2\cdot \Delta_{start}]$ Cheia 2 este folosită atât pentru criptare, cât şi pentru decriptare, iar dispozitivul primeşte Cheia 3 pentru a-şi putea menţine posibilitatea de comunicare cu reţeaua RF;

u7) Ciclul u3) – u6) este repetat continuu cât timp dispozitivul este parte din reţeaua RF, cu precizarea că momentele de timp şi cheile utilizate într-un nou ciclu glisează spre dreapta astfel încât momentul referit la o nouă parcurgere a pasului u3) să fie înlocuit cu limita dreaptă a intervalului referit la ultima parcurgere a pasului u6), iar cheia referită la o nouă parcurgere a pasului u3) să fie înlocuită cu cheia obţinută de dispozitiv la ultima parcurgere a aceluiaşi pas u6).

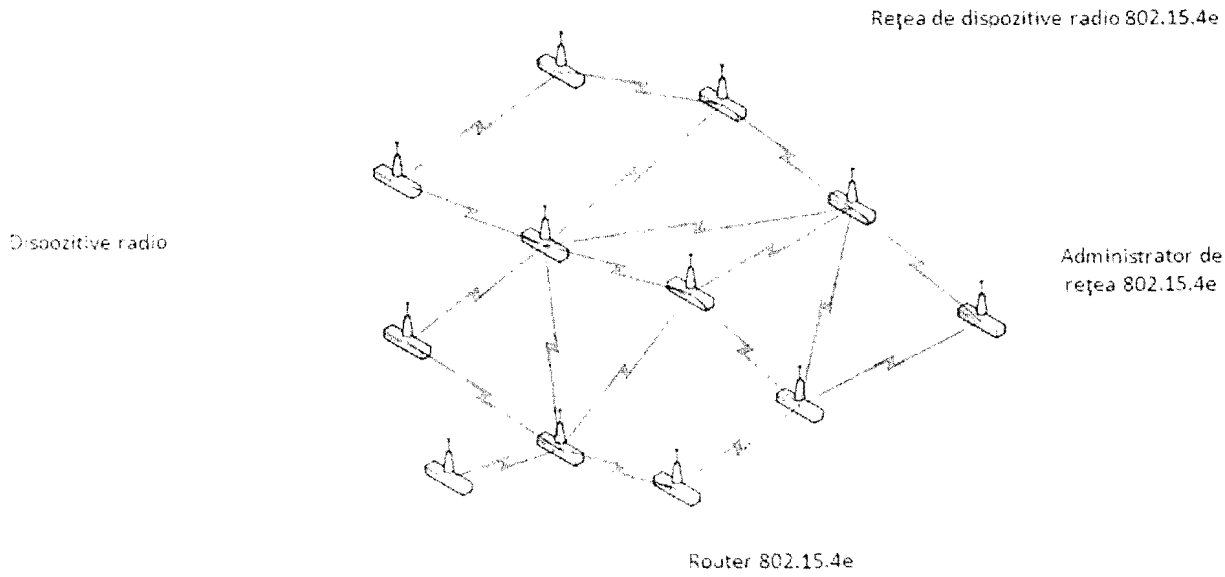
Rețea de dispozitive radio 802.15.4e
Dispozitive radio
Administrator de rețea 802.15.4e
Router 802.15.4e

Figura 1

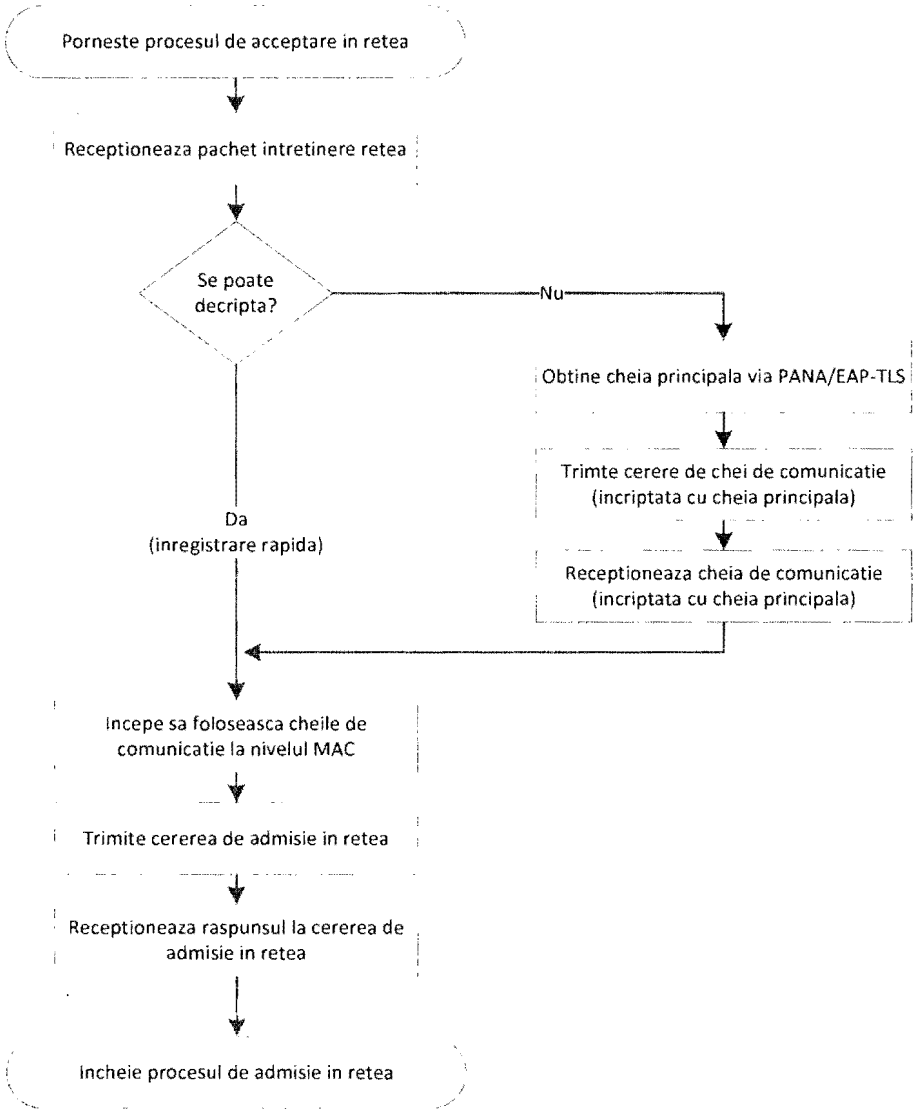
Porneste procesul de acceptare in retea
Receptioneaza pachet intretinere retea
Se poate decripta?
Nu
Obtine cheia principala via PANA/EAP-TLS
Trimte cerere de chei de comunicatie (incriptata cu cheia principala)
Receptioneaza cheia de comunicatie (incriptata cu cheia principala)
Da (inregistrare rapida)
Incepe sa foloseasca cheile de comunicatie la nivelul MAC
Trimite cererea de admisie in retea
Receptioneaza raspunsul la cererea de admisie in retea
Incheie procesul de admisie in retea

Figura 2

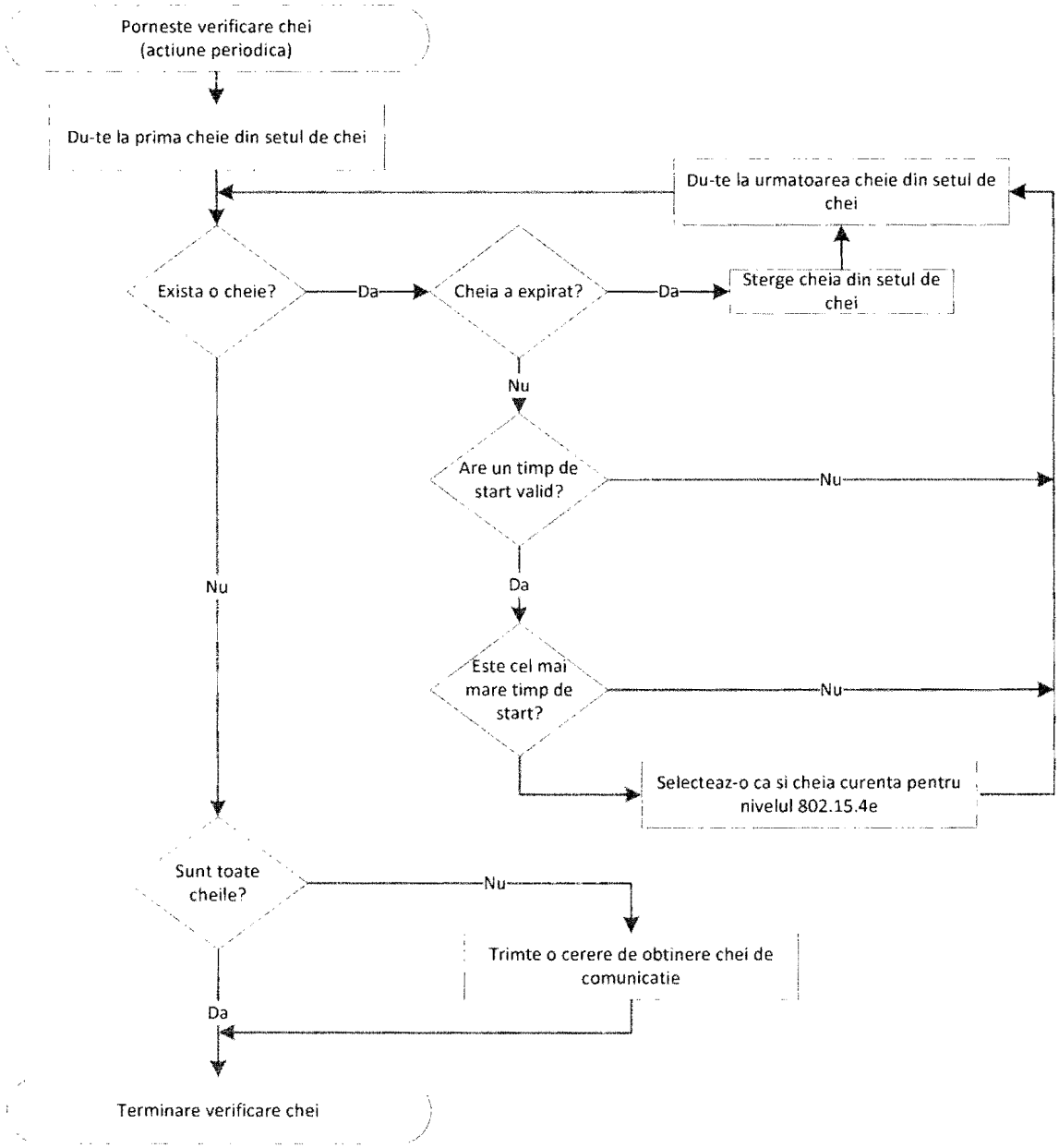
Porneste verificare chei (actiune periodica)
Du-te la prima cheie din setul de chei
Du-te la urmatoarea cheie din setul de chei
Exista o cheie?
Da
Cheia a expirat?
Da
Sterge cheia din setul de chei
Nu
Are un timp de start valid?
Nu
Da
Este cel mai mare timp de start?
Nu
Selecteaz-o ca si cheia curenta pentru nivelul 802.15.4e
Nu
Sunt toate cheile?
Nu
Trimte o cerere de obtinere chei de comunicatie
Da
Terminare verificare chei

Figura 3

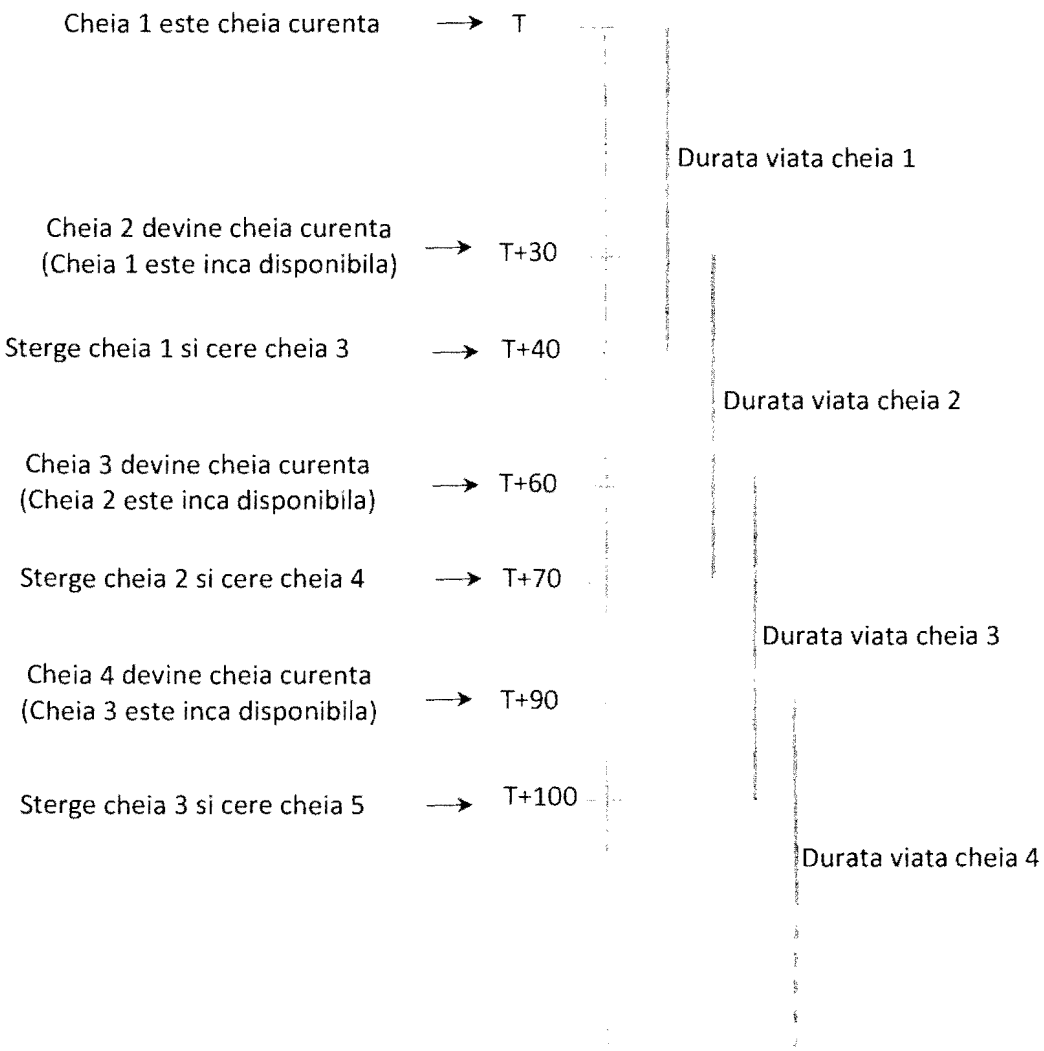
Cheia 1 este cheia curenta → T
Durata viata cheia 1
Cheia 2 devine cheia curenta
(Cheia 1 este inca disponibila) → T+30
Sterge cheia 1 si cere cheia 3 → T+40
Durata viata cheia 2
Cheia 3 devine cheia curenta
(Cheia 2 este inca disponibila) → T+60
Sterge cheia 2 si cere cheia 4 → T+70
Durata viata cheia 3
Cheia 4 devine cheia curenta
(Cheia 3 este inca disponibila) → T+90
Sterge cheia 3 si cere cheia 5 → T+100
Durata viata cheia 4

Figura 4

Interval	Utilizare
T ... T−30	Cheia 1 este folosită atât pentru criptare, cât și pentru decriptare.
T−30 ...T−40	Cheia 2 este folosită pentru criptare, Cheia 1 și Cheia 2 sunt folosite pentru decriptare.
T−40 ...T−60	Cheia 2 este folosită atât pentru criptare, cât și pentru decriptare, primește Cheia 3
T−60 ...T−70	Cheia 3 este folosită pentru criptare. Cheia 2 și Cheia 3 sunt folosite pentru decriptare.
T−70 ...T−90	Cheia 3 este folosită atât pentru criptare, cât și pentru decriptare, primește Cheia 4
T−90 ...T−100	Cheia 4 este folosită pentru criptare. Cheia 3 și Cheia 4 sunt folosite pentru decriptare.

Figura 5