(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 137270 A2**
(51) **Int.Cl.**
***H04W 4/02*** (2009.01);
***H04W 64/00*** (2009.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2021 00436**

(22) Data de depozit: **28/07/2021**

(41) Data publicării cererii:
**30/01/2023** BOPI nr. **1/2023**

(71) Solicitant:
• **UNIVERSITATEA "ALEXANDRU IOAN CUZA" DIN IAŞI**, *BD. CAROL I NR. 11, IAŞI, IS, RO;*
• **HEAVEN SOLUTIONS 2005 S.R.L.**, *STR.ARCU, NR.31, BL.C15, SC.A, AP.24, IAŞI, IS, RO*

(72) Inventatori:
• **BARAN ANDREI BOGDAN**, *SAT COADA STÂNCII, COMUNA UNGHENI, IS, RO;*
• **ALBOAIE LENUŢA**, *STR.PROF.IOAN PETRU CULIANU NR.58, IAŞI, IS, RO;*
• **ALBOAIE SÎNICĂ**, *STR.COSTACHE NEGRII NR.39, BL.Z2, AP.36, IAŞI, IS, RO*

*Această publicaţie include şi modificările descrierii, revendicărilor şi desenelor depuse conform art.35 alin.(20) din HG nr.547/2008*

(54) # SISTEM DE LOCALIZARE A UNUI GRUP DE TURIŞTI PE DISTANŢE MARI CE ASIGURĂ PROTECŢIA ŞI CONFIDENŢIALITATEA DATELOR PERSONALE

(57) **Rezumat:**

Invenţia se referă la un sistem de localizare pe distanţe mari, a unui grup de turişti, cu asigurarea protecţiei şi confidenţialităţii datelor personale. Sistemul, conform invenţiei, cuprinde un dispozitiv hardware portabil pentru fiecare utilizator înregistrat într-o reţea de tip mesh alcătuită din trei tipuri de noduri: nod master (**M**) cu rol de coordonator şi centru de încredere, nod router secundar (**RS**) cu rol de propagare a mesajelor dintr-o sub-reţea şi de extindere a acesteia, şi un nod terminal (**T**) care comunică cu restul nodurilor prin Bluetooth şi tehnici de triangulare, informaţiile fiind distribuite între noduri într-un mod criptat folosind identificatori descentralizaţi (**DID-W3C**) şi tehnici criptografice, de exemplu semnături digitale.

Revendicări iniţiale: 2
Revendicări amendate: 1
Figuri: 3

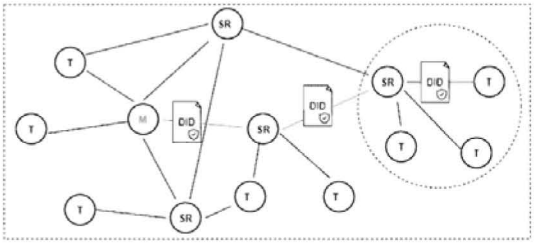


**Fig. 1**



RO 137271 A2

**Sistem de localizare a unui grup de turişti pe distanţe mari ce asigură protecţia şi confidenţialitatea datelor personale**

În descrierea invenţiei vom folosi următoarele noţiuni:

- LBS - serviciu bazat pe locaţie/server de localizare
- DID - identificator descentralizat
- DLT - registru de date distribuit ("ledger")
- LE - "low energy"
- TOA - timpul de sosire
- TDOA - diferenţa timpului de sosire
- RSS - puterea semnalului primit

În urma dezvoltării platformei Politrip [1] ce permite organizarea de experienţe cu tematici specifice pentru turişti şi a contribuţiilor aduse în platforma Privatesky[2], proiect de dezvoltare cercetare prin colaborare ce oferă soluţii cu caracteristici avansate de protecţie a datelor, propunem o invenţie ce se referă la un dispozitiv portabil care este folosit de membrii unui grup de turişti pentru localizare şi comunicare fără a folosi un furnizor GSM, cu accent pe protecţia datelor cu caracter privat.

Majoritatea soluţiile existente tratează problema localizării din punct de vederea al confidenţialităţii, prin folosirea unui server central de localizare (LBS)[3] unde se pot configura diverse reguli ce pot asigura un nivel de protecţie, prin anonimizarea datelor (locaţie şi timpul înregistrării) sau prin creşterea nesiguranţei adversarului de a afla poziţia curentă a utilizatorului. Însă aceasta abordare are diferite dezavantaje, cum ar fi: dependenţa ridicată de un nod central sau furnizor, un singur punct al eşecului, iar controlul nu este la dispoziţia utilizatorului.

Scopul invenţiei este de a elimina nodul central (LBS), de a creşte gradul de protectie a datelor personale (locaţie şi alte date cu caracter personal) şi de a oferi controlul absolut asupra nivelului de confidenţialitate al informaţiilor utilizatorului final, prin intermediul dispozitivului hardware, date distribuite într-un mod criptat.

Problema pe care o rezolvă invenţia este reprezentată de abordarea descentralizată prin care informaţia e distribuită între noduri într-un mod criptat, controlul nivelului de confidentialitate al informaţiilor fiind la dispoziţia utilizatorului prin intermediul dispozitivului hardware.

Fiecare dispozitiv are asociat un identificator **DID**[4] ce permite identificarea digitală într-un sistem descentralizat, fiind un identificator unic global, ce identifica un **document DID**[5] ce contine un set de

[1] https://politrip.com/
[2] https://github.com/PrivateSky/privatesky
[3] Wang, Peng & Yang, Jing & Zhang, Jian-Pei. (2016). Protection of Location Privacy Based on Distributed Collaborative Recommendations. PLOS ONE. 11. 10.1371/journal.pone.0163053.
[4] https://www.w3.org/TR/did-core/
[5] https://www.w3.org/TR/did-core/#dfn-did-documents

Companie
Heaven Solutions 2005 SRL

SOCIETATEA COMERCIALA CUI 18756121 HEAVEN SOLUTIONS 2005 SRL J22/2872/2005 IASI ROMANIA

Rector,
Prof. Dr. Tudorel Toader

date care descrie subiectul (dispozitivul harware), o cheie publica criptografică ce este folosită pentru autentificare şi a demonstra asocierea cu identificatorul DID, date propriu-zise ce trebuie protejate, un **controler DID** ce are capabilităţi de a face acţiuni asupra **documentului DID** prin intermediul unor **metode DID** ale căror specificatii definesc operaţiile care pot fi folosite asupra documentului cum ar fi: creare, citire, modificare sau dezactivare de către un alt nod din reţea sau propriul nod. Deţinătorul unui document DID poate dovedi proprietatea acestuia folosind cheia privată asociată. Acesta fiind un concept puternic, eliminand serviciile centralizate pentru a dovedi proprietatea asupra unui document DID. Mai mult de atat, tranzacţiile asupra unui document DID pot fi verificate în **registru de date distribuit DLT** ("ledger"), la care are acces orice nod din reţea asigurându-se astfel transparenţă, rezistenţă la manipularea datelor şi o arhitectura rezistentă la erori.

Din punct de vedere al infrastructurii, sistemul este reprezentat de o reţea de tip mesh alcătuită din 3 tipuri de noduri: **master** (M) cu rol de coordonator şi centru de încredere, un nod **router secundar** (SR) cu rol de propagare a mesajelor dintr-o sub reţea şi cu rol de extinderea ei şi un nod **terminal** (T) care comunică cu restul nodurilor prin Bluetooth 5.0 Low Energy (LE) şi tehnici de triangulare, folosind documente DID.
Pentru determinarea locaţiei unui punct există tehnici bazate pe distanţă cum ar fi: timpul de sosire (TOA), diferenţa timpului de sosire (TDOA) sau puterea semnalului primit (RSS), sau tehnici bazate pe direcţie cum ar fi unghiul de sosire (AOA). Pentru soluţia propusă, folosim **distanţa Euclidiană** a puterii semnalului primit (**RSS**)[6].
Comunicarea se realizeaza prin intermediul documentelor DID şi ale **serviciilor DID**[7] ce expun operaţii pentru determinarea locaţiei unui nod din reţea şi propagarea informaţiilor în reţeaua mesh, într-un mod criptat.
Avantajele pe care le aduce invenţia sunt reprezentate prin modul de comunicare distribuit şi criptat cu accent pe protecţia datelor cu caracter privat, utilizatorii finali avand posibilitatea de a şterge informaţiile cu caracter privat cum ar fi date personale sau date colectate în urma localizării.

Un exemplu de configurare al nivelului de confidenţialitate al informaţiilor de către utilizator realizate prin intermediul butoanelor programabile este:

- butonul **B1** - permite citirea numelui şi a locaţiei de către organizator
- butonul **B2** - permite citirea doar a locaţiei de către organizator
- butonul **B3** - permite ştergerea tuturor informaţiilor despre utilizator de pe toată durata folosirii dispozitivului din întreaga reţea

Din punct de vedere al aplicabilităţii, acest dispozitiv este folosit de grupurile de turişti care participă la experienţe şi excursii tematice realizate prin intermediul platformei Politrip. Grupul de turişti este format din un organizator şi *N* participanţi care pot folosi dispozitivul astfel: localizarea ghidului în cazul în care unul dintre turişti s-a îndepărtat faţă de grup, trimiterea unui mesaj text către organizator sau stabilirea unui punct de intalnire, într-un spaţiu deschis pe distanţe mari, unde nu există conexiune GSM. Totodată, controlul nivelului de confidentialitate a mesajelor transmise între noduri fiind la dispoziţia turistului, putând opta atat pentru o partajare parţială sau totală a unor date (locaţie, mesaje text), cat si pentru ştergerea definitivă a lor.

[6] B. Wang et al., "A Novel Weighted KNN Algorithm Based on RSS Similarity and Position Distance for Wi-Fi Fingerprint Positioning," in IEEE Access, vol. 8, pp. 30591-30602, 2020, doi: 10.1109/ACCESS.2020.2973212.
[7] https://www.w3.org/TR/did-core/#dfn-service

Companie
Heaven Solutions 2005 SRL

Rector,
Prof. Dr. Tudorel Toader

13

## REVENDICĂRI

1. Un sistem descentralizat pentru localizare pe distanţe mari, a unui grup de turişti cu accent pe protecţia datelor cu caracter privat caracterizat prin aceea că folosind documente DID (W3C) şi un registru de date distribuit DLT ("ledger") se asigură transparenţa şi rezistenţa la manipularea datelor.
2. Configurarea nivelului de confidentialitate a informaţiilor folosind butoane presetate pe un dispozitiv hardware caracterizat prin aceea că partajarea şi controlul nivelului de confidenţialitate a informaţiilor se află la dispoziţia utilizatorului final prin intermediul dispozitivului portabil.

Companie
Heaven Solutions 2005 SRL

Rector,
Prof. Dr. Tudorel Toader

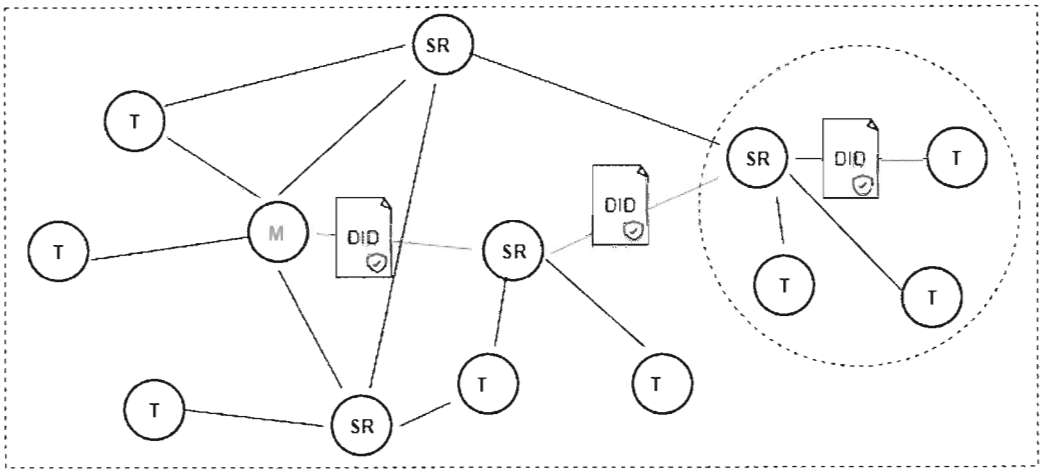


Fig. 1. Rețea mesh comunicând prin documente DID și Bluetooth 5.0 Low Energy

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:politrip:123456789abcdefghi",
  "authentication": [{
    "id": "did:politrip:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2021",
    "controller": "did:politrip:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    "id":"did:politrip:123456789abcdefghi#vcs",
    "type": "LocalizationService",
    "serviceEndpoint": "https://politrip-devices.local/vcs/"
  }]
}
```

Fig. 2. Exemplu document DID cu serviciu pentru localizare

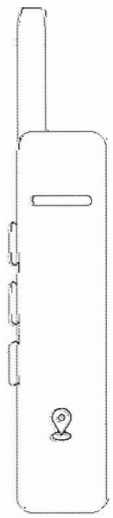

Fig. 3. Dispozitiv rețea mesh cu antena Bluetooth 5.0 LE și butoane pentru setarea nivelului de confidențialitate a informațiilor

Companie
Heaven Solutions 2005 SRL

Rector,
Prof. Dr. Tudorel Toader

## REVENDICĂRI

1. Un sistem hardware şi software pentru localizare pe distanţe mari, a unui grup de turişti, **caracterizat prin aceea ca**
   a. oferă un nivel superior de protecţie a datelor cu caracter privat şi folosirea noilor standarde W3C a identităţilor *self sovereign* (DIDs) şi prin folosirea unui registru de date distribuite DLT ("ledger") ce asigură transparenţa şi rezistenţa la manipularea datelor.
   b. uşurinţa de utilizare prin proiectarea unor butoane presetate pe un dispozitiv hardware ce permite partajarea şi controlul nivelului de confidenţialitate a informaţiilor.

Companie
Heaven Solutions 2005 SRL

Rector,
Prof. Dr. Tudorel Toader