Proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013
Investește în oameni!

Proiect EXCELDOC - POSDRU/159/1.5/S/132397
Excelență în cercetare prin burse doctorale și postdoctorale

UNIVERSITATEA **POLITEHNICA** DIN BUCUREŞTI
Facultatea Automatică și Calculatoare
Departamentul de Automatică și Informatică Industrială

Nr. Decizie Senat _____din _____

TEZĂ DE DOCTORAT

Contribuții la securizarea rețelelor de senzori wireless

Contributions for the security of wireless sensor networks

Autor: Ing. Ionela HALCU
Conducător de doctorat: Prof. dr. ing. Valentin SGÂRCIU

COMISIA DE DOCTORAT

Președinte	Prof. dr. ing. Dan POPESCU	de la	Universitatea Politehnica București
Conducător de doctorat	Prof. dr. ing. Valentin SGÂRCIU	de la	Universitatea Politehnica București
Referent	Prof. dr. ing. Nicolae PARASCHIV	de la	Universitatea Petrol și Gaze Ploiești
Referent	Prof. dr. ing. Sergiu CARAMAN	de la	Universitatea Dunărea de Jos Galați
Referent	Prof. dr. ing. Dorin CÂRSTOIU	de la	Universitatea Politehnica București

București

Cuprins

Pag.

Mulțumiri

Cele mai alese gânduri de recunoștință și mulțumire conducătorului științific, domnul profesor dr. ing. Valentin Sgârciu, care m-a sprijinit constant în activitatea mea doctorală și a dat dovadă de multă răbdare în îndrumarea competentă și permanentă pe parcursul elaborării acestei lucrări.

Mulțumesc domnului ș.l. dr. ing. Grigore Stamatescu care, cu generozitate, răbdare și profesionalism, a contribuit la conținutul ideatic și științific al cercetărilor mele, precum și pentru sprijinul continuu, atât profesional, cât și personal.

De asemenea, doresc să mulțumesc tuturor colegilor din cadrul departamentului de Automatică și Informatică Industrială pentru sprijinul permanent acordat și colaborarea în decursul celor 3 ani, concretizată printr-o listă de realizări comune.

Rezultatele prezentate în această lucrare au fost obținute cu sprijinul Ministerului Fondurilor Europene prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013, Contract nr. POSDRU/159/1.5/S/132397.

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/159/1.5/S/132397.

INTRODUCERE

1. OBIECTIVELE LUCRĂRII

Zi de zi se dezvoltă numeroase aplicații care au la bază rețelele de senzori wireless (WSN). Acum și în viitorul apropriat rețelele WSN vor ocupa un rol din ce în ce mai important în viața noastră de zi cu zi. Rețelele WSN deja constituie un element esențial în industrie, agricultură, medicină, aplicații casnice și militare. Afirmațiile de mai sus se bazează pe faptul ca în momentul de față există o implicare intensă în cercetarea rețelelor de senzori, care aduc imense beneficii și totodată provocări.

Tot mai multe aplicații WSN de detecție, monitorizare și control devin conectate la Internet, iar aceste comunicări trebuie să fie fiabile și sigure. Odată cu creșterea utilizării la scară globală a comunicațiilor IPv6, nodurile rețelei evoluează pentru a deveni compatibile cu IPv6, iar noi aplicații sunt proiectate sau adaptate să depindă de conectivitatea IPv6 cu nodurile senzoriale. În aceste condiții, securitatea joacă un rol vital în integrarea rețelelor WSN cu Internetul, ceea ce constituie o contribuție majoră în evoluția Internet of Things.

În cadrul tezei, sunt studiate problematici importante ale rețelelor WSN, cum sunt: securitatea și comunicațiile wireless dintre nodurile rețelei bazate pe tehnologii IPv6, menținând compromisuri ca eficiența energetică, fiabilitatea și disponibilitatea rețelei.

Principalele obiective propuse în lucrarea de față sunt următoarele:

- ✓ Analiza stadiului actual în domeniul rețelelor de senzori wireless. Se realizează studiul arhitecturilor, standardelor, și tehnologiilor specifice rețelelor de senzori, precum și integrarea acestora în diferite aplicații.
- ✓ Identificarea și analiza problematicilor vizând securitatea rețelelor WSN implementate în diverse aplicații. Identificarea cerințelor unei rețele de senzori wireless sigure. Analiza stadiului actual asupra tipurilor de amenințări existente în contextul unei rețele tipice de senzori wireless, și asupra celor mai recente tehnici de prevenire și combatere a acestora.
- ✓ Implementarea și validarea prin simulări a unor de mecanisme de securitate a rețelelor de senzori prin utilizarea unor tehnici de securizare actuale, menținând cerințele de securitate necesare și luând în considerare limitările rețelelor WSN.
- ✓ Implementarea unor mecanisme de securitate pentru diverse topologii de rețele WSN bazate pe comunicații IPv6, utilizând sistemul de operare Contiki. În plus față de adăugarea unui nou protocol suitei de protocoale suportate de Contiki, acest proiect își propune atât evaluarea cât și adaptarea mecanismelor de securitate la cerințele sporite ale diferitelor aplicații cu rețele WSN. De asemenea, aceste mecanisme trebuie să asigure transportul sigur al datelor atât în interiorul rețelelor, cât și în afara acestora, în cazul în care datele sunt accesate prin Internet.
- ✓ Modelarea și analizarea performanțelor rețelelor de senzori wireless industriale (IWSN) utilizând comunicații IPv6. Analiza problematicilor vizând securitatea rețelelor de senzori wireless industriale și implementarea unei metode de securitate propuse, adaptabilă acestor tipuri de rețele.
- ✓ Integrarea în siguranță a aplicațiilor cu rețele WSN bazate pe IPv6 în Internet, contribuind astfel la evoluția și securitatea aplicațiilor Internet-of-Things.

2. PREZENTAREA CONȚINUTULUI LUCRĂRII

Conținutul lucrării este dezvoltat pe parcursul a cinci capitole după cum urmează:

În primul capitol sunt prezentate succint evoluția și stadiului actual al rețelelor WSN. Se prezintă, pe lângă noțiuni preliminare și aspecte privind caracteristicile și provocările WSNs, standarde, sisteme de operare, aplicații și platforme de dezvoltare dedicate rețelelor de WSN.

În **Capitolul 2** se discută principalele aspecte referitoare la securitatea rețelelor WSN. În prima parte sunt identificate problematicile importante ale WSNs în vederea dezvoltării de noi metode de securitate. Apoi se prezintă cerințele de securitate necesare protejării unei WSN împotriva principalelor tipuri de atacuri dedicate, urmând o analiză a stadiului actual asupra mecanismelor de securitate existente, din orice punct de vedere al rețelei (de ex., asupra protocoalelor de rutare, detecția intruziunilor, mecanisme de protejare fizică etc.).

În **Capitolul 3** sunt prezentate mecanismele existente pentru asigurarea securității într-un WSN bazat pe comunicații IPv6. Sunt prezentate specificațiile IPv6 peste tehnologiile de senzori wireless, împreună cu principalele mecanisme de securitate implementate pentru diferite nivele din stiva 6LoWPAN, care permit protecția comunicațiilor IPv6 peste rețele WSN IEEE802.15.4. Tot aici sunt prezentate și două studii de caz pentru evaluarea unor mecanisme de securitate, în contextul unor rețele WSN bazate pe 6LoWPAN, cu ajutorul mediului de dezvoltare Contiki/Cooja. Se oferă o analiză experimentală pentru o abordare combinată de securitate și de comunicare într-un design de sistem WSN 6LoWPAN.

În **Capitolul 4** se dezvoltă un model de securitate pentru rețele de senzori wireless industriale (IWSN). În prima parte se face o analiză a stadiului actual în ceea ce privește utilizarea rețelelor 6LoWPAN ce rulează Contiki în aplicații din domeniul industrial. Se identifică proprietățile și provocările tehnice pentru realizarea de aplicații IWSN. Aplicabilitatea în domeniul industrial este bazată pe un număr de provocări de securitate asociate cu acest tip de aplicații. Se prezintă un studiu de caz cu propunerea unei arhitecturi de securitate studiate și analiza performanțelor, într-un context IWSN.

Capitolul 5 prezintă un studiu de caz asupra integrării WSN în IoT și CPS. Se studiază principalele mecanisme de asigurare a confidențialității în contextul accesării rețelei WSN din Internet. Se pune accentul pe confidențialitatea datelor și a utilizatorilor într-un context Human-in-the-Loop Cyber-Physical System (HiTLCPS), o paradigmă în care utilizatorul este parte integrantă din bucla de control, iar acțiunile sale afectează ieșirile sistemului. În ultima parte se dezvoltă o arhitectură de asigurare a confidențialității utilizatorilor unui astfel de sistem.

În finalul lucrării sunt prezentate concluziile, contribuțiile personale și posibile direcții de cercetare în opinia autorului.

CAPITOLUL 1
REȚELE DE SENZORI WIRELESS

1.1. CARACTERISTICI ALE REȚELELOR DE SENZORI WIRELESS

Rețelele de senzori wireless reprezintă un grup de dispozitive inteligente autonome, distribuite spațial, care cooperează pentru monitorizarea unor parametri fizici ai mediului în care sunt amplasate. [1]

Elementele rețelei de senzori vor fi referite în cadrul lucrării prin termenii *senzor* sau *nod*. Nodurile sunt de regulă dispozitive compacte, de mici dimensiuni, ușoare, necesită puțină energie pentru a opera, și pot fi amplasate în zona de monitorizat, având o funcționare de lungă durată și un grad de fiabilitate ridicat.

În comparație cu rețelele tradiționale, câteva caracteristici și considerații ale rețelelor de senzori wireless sunt discutate și abordate în proiectarea WSN-urilor: acestea dispun de o arhitectură non-centralizată, au capacitatea de a se auto-organiza, sunt capabile de transmiterea datelor în modul multi-hop, iar majoritatea arhitecturilor de rețele de senzori au o topologie dinamică. Acestor caracteristici li se alătură o serie de constrângeri si provocări care pot apărea la proiectarea aplicațiilor.

1.2. PROVOCĂRI ALE REȚELELOR DE SENZORI WIRELESS

Provocările rețelelor de senzori apar la proiectarea hardware, protocoalele de comunicații și proiectarea aplicațiilor. Mărirea duratei de funcționare a unei rețele de senzori și construirea unui sistem inteligent de colectare a datelor sunt două provocări importante ale rețelelor de senzori. Alte provocări sunt:

- Topologia rețelelor de senzori se schimbă foarte repede;
- Senzorii folosesc un model de comunicație broadcast în timp ce majoritatea rețelelor sunt bazate pe comunicații “punct la punct”;
- Senzorii sunt limitați în ceea ce privește energia, capacitățile de calcul și memoria;
- Senzorii sunt predispuși la eșecuri;
- Senzorii sunt dispuși compact în număr mare. Problema poate apărea în termeni de coliziuni și congestie. Pentru a evita coliziunile, senzorii care sunt în aria de emisie a altor senzori nu trebuie să emită în același timp;
- Amplasarea ad-hoc necesită ca sistemul să identifice și să facă față la consecințele distribuirii și legăturilor dintre nodurile rețelei;
- Mediul dinamic în care funcționează senzorii impune rețelei să se adapteze în timp la modificările legăturilor dintre noduri și la diverși stimuli exteriori rețelei.

Una din provocările majore ale WSN impune cerințe de securitate sporită cu resurse limitate. Cerințele de securitate cuprind autentificarea nodurilor, confidențialitatea datelor, non-repudierea și rezistența împotriva analizei traficului. Totuși, WSNs sunt compromise de atacatori atât datorită comunicației de tip wireless, deoarece folosesc un mediu de transmisie broadcast, cât și datorită lipsei de rezistență la manipulare. Așadar, un atacator poate asculta traficul din rețea, insera pachete rău intenționate, reutiliza pachete mai vechi sau chiar compromite un nod.

1.3. APLICAȚII ALE REȚELELOR DE SENZORI WIRELESS

Cele mai frecvent utilizate aplicații ale rețelelor de senzori wireless se pot clasifica în trei domenii majore, după cum urmează:

Fig. 1.1 Cele mai frecvent utilizate aplicații ale WSN, clasificate în domenii majore

Reacția la dezastre reprezintă una din cele mai frecvent utilizate aplicații ale rețelelor wireless de senzori. Un scenariu tipic este detecția incendiilor din medii extraurbane, nodurile echipate cu senzori optici de fum și de temperatură, uneori cu tehnologii de localizare, sunt răspândite în mediul respectiv. Din datele centralizate se formează o hartă termică a regiunii, pe care se pot determina zonele de temperatură ridicată accesibile terestru [2]. Scenarii similare se pot imagina și pentru monitorizarea accidentelor chimice. Rețelele de senzori wireless pot fi utilizate și în **controlul calității mediului**, monitorizând emanațiile de gaze, substanțe chimice periculoase, rampe de gunoi, sau monitorizarea platoului marin printr-o mai bună înțelegere a fenomenelor de eroziune ale acestuia.

În domeniul **controlului ecologic** aceste rețele de senzori se pot utiliza pentru evaluarea numărului de specii de plante și animale dintr-un habitat, acest lucru implicând o mapare a biodiversității. Principalele avantaje ale utilizării rețelelor WSN în astfel de aplicații sunt legate de funcționarea pe o durată cât mai lungă a senzorilor în maximă proximitate cu punctele de interes. Nodurile senzoriale pot fi utilizate în **monitorizarea stresului mecanic** la care sunt supuse clădirile în zonele active seismic. Prin măsurarea parametrilor mecanici, cum ar fi încărcarea la încovoiere a grinzilor, este posibil să se stabilească pe baza informațiilor provenite de la rețelele de senzori, dacă o clădire mai constituie un obiectiv sigur după un cutremur sau dacă este în pragul colapsului, în rețea putând participa și tipuri de senzori dedicați detecției formelor de viață prinse în clădirile prăbușite. În funcție de tipul de aplicație, nodurile senzoriale pot fi instalate în clădiri deja construite, sau încorporați în clădiri aflate în construcție.

CAPITOLUL 2
SECURITATEA REȚELELOR DE SENZORI WIRELESS

2.1. PROBLEMATICA SECURITĂȚII ÎN WSN

O rețea de senzori wireless este o rețea specială ce deține multe constrângeri în comparație cu o rețea de calculatoare tradițională. Datorită acestor constrângeri este dificil a se folosi abordările de securitate existente în aria rețelelor de senzori wireless. Așadar, pentru a dezvolta mecanisme utile împrumutând ideile de la tehnicile de securitate existente, este necesar a se ști și înțelege aceste constrângeri mai întâi.

- **Resurse limitate.** Toate abordările de securitate necesită într-o anumită măsură resurse pentru implementare, incluzând memorie, spațiu de stocare și energie pentru ca senzorul să funcționeze. În prezent, aceste resurse sunt foarte limitate în rețelele mici de senzori.
- **Mediu de comunicare nesigur.** Cu certitudine, mediul de comunicare este o altă amenințare a securității unui senzor. Securitatea rețelei constă în mare parte dintr-un protocol, care la rândul său depinde de mediul de comunicare.
- **Operare nesupravegheată.** În funcție de scopul unei rețele de senzori, nodurile sale pot fi lăsate nesupravegheate pentru perioade îndelungate. Există trei riscuri la care se expun nodurile nesupravegheate: expunerea la atacuri fizice, gestionarea de la distanță și lipsa unui punct central de administrare. Poate cel mai important aspect de care trebuie ținut cont este faptul că lăsarea nesupravegheată a unui senzor o perioadă îndelungată mărește gradul de risc ca un nod să fie compromis.

În completarea acestor probleme de securitate, se observă că multe tehnici de securizare a rețelelor de senzori de uz general își asumă că toate nodurile sunt cooperante și sigure. Acesta nu este cazul pentru multe din ele, sau mai mult, aplicațiile de rețele WSN reale au nevoie de un anumit grad de încredere în măsură să mențină o funcționalitate corectă. În plus, există numeroase atacuri proiectate să exploateze canalele de comunicație nesigure și operațiunile nesupravegheate ale rețelelor de senzori wireless.

Se pot clasifica principalele aspecte ale securității WSN în patru mari categorii: (1) Obstacolele securității în WSN; (2) Cerințele unei rețele de senzori wireless sigure; (3) Atacuri; (4) Măsuri de protecție.

2.2. CERINȚE DE SECURITATE SPECIFICE REȚELELOR DE SENZORI

O rețea de senzori este un tip special de rețea. Împarte câteva atribute comune cu o rețea tipică de calculatoare, dar de asemenea ridică și câteva cerințe proprii, așa cum a fost explicat în Capitolul 1. Așadar, ne putem gândi la cerințele globale ale unei rețele WSN ce cuprinde atât cerințele unei rețele tipice, cât și cerințele unice convenite doar de rețelele de senzori wireless.

Obiectivele privind securitatea WSN sunt clasificate în obiective *primare* și *secundare*. Obiectivele principale, cunoscute ca obiective de securitate standard, sunt *confidențialitatea, integritatea, autentificarea* și *disponibilitatea.* Obiectivele secundare se referă la actualitatea datelor (*data freshness*), auto-organizarea (*self-organization*), sincronizarea (*time synchronization*) și localizarea sigură (*secure localization*).

2.3. TIPURI DE ATACURI ASUPRA SECURITĂȚII ÎN WSN

Rețelele de senzori sunt vulnerabile în particular la câteva tipuri de atacuri. Aceste atacuri pot fi efectuate în diferite moduri, cele mai frecvente sunt atacurile de tip Denial of Service (DoS), dar și prin analiza traficului, încălcare a confidențialității, atacuri fizice, și altele. Atacurile de tip DoS în rețelele de senzori wireless pot varia de la blocarea mediului de comunicare al senzorilor până la atacuri mai sofisticate proiectate să încalce protocolul 802.15.4 MAC sau alte nivele ale rețelei de senzori wireless [1].

Datorită potențialei asimetrii în ceea ce privește puterea de alimentare și constrângerile operaționale, protejarea împotriva unui atac DoS bine planificat poate fi chiar și imposibilă. Un nod mai puternic poate bruia cu ușurință un nod-senzor, în consecință poate preveni rețeaua să-și îndeplinească sarcinile alocate [3].

Se observă că atacurile asupra rețelelor de senzori wireless nu sunt limitate la atacuri de tip DoS, ci mai degrabă înglobează o serie de tehnici inclusiv compromiterea nodurilor, atacuri asupra protocoalelor de rutare și de analiză a traficului, atacuri adresate confidențialității și atacuri fizice [4].

Atacurile asupra securității în rețelele WSN pot fi clasificate în două clase principale: atacuri *active* si *pasive*. Atacurile pasive, în care adversarii nu aduc modificări, sunt în principal împotriva confidențialității datelor. În cazul atacurilor active, actele malițioase nu se desfășoară doar asupra confidențialității datelor ci și asupra integrității lor. Atacurile active țintesc de asemenea către accesul neautorizat și utilizarea resurselor sau întreruperea comunicațiilor între noduri. Un atacator activ formează o emisie sau acțiune care poate fi detectată.

Spre deosebire de atacurile de securitate, inutilitatea este de asemenea un factor important. Din greșeală, utilizatorii pot expune noduri la atacuri ca manipularea și distrugerea acestora, iar datele și resursele la accesul neautorizat. Schemele de securitate si toleranță la defecte ar trebui să abordeze atât securitatea cât și siguranța provocărilor create de utilizarea neglijentă sau evenimentele neprevăzute [5].

Atacurile care acționează la nivelul rețelei se numesc *atacuri de rutare*. Următoarele atacuri se întâmplă în timp ce pachetele sunt transmise:

- Informații falsificate, alterate sau retransmise - fiecare nod se poate comporta ca un router și poate afecta în mod direct informațiile de rutare: creează bucle de rutare, extind sau scurtează rutele de servicii, generează mesaje de eroare false, mărește latența end-to-end.
- Redirecționare selectivă - un nod malițios aruncă doar anumite pachete.
- Sinkhole (atac de tip ”scurgere”) - nodul malițios atrage tot traficul din rețea.
- Wormhole (atac de tip ”gaură de vierme”) - atacatorul înregistrează pachetele dintr-o locație și apoi le retransmite într-o altă locație din rețea.

Atacurile de tip DoS apar atunci când un nod malițios încearcă să întrerupă funcționalitatea normală a rețelei sau când un eveniment influențează un serviciu să ruleze anormal. Mecanismele pentru prevenirea atacurilor DoS includ autentificare solidă și identificarea traficului [6].

Compromiterea unui nod are loc atunci când un nod este capturat pentru informațiile stocate în acesta. Când un nod funcționează incorect, integritatea datelor poate fi afectată. În alte cazuri, informația transmisă de către acel nod poate fi redirecționată către alte noduri și funcționalitatea întregii rețele poate fi compromisă. Întreruperea unui nod apare în situația în care un nod nu mai funcționează. În cazul în care conducătorul unui cluster nu mai funcționează, protocoalele rețelei de senzori ar trebui să rezolve efectele întreruperii nodului prin rutarea pachetelor către alte noduri, fără să afecteze funcționalitatea rețelei.

WSN operează de regulă în medii externe ostile. În aceste medii, un nod poate fi înlocuit cu un altul pentru a obține informații cruciale din rețea, sau pentru a retransmite informații false pentru întreruperea funcționalității rețelei. Un atacator care cunoaște câte ceva despre rețea poate intercepta cu ușurință datele transmise dacă pachetele nu sunt criptate.

Atacurile împotriva rețelelor de senzori wireless ar putea fi larg considerate din două puncte de vedere. Unul este atacul împotriva mecanismelor de securitate și celălalt împotriva mecanismelor de bază (ca de ex. mecanismele de rutare).

2.4. TEHNICI DE SECURIZARE A REȚELELOR DE SENZORI WIRELESS

S-au realizat multe cercetări referitoare la securizarea datelor, echipamentelor și a aplicațiilor WSN [3], [5], [7], [8]. În continuare, se clasifică schemele pentru rețelele de senzori wireless în diferite tipuri, bazate pe scenariile de utilizare, incluzând: implementarea, organizarea, realocarea cheilor, criptografia și autentificarea.

Tabelul 2.1 Clasificarea schemelor de comunicații sigure

Clasificare	**Caracteristici**
Instalare	Instalare dispersată Zone desemnate
Organizare	WSNs distribuite WSNs ierarhice
Realocarea cheilor	Actualizare periodică Revocarea/atașarea nodului
Criptografie	Chei simetrice Chei asimetrice Funcții hash
Autentificare	Autentificarea perechilor Autentificarea grupurilor

Printre tehnicile de securizare specifice rețelelor de senzori wireless, întâlnim:

- Mecanisme de management și distribuție a cheilor;
- Tehnici criptografice;
- Metode de protejare împotriva atacurilor de tip DoS;
- Securizarea comunicațiilor tip *broadcast* și *multicast*;
- Protejarea împotriva atacurilor la nivelul protocoalelor de rutare;
- Detectarea atacurilor de replicare a nodurilor;
- Combaterea atacurilor de analiză a traficului;
- Protejarea împotriva atacurilor adresate confidențialității/ intimității;
- Detectarea intruziunilor în rețelele de senzori wireless;
- Securizarea agregării datelor;
- Protejarea împotriva atacurilor fizice.

CAPITOLUL 3
MECANISME DE SECURITATE PENTRU REȚELE DE SENZORI WIRELESS BAZATE PE IPV6

3.1. PRELIMINARII

Utilizarea IPv6 în rețelele de senzori wireless permite integrarea aplicațiilor senzoriale, existente sau noi, în Internet. Acest lucru ridică o serie de probleme de securitate suplimentare față de cele existente, prezentate în capitolul anterior. Așadar, sunt necesare noi modele și mecanisme de securitate pentru a sprijini integrarea în siguranță a rețelelor WSN în Internet. Un astfel de model ar trebui să permită securitate end-to-end și să fie în măsură să ofere mecanisme care permit adaptarea flexibilă a securității la limitările nodurilor senzoriale. Acest capitol prezintă și discută o varietate de astfel de protocoale și mecanisme existente, într-o abordare 6LoWPAN arhitecturală. O imagine sugestivă ce reprezintă modul de interconectare și integrare al rețelelor WSN în Internet este prezentată în Fig. 3.1.

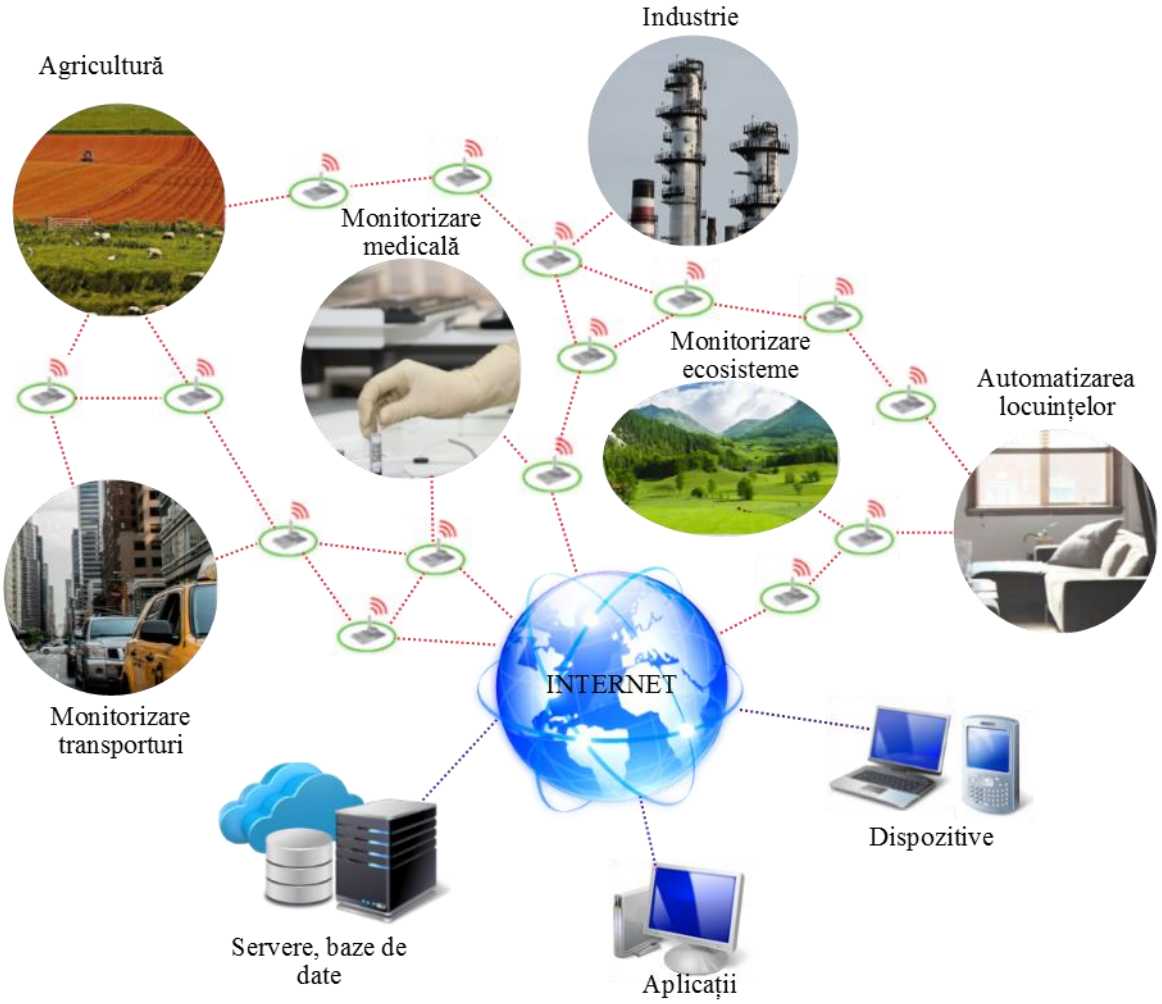

Fig. 3.1 Interconectarea rețelelor de senzori wireless și integrarea acestora în Internet

3.2. 6LOWPAN – IPV6 PENTRU REȚELE WIRELESS DE JOASĂ-PUTERE

6LoWPAN este un acronim pentru *IPv6 over Low power Wireless Personal Area Network* [9]. Acesta este un standard dezvoltat de IETF ce permite utilizarea protocolului IPv6 în WSNs. Nivelul de adaptare 6LoWPAN este situat între nivelul legăturii de date MAC și nivelul rețea, pentru a permite transportul datelor de la nivelele de comunicație de joasă putere la nivelele superioare (Fig. 3.2). Acesta optimizează utilizarea spațiului limitat al sarcinii utile prin compresia antetului pachetelor, în același timp definind mecanisme pentru suportul operațiilor specifice IPv6, în particular descoperirea vecinilor și auto-configurarea adreselor. Inițial, nivelul de adaptare a fost definit în [9], suferind modificări în diferite documente RFC de-a lungul timpului [10]–[13].

Această nouă tehnologie combină diferite rețele eterogene de joasă putere și permite dispozitivelor integrate să comunice cu dispozitivele conectate la Internet. 6LoWPAN a câștigat rapid popularitate prin aplicabilitatea sa largă, plecând de la îngrijiri medicale la monitorizare ambientală.

6LoWPAN permite utilizarea arhitecturilor orientate pe servicii (SOAs – Service Oriented Architectures) în WSN. IETF a definit protocolul CoAP (Constrained Application Protocol) [14], un protocol de transfer pe web ce oferă câteva din funcționalitățile HTTP (Hypertext Transfer Protocol), dar redefinit pentru dispozitivele integrate constrânse. CoAP permite aplicațiilor WSN să fie construite peste arhitecturile REST (Representational State Transfer).

6LoWPAN oferă mecanisme de încapsulare și compresie a headerului ce permit pachetelor IPv6 sa fie transmise și recepționate peste rețelele bazate pe IEEE802.15.4. Nu există mecanisme de securitate definite în prezent în contextul stratului de adaptare 6LoWPAN, dar documentele relevante includ discuții cu privire la vulnerabilități de securitate, cerințe și abordări de considerat pentru utilizarea securității la nivelul rețea [15].

În prezent există diferite implementări ale acestui standard în practică, așadar este interesant a se evalua performanțele acestora în ceea ce privește memoria și păstrarea limitelor impuse. Printre implementările cele mai utilizate în prezent există µIPv6/Contiki [16], SICSlowpan, 6lowpancli, B6LoWPAN, BLIP, NanoStack etc.

Așa cum este prezentat în Fig. 3.2, la Nivelul 1 și 2, protocolul IEEE802.15.4 Media Access Control (MAC) și nivelul fizic (PHY) transmit cadre către vecinii aflați la un hop distanță. La Nivelul 2.5, nivelul adaptat 6LoWPAN fragmentează și face compresie pachetelor IPv6. Fragmentarea este necesară deoarece IEEE802.15.4 are un MTU de 127 bytes. Compresia, pe de altă parte, reduce consumul de energie necesar transmiterii și recepției pachetelor IPv6. La Nivel 3, 6LoWPAN Neighbor Discovery (6LoWPAN-ND)[13] diseminează conținutul informațiilor pentru compresia prefixelor de rețea IPv6 arbitrare. De asemenea la Nivelul 3, protocolul de rutare IPv6 pentru rețele de joasă putere și pierderi (RPL) [17] rutează pachetele IPv6. La Nivelul 7, sunt implementate protocoale bazate pe UDP, cum ar fi CoAP [14].

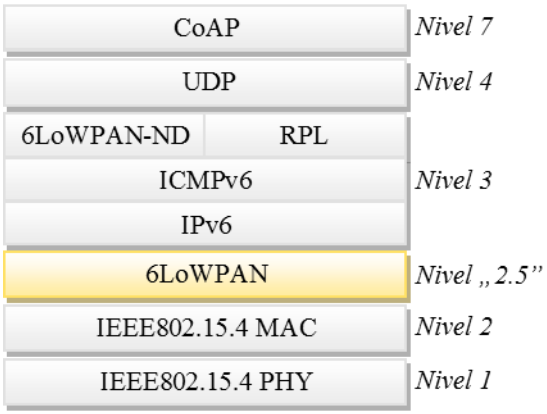

Fig. 3.2 Stiva 6LoWPAN

Datorită utilizării mediului wireless, atacatorii pot injecta și retrimite cadre-uri IEEE802.15.4. Dacă un filtru aplicat la nivelul legăturii de date IEEE802.15.4 nu există, atunci aceste atacuri pot avea consecințe severe. Pe nivelul 2.5, atacatorii pot lansa atacuri de fragmentare, care distrug pachetele reasamblate sau epuizează buferele [18]. La Nivelul 3, un atacator ar putea lansa atacuri tip path-DoS (PDoS). Într-un atac de tip PDoS, un atacator injectează pachete IPv6 false, care sunt apoi rutate prin rețeaua 6LoWPAN, epuizând astfel bateria. Un alt atac la Nivelul 3 este de a injecta mesaje Internet Control Message Protocol for IPv6 (ICMPv6) pentru a bloca protocoalele RPL sau 6LoWPAN-ND.

3.3. ANALIZA CONSTRÂNGERILOR DE COMUNICAȚII ȘI DE SECURITATE ALE REȚELELOR WSN BAZATE PE IPV6

Pentru a evalua beneficiile utilizării µIPv6 al Contiki, împreună cu o soluție de securitate pentru o rețea 6LoWPAN, s-a implementat mecanismul ContikiSec [19] într-un mediu de simulare. Modul de implementare și analizele experimentale sunt descrise în [20], [21]. Topologia de rețea utilizată pentru testare este ilustrată în figura următoare:

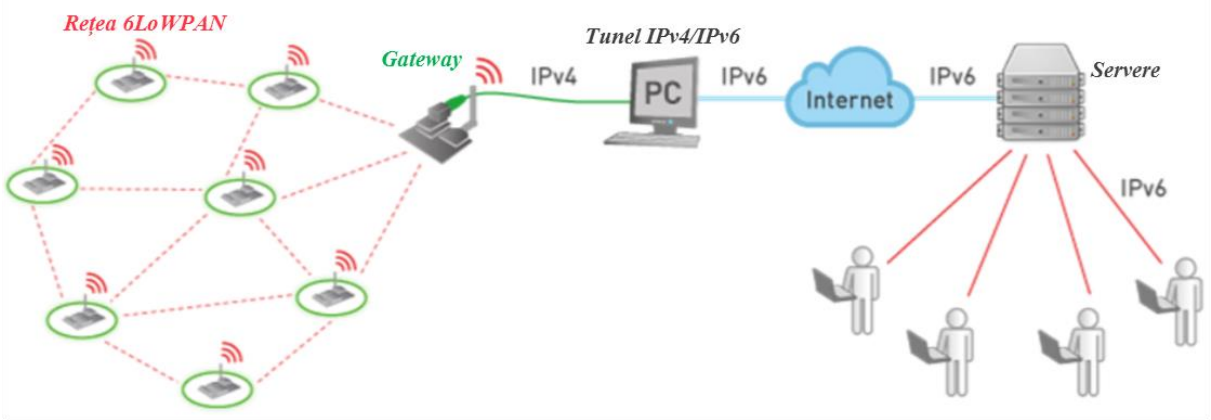

Fig. 3.3 Rețea end-to-end cu conectivitate IPv6, formată din senzori wireless distribuiți, routere IP și aplicații Internet

Acest model de referință consideră o rețea WSN, tip mesh, conectată la Internet prin intermediul unui router (border router/ gateway). Acesta preia informația primită de la nodurile senzoriale și o transmite către un server pentru colectare, utilizând interfața IPv4/IPv6 Ethernet. Uneori, gateway-ul și PC-ul de tunelare reprezintă același echipament. Astfel, utilizatorii care au acces la Internet se pot conecta la rețeaua 6LoWPAN, respectiv la datele stocate în servere dedicate.

Pentru a simula implementarea 6LoWPAN în această rețea, s-a utilizat un mediu dedicat de simulare pentru WSN numit Cooja, special creat pentru Contiki. Ca platformă hardware dedicată, s-a selectat Tmote Sky pe care rulează sistemul de operare Contiki. Tmote Sky este una dintre primele platforme ce oferă o implementare deschisă a stratului de adaptare 6LoWPAN și protocoale de nivel înalt ca RPL, CoAP etc. De asemenea, Tmote Sky oferă caracteristici de optimizare a energiei, cum ar fi auto-suspend, trezire, și modul dormire [22]. Până în momentul redactării acestei lucrări, aceasta este prima implementare a mecanismului ContikiSec pe platforma TelosB/ Tmote Sky. Mecanismul a fost inițial proiectat și testat numai pentru platforma MSB-430 [19]. De asemenea, ContikiSec nu definește nici o tehnică de distribuire a cheilor. În structura generală a stivei de protocoale Contiki cu 6LoWPAN (Fig. 3.2), ContikiSec se situează imediat deasupra nivelului fizic, ca subnivel al IEEE802.15.4 MAC.

Cele trei moduri de securitate suportate de ContikiSec sunt obiectul principal al acestei analize: *ContikiSec-Enc*, *ContikiSec-Auth* și *ContikiSec-AE*. Acestea oferă, pe rând, următoarele caracteristici de securitate: doar confidențialitate, numai autentificare și autentificare cu criptare. Pentru o implementare reală, acest lucru permite flexibilitate în adaptarea nivelul de securitate cu cerințele de procesare și de comunicare, și de asemenea potrivit constrângerilor de aplicare. În Tabelul 3.1 sunt definite cele trei moduri de securitate ale ContikiSec și diferiți parametri asociați acestora.

Tabelul 3.1 Modurile de securitate ale ContikiSec

	ContikiSec-Enc	***ContikiSec-Auth***	***ContikiSec-AE***
Proprietăți	confidențialitate	integritate și autentificare	confidențialitate, integritate si autentificare
Mod de operare	CBC-CS	CMAC	OCB
Timp [us]	99	99	122
RAM [kB]	0.21	0.21	0.24
Mărime cod [kB]	39.74	41.54	45.5

*Cifrul utilizat este AES cu o dimensiune a cheii de 128 de biți.

Operațiunile de securitate (criptare, decriptare și autentificare) sunt efectuate în momentul trimiterii și primirii pachetelor de date. În Tabelul 3.1 este prezentat timpul necesar și consumul de memorie pentru fiecare operațiune în timpul transmisiei sau recepției unui pachet de un nod vecin, și dimensiunea codului în ceea ce privește amprenta de memorie pe un nod obișnuit. Una dintre caracteristicile aplicațiilor de WSN care trebuie să fie luată în considerare atunci când se alege o soluție de securitate este consumul de energie al nodurilor de senzori.

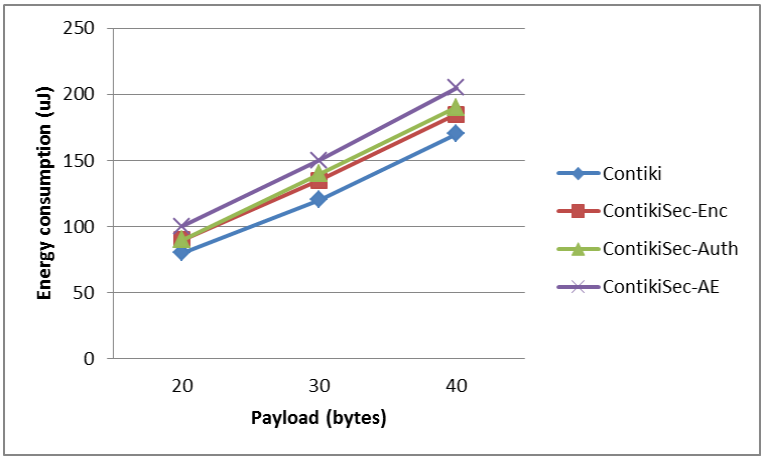

Fig. 3.4 Consumul de energie pentru fiecare din cele trei moduri de securitate

Așa cum este prezentat în Fig. 3.4, consumul de energie al Contiki în mod implicit variază de la 80 μJ la 170 μJ pentru pachete cu sarcini utile de la 20 la 40 bytes. Cu mecanismul de securitate aplicat, *ContikiSec-Enc* și *ContikiSec-Auth* au aproape același consum de energie, deoarece ambele suportă un overhead de 2 octeți. În final, *ContikiSec-AE* deține cea mai mare cerință de energie, consumând în jur de 15% mai mult decât Contiki în modul de bază, pentru mesaje de date cu sarcina utilă de 40 bytes.

Fig. 3.5 Topologia de rețea în mediul de simulare Contiki/COOJA

Datorită limitărilor de resurse ale acestor tipuri de rețele, este esențială măsurarea performanțelor rețelei în termen de eficiență, memorie, viteza de criptare, și consumul de energie. În Fig. 3.5 este prezentată rețeaua de test, formată din 15 noduri tip Tmote Sky.

În scenariul de testare, s-au folosit 14 noduri senzori (clienți) distribuite ierarhic, care trimit pachetele spre rădăcină (GW, nodul 1). De fapt, tot traficul este destinat nodului 1 (server), deoarece acest nod acționează ca un router pentru a transmite datele în Internet. Nodul server rulează protocolul UDP peste RPL. Serverul are rolul de a seta prefixul IPv6 al rețelei și de a genera arborele de rutare RPL

Canalul wireless utilizat în simulare este Unit Disk Graph Medium (UDGM) – Distance Loss, în care două noduri pot comunica unul cu celălalt numai dacă acestea se află în aceeași arie de transmisie. Raza de interferență reprezentată de cercul gri (a se vedea Fig. 3.5), este aria în care pot exista interferențe radio ale nodului curent. Topologia de rețea este selectată ca fiind una de tip mesh. Nodurile sunt configurate să aibă maxim 7 hopuri până la destinație, așa cum se poate vedea în Fig. 3.6. Numărul de hopuri reprezintă numărul de noduri intermediare prin care trece un pachet în ruta sa de la sursă spre destinație. Aceste valori sunt necesare pentru analiza comunicațiilor și a securității la nivel de nod. Legăturile rutelor descoperite au o rată mare de succes în cazul în care apar și alte transmisii în desfășurare (până la 100%).

Deși în general, rețelele de senzori wireless sunt foarte dependente de date, adică sunt conștiente de constrângerile în timpul transmiterii datelor, acest lucru poate fi folosit pentru a configura rețeaua. Astfel, se pot obține indicatorii de performanță cantitativi și calitativi specificați.

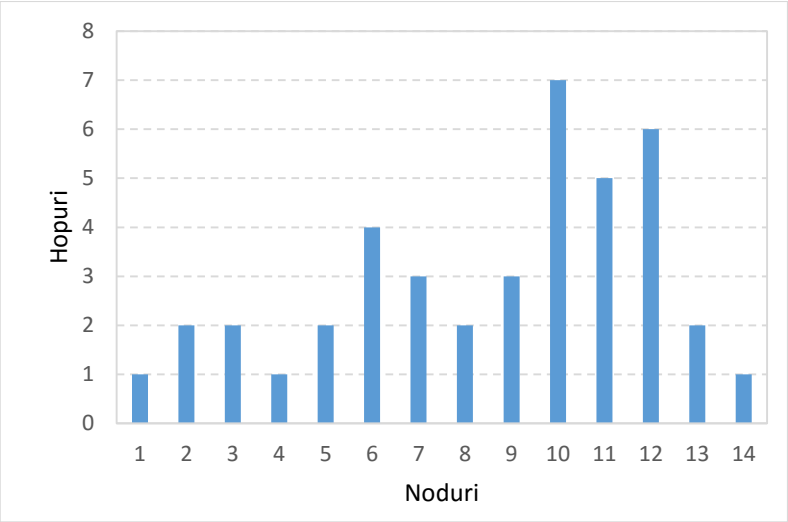

Fig. 3.6 Numărul de hopuri per nod

Operațiile de securitate necesită flexibilitate în ceea ce privește utilizarea memoriei RAM. Mai există desigur și alți factori care influențează consumul de resurse, cum ar fi numărul de noduri vecine, raza de transmisie, sau dimensiunea sarcinii utile. Mai multă procesare rezultă mai multă utilizare a memoriei.

Într-un mediu IEEE802.15.4, toate comunicațiile sunt bazate pe pachete. Pentru a evalua constrângerile de comunicație ale schemei propuse în termen de timp consumat pentru schimbul de pachete, s-au utilizat proprietățile simulatorului Cooja. Mediul de simulare constă într-o rețea identică cu cea prezentată în Fig. 3.5. Fiecare mod de securitate al ContikiSec a fost evaluat, iar timpul necesar operațiilor și energia consumată pentru criptarea pachetelor IPv6 sunt oferite în figurile următoare.

Experimentele s-au desfășurat în decurs de 60 de minute ca timp total de simulare. Toate pachetele de date sunt trimise de la nodurile client, prin rețeaua 6LoWPAN, către nodul server, cu o sarcină utilă de 30 bytes. Radioul este capabil să transmită un total de 48 bytes per cadru de date, în forma ContikiSec-AE. Toate nodurile dețin în faza de setare inițială o cheie de 128 de biți.

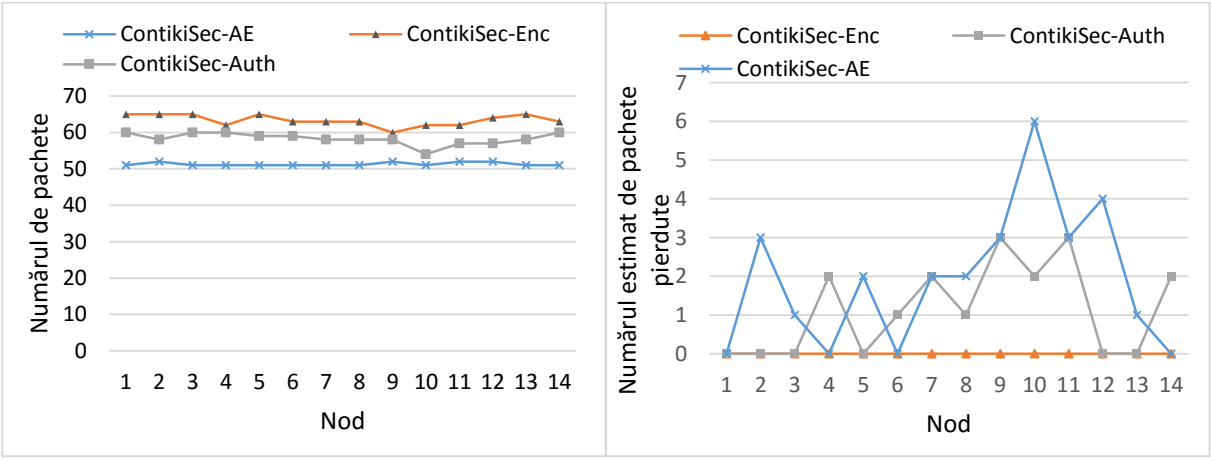

Fig. 3.7 Media estimată a pachetelor primite (stânga) și a celor pierdute (dreapta) per nod

Fig. 3.7 sugerează numărul de pachete transmise/ recepționate cu succes aplicând cele trei moduri de securitate examinate. Rezultatele arată că pierderea de pachete este mai mare pentru nodurile cu overhead suplimentar, ca în cazul ContikiSec-AE, și de asemenea, pentru

nodurile care se află la mai multe hopuri distanță de nodul colector. Aceste rezultate arată că ContikiSec-AE are un randament aproximativ excelent.

Deoarece energia este o sursă limitată în orice WSN, este necesară analiza impactului dintre cele trei moduri de securitate asupra performanțelor hardware. Contiki oferă un mecanism de înregistrare a energiei bazat pe software care ține evidența consumurilor de energie pentru fiecare nod. Fiind bazat pe software, mecanismul permite înregistrarea energiei la scara de rețea, fără niciun hardware suplimentar.

În Fig. 3.8 este ilustrată media ciclului de funcționare radio pe fiecare nod, fie în modul de ascultare sau modul de trimitere, calculat ca timpul total în care procesorul este activ. Datorită numărului de hopuri, unele noduri au calitatea de routere pentru vecinii lor, prin urmare acestea au ciclu de funcționare radio și consum de energie mai mari.

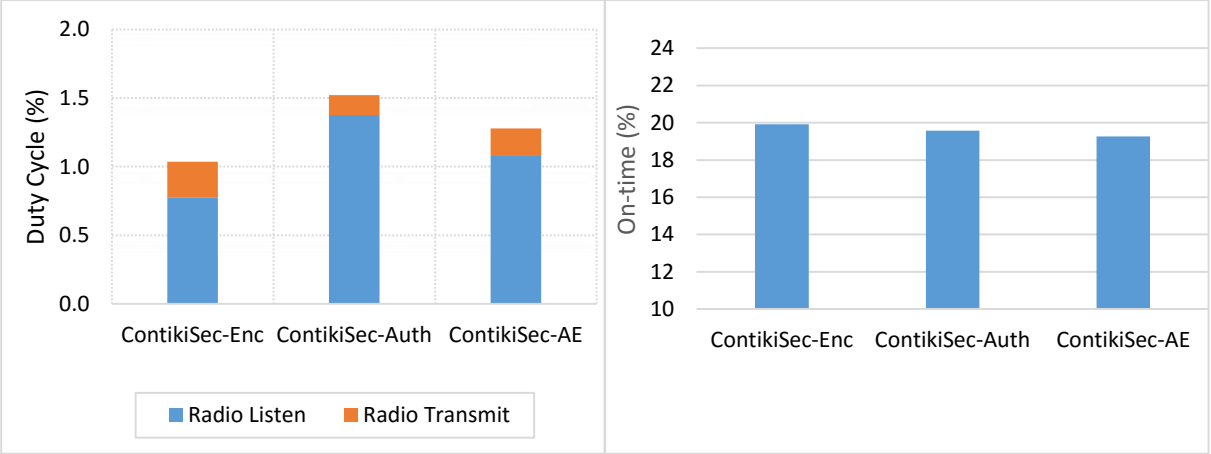

Fig. 3.8 Media ciclului de funcționare radio (stânga) și timpul total de activitate (dreapta)

După cum se poate observa în Fig. 3.8, radioul este activ între 19.26% - 19.92% din timpul total. Media timpului de activitate în care radioul a fost în modul de transmitere și modul de ascultare, variază între 1% - 1.5%. Timpul total de activitate este calculat ca suma timpului activ petrecut al radioului în cele două moduri de funcționare. Numerele din Fig. 3.8 reprezintă o metrică pentru a determina eficiența energetică a diferitelor configurații aplicate, deoarece acestea denotă cât timp a fost consumat de activitatea radio pentru fiecare pachet, în medie.

În rețelele de joasă-putere, transceiverul radio trebuie să fie oprit cât mai mult posibil pentru a economisi energie. Acest lucru este recomandat pentru aplicațiile în care nodurile sunt operate pe baterii. În Contiki, consumul redus de energie poate fi realizat cu ajutorul nivelului Radio Duty Cycle (RDC). Protocoalele configurate RDC și MAC pentru acest context sunt ContikiMAC și NullMAC. Timpul de repaus radio de aproximativ 80% se datorează mecanismului ContikiMAC utilizat în toate simulările.

Consumul de putere este descompus în categorii (Fig. 3.9), considerând memoria low-power, CPU și modurile radio de ascultare și de transmitere. Puterea în modul de ascultare este mai mare decât în modul de transmisie, pentru că nodurile au petrecut cea mai mare parte a timpului activ ascultând pachetele de la gateway, cereri de rutare și actualizări ale rutelor de vecini, decât transmițând date.

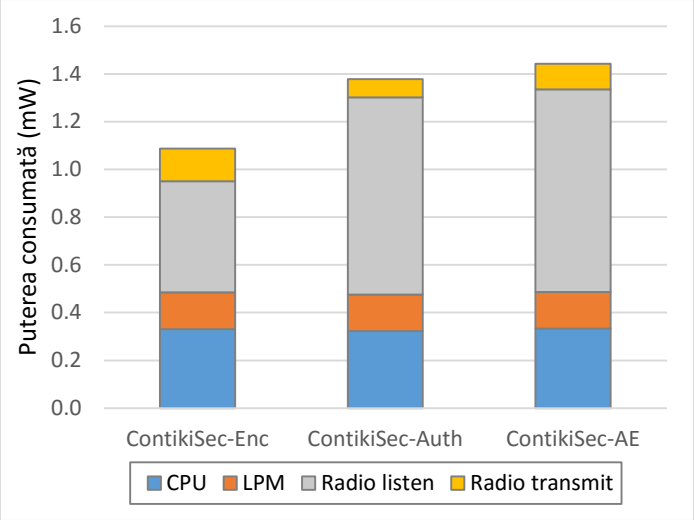

Fig. 3.9 Puterea consumată în medie, simulată

În faza inițială de set-up, nodurile client au nevoie de putere mai mare. Acest lucru se datorează schimbului de chei dintre noduri, descoperirea vecinilor și crearea arborelui de rutare, alocarea adreselor IPv6, etc.

Consumul de energie poate depinde de punerea în aplicare a rețelei și este specific hardware. De asemenea, rezultatele de simulare pot varia ușor la punerea în aplicare pe platforme de WSN reale. Aceste analize au rolul de a demonstra capacitatea rețelei de a include straturi de securitate și a proteja rețeaua respectivă atât împotriva atacurilor, pierderii de date, compromiterii nodurilor, eliminarea datelor eronate etc. Antetul ContikiSec poate reprezenta un factor de limitare cu privire la rata maximă de transmisie în aplicațiile WSN bazate pe IPv6. Acest factor, împreună cu impactul ContikiSec asupra energiei necesare nodurilor de senzori, demonstrează că acest mecanism comprimat oferă garanție și trebuie, de preferință, utilizat în aplicații cu cerințe de securitate ridicate.

3.4. STUDIU DE CAZ – ADĂUGAREA UNUI SUBSTRAT DE SECURITATE ÎN STIVA 6LOWPAN

3.4.1. Context

Securitatea 6LoWPAN depinde în principal de substratul de securitate IEEE802.15.4. Acest substrat oferă, de asemenea, chei-pereche între noduri pentru a diminua compromiterea de noduri. În prezent, stabilirea de chei-pereche este totuși nespecificată. Mai mult, cheile de tip broadcast sunt împărțite între noduri multiple, ceea ce nu prezintă rezistență la compromisuri.

În Fig. 3.10 este prezentată stiva de protocoale 6LoWPAN în care este reprezentat substratul LLSEC ce conține două add-on-uri IEEE802.15.4 eficiente-energetic și rezistente la atacuri DoS, și anume APKES și EBEAP. Acestea sunt soluții moderne, propuse în [23], ce prezintă un mecanism adaptabil pentru managementul cheilor, și un protocol de autentificare și criptare a mesajelor de tip broadcast în cazul rețelelor 6LoWPAN.

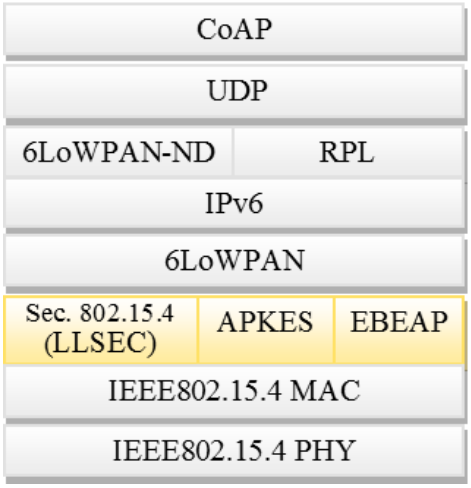

Fig. 3.10 Stiva de protocoale 6LoWPAN adaptată cu LLSEC

Introducerea securității în substratul legăturii de date prezintă o importanță deosebită. Datorită utilizării unui mediu wireless, atacatorii pot injecta și reda cadre IEEE802.15.4. În cazul în care substratul de securitate IEEE802.15.4 nu le filtrează, astfel de atacuri pot avea consecințe grave. Pe Nivelul 2.5, atacatorii pot lansa atacuri de fragmentare, care distrug pachetele IPv6 parțial reasamblate sau memoria cache [18]. Pe Nivelul 3, un atacator poate lansa atacuri DoS pe bază de cale (PDoS). Într-un atac PDoS, un atacator injectează pachete IPv6 fictive, care sunt dirijate prin intermediul rețelei 6LoWPAN, epuizând astfel bateria. Un alt atac asupra Nivelului 3 este de a injecta mesaje false Internet Control Message Protocol pentru IPv6 (ICMPv6) pentru a paraliza RPL sau 6LoWPAN-ND. Așa cum s-a discutat și în subcapitolul 3.3.2, mecanismele de securitate propuse sunt specifice doar anumitor aplicații, introduc complexitate sau nu previn toate atacurile WSN cunoscute. Substratul LLSEC propus în continuare protejează împotriva tuturor atacurilor cunoscute și este, așadar, mai eficient. În afară de asta, APKES previne nodurile neautorizate să se alăture unei rețele 6LoWPAN.

3.4.1. Analiza experimentală și rezultate obținute

Pentru a impactul adăugării mecanismelor de criptare suplimentare în sistemul de operare Contiki asupra randamentului unui nod, s-au realizat simulări cu diferite scenarii. Pentru evaluări, s-a folosit platforma hardware Tmote Sky, ale cărei caracteristici sunt de 16-bit MSP430 MCU, 10 kB RAM, 48KB ROM, stație radio de emisie-recepție CC2420, o memorie Flash externă, și diverse elemente sensibile (senzor de temperatură, luminozitate, zgomot, localizare etc.). Această configurație hardware furnizează un raport energie/ putere de calcul excelent și radio capabil cu standardul IEEE802.15.4. În continuare s-a folosit simulatorul integrat de rețea Cooja, care este capabil să imite noduri Tmote Sky (printre alte platforme) și să le conecteze. Codul executat de noduri este exact același firmware care rulează pe nodurile fizice. Modul de implementare și analizele experimentale sunt descrise în [24]. Un exemplu de o topologie utilizată pentru evaluare este reprezentată în Fig. 3.11.

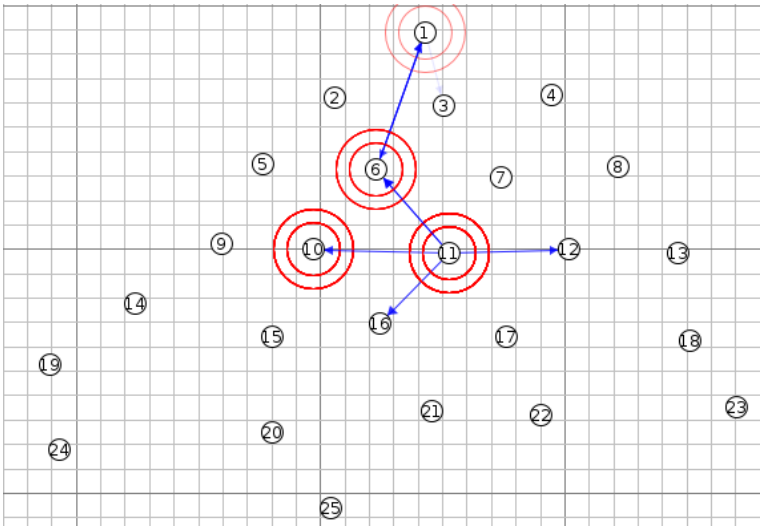

Fig. 3.11 Topologie WSN ierarhică propusă pentru evaluare, ce constă dintr-o rețea 6LoWPAN de noduri Sky emulate

Un nod (nod ID 1) este setat ca un border-router, în timp ce alte noduri se bazează pe comunicare RPL multi-hop. Border-router-ul va seta prefixul IPv6 a rețelei și va iniția crearea arborelui de rutare RPL. După cum se poate vedea în Fig. 3.11, nodurile sunt distribuite ierarhic, având un traseu configurat până la 6 hopuri și o gamă de transmisie de 70m. Link-urile de pe rutele folosite au o rată destul de ridicată de succes în cazul altor transmisii în curs de desfășurare (≥ 75%).

Contiki include un număr de protocoale ale ciclului de funcționare radio (RDC), cum ar fi ContikiMAC, LPP, și NullRDC. În ceea ce privește MAC, CSMA și NullMAC (non-persistent CSMA) sunt acceptate. Straturile implicite RDC și MAC în Contiki pe Tmote Sky sunt ContikiMAC și CSMA.

Prin rularea tuturor experimentelor cu trei nivele diferite de securitate pe nivelul legătură de date (link-layer), se investighează în detaliu impactul stratului LLSEC privind performanțele end-to-end ale rețelei pe care este implementat. În prezent, există trei drivere LLSEC disponibile:

- *nullsec*, este activat în mod implicit și practic nu face nimic. Aceasta este utilizată ca referință în experimentele realizate.
- *noncoresec*, este o implementare de securitate IEEE802.15.4, cu capacitate de adaptare noncompromis (*noncompromise resilient*), care utilizează o singură cheie la nivelul întregii rețele.
- *coresec*, este un driver LLSEC compromis rezilient (*compromise resilient*), care pune în aplicare securitatea IEEE802.15.4, și protocoalele APKES și EBEAP, descrise anterior. APKES prevede perechi de chei pentru fiecare sesiune stabilită cu noduri vecine. Diferite scheme de predistribuire a cheilor pot fi conectate la APKES, astfel încât să se adapteze la diferite rețele 6LoWPAN și modele de amenințare. În prezent, sunt disponibile schemele de ”criptare localizată și autentificare” (LEAP) și sistemul complet de stabilire a perechilor de chei (*fully pairwise keys*). EBEAP este utilizat pentru autentificarea (și opțional criptarea) cadrelor broadcast.

3.4.1.1. *Analiza alocării de memorie*

În scopul de a analiza amprenta de memorie a diferitelor niveluri de securitate aplicate unei rețele 6LoWPAN, s-a măsurat dimensiunea memoriei de program pentru ambele tipuri de noduri: border-router și nodurile expeditor.

În Tabelul 3.2 este analizat efectul folosirii diferitelor configurații ale subnivelului de securitate, în ceea ce privește dimensiunea codului firmware.

Tabelul 3.2. Amprenta memoriei asupra dimensiunii codului (kB)

Mod LLSEC	Border router	Nod 6LoWPAN
nullsec	39.47 kB	39.22 kB
noncoresec	40.33 kB	40.08 kB
coresec + NullRDC + NullMAC	40.17 kB	39.93 kB
coresec + ContikiMAC + CSMA	43.78 kB	43.53 kB
coresec + ContikiMAC + NullMAC	41.81 kB	41.57 kB

Memoria de program necesară este acceptabilă pe nodurile Tmote Sky, care au în total 48kB de memorie de program. Utilizarea configurației ContikiMAC + CSMA presupune un consum mai mare de memorie. În principiu, cele mai bune opțiuni pentru a salva memorie sunt, de exemplu, dezactivarea optimizării fazei, folosind NullMAC în loc de CSMA, sau dezactivarea criptării datelor.

Pentru fiecare tip de driver de securitate, s-a măsurat impactul securității asupra amprentei de memorie utilizată. După cum se poate vedea în Fig. 3.12, dimensiunea memoriei crește liniar odată cu numărul de vecini.

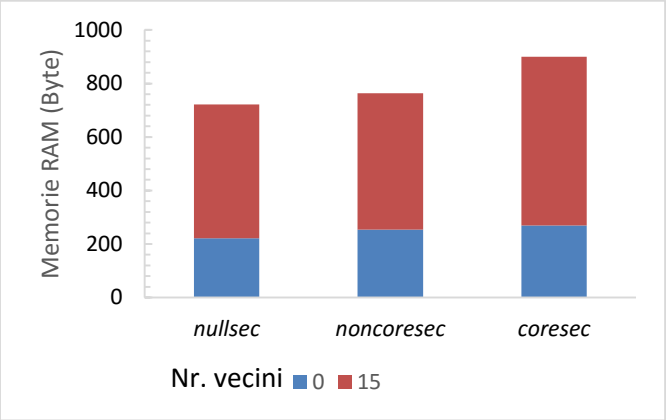

Fig. 3.12 Amprenta memoriei în funcție de numărul de vecini

În exemplul nostru, mărimea cheii pentru stabilirea perechilor de noduri este de 12 octeți și cheia de broadcast este de 8 octeți. Având în vedere că nodurile Tmote Sky au 10kB de RAM, overhead-ul asupra memoriei RAM rezultat este semnificativ. În acest caz, capacitatea nodurilor de senzori de a șterge vecini este imperativă.

3.4.1.2. *Analiza consumului de energie*

În scopul de a măsura timpul de calcul și energia necesară pentru criptarea unui pachet 6LoWPAN, fiecare experiment a rulat cel puțin 30 de minute pentru ca nodurile expeditor să trimită cat mai multe pachete posibil la border-router. Toate pachetele de date au o sarcină utilă de 16-byte. Radioul trebuie să transmită un total de 79 de bytes per cadru de date. Toate experimentele au fost efectuate cu și fără securitate activată; prin urmare, o stivă Contiki nemodificată este menționată cu *nullsec* în figurile următoare.

Consumul de energie este descompus în categorii, având în vedere memoria low-power, CPU, și modurile radio de a asculta și de a transmite. Consumul de putere în modul de ascultare este mai mare decât în modul de transmisie, deoarece nodurile petrec cel mai mult timp activ ascultând pachete de la nodul colector, cererile de rutare și actualizări ale rutelor de la vecini, decât transmiterea propriu-zisă de date.

Fig. 3.13 ilustrează numărul de pachete transmise cu succes a celor trei moduri de securitate examinate, în funcție de numărul de hopuri. Din Fig. 3.13 (dreapta) reiese ciclul de

activitate al nodurilor, de asemenea dependent de numărul de hopuri. Timpul total este calculat prin însumarea timpului petrecut cu radio activ și timpul petrecut în modul ascultare. Numerele din Fig. 3.13 (dreapta) reprezintă o metrică pentru eficiența energetică a diferitelor configurări, deoarece acestea indică modul în care radioul a petrecut mult timp în modul activ, per pachet, în medie.

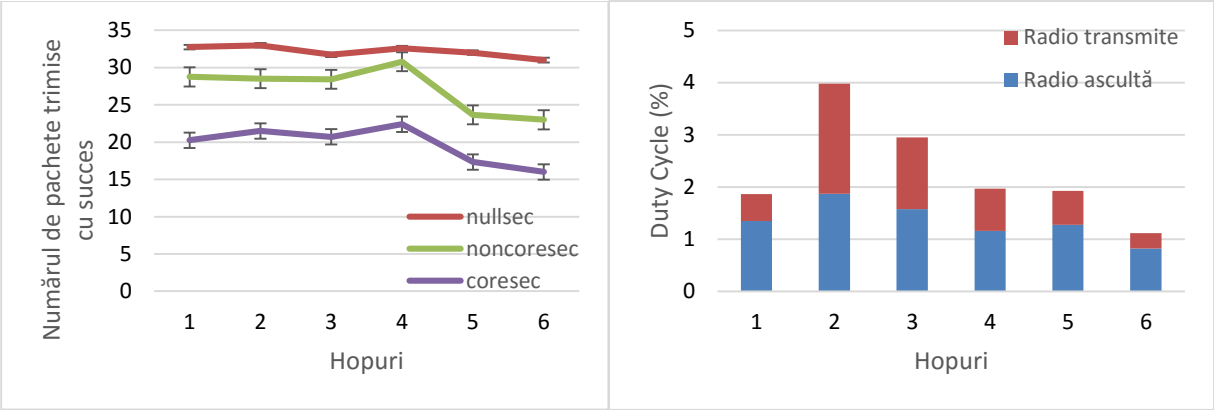

Fig. 3.13 Transferul de date comparativ al driverelor *nullsec*, *noncoresec*, și *coresec* (stânga) și consumul de energie, per ansamblu, activând cele trei moduri LLSEC (dreapta)

Consumul de energie pentru a transmite cadre depinde în mare măsură de protocolul MAC utilizat. Atunci când se utilizează ContikiMAC, trimiterea de cadre broadcast este relativ consumatoare de energie, deoarece fiecare cadru este în mod repetat transmis în timpul unui interval de trezire. Potrivit [25], acesta consumă ≈1.8mJ pe nodurile Tmote Sky, indiferent de lungimea pachetului broadcast. Prin contrast, o recepție a pachetului broadcast consumă doar ≈0.2mJ în ContikiMAC.

CAPITOLUL 4
REALIZAREA UNUI MODEL DE SECURITATE 6LOWPAN PENTRU REȚELE DE SENZORI WIRELESS INDUSTRIALE

4.1. REȚELE DE SENZORI WIRELESS INDUSTRIALE (IWSN)

Rețelele de senzori wireless industriale (IWSN) reprezintă un sector în curs de dezvoltare al rețelelor de senzori wireless (WSN), având constrângeri specifice legate de particularitățile sistemelor de automatizare industriale. Proiectarea și implementarea rețelelor de senzori wireless industriale sunt sarcini extrem de dificile. Cele mai multe din provocările actuale IWSN sunt legate de mediul dinamic în cazul în care sunt amplasate IWSNs, durata de viață de funcționare, eterogenitatea, operare autonomă, mentenabilitatea, fiabilitatea și nu în ultimul rând, securitatea [26].

Securitatea este una dintre principalele provocări în IWSN. Conceptul de securitate se poate referi la informațiile care curg prin sistem, produselor și echipamentelor, sau securitatea persoanelor. În acest studiu de caz, obiectivul principal se centrează pe asigurarea informațiilor în timp real oferite de rețea. Pentru obiectivele relevante, se consideră că securitatea ar trebui să fie abordată în mod corespunzător ca parte integrantă a straturilor din stiva de protocoale, atât la nivel scăzut cât și la nivel înalt. Amenințările posibile prezente într-o IWSN includ: divulgarea datelor sensibile / confidențiale, Denial of Service (DoS), accesul neautorizat la resursele wireless, potențiala slăbire a măsurilor de securitate existente în rețelele și sistemele conectate.

În prezent, există o tendință de a folosi protocolul IPv6 în zona WSN. Este important a se determina dacă dezvoltările recente ale rețelelor fără fir bazate pe IPv6 (de ex., 6LoWPAN, SNAP) sunt potrivite pentru IWSNs. Aceste protocoale sunt în principal destinate pentru automatizarea locuințelor și nu a aplicațiilor industriale. Principala nelămurire cu protocoalele wireless bazate pe IP este dacă overhead-ul mare al protocolului poate fi justificat într-un caz industrial. Este important pentru dezvoltarea comercială a IWSNs de a presta servicii care pot fi accesate de la distanță de pe Internet, și, prin urmare, trebuie să fie integrate cu protocolul IP [27].

IWSNs suportă aplicații industriale eterogene cu cerințe diferite. Este necesar să se dezvolte arhitecturi scalabile și flexibile, care pot depăși toate cerințele într-o singură infrastructură [27]. O arhitectură generală a unui IWSN este ilustrată în Fig. 4.1.

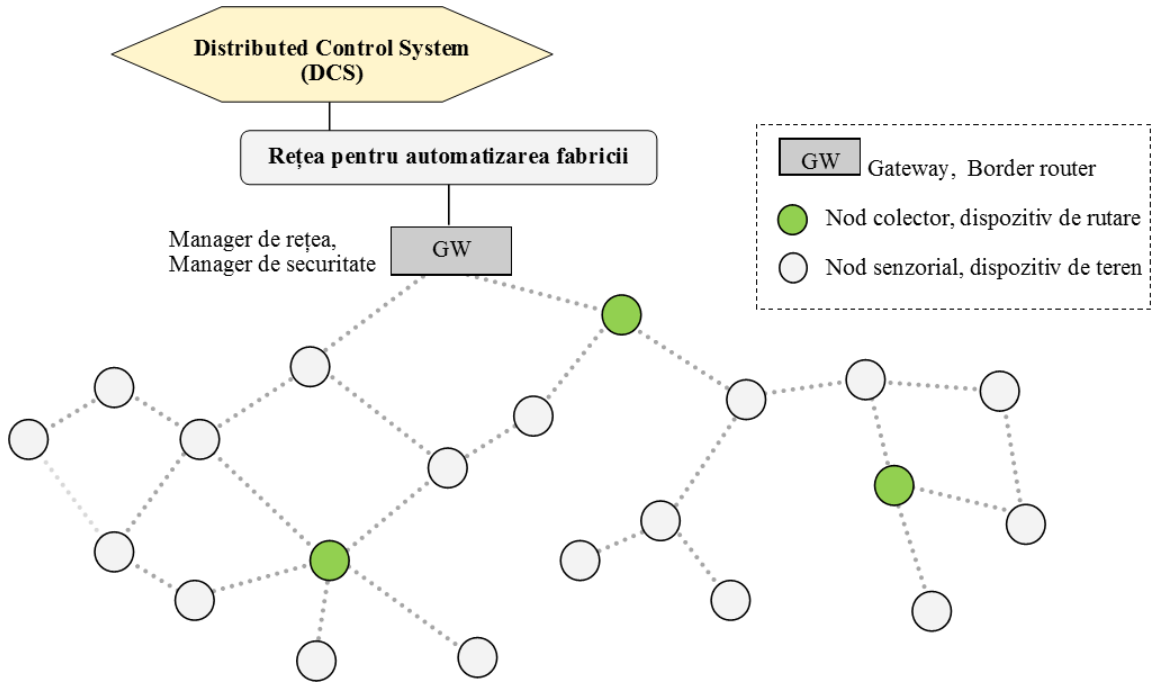

Fig. 4.1 Arhitectura generală a unei rețele se senzori wireless industriale

4.2. PROVOCĂRI ALE SECURITĂȚII ÎN REȚELE IWSN

În general, problemele de securitate nu sunt tratate în mod independent, un compromis între gradul de utilizare și performanță trebuie să fie adresat [27]. Nodurile senzoriale sunt dispozitive cu resurse limitate, iar unele dintre ele pot fi mobile. Această mobilitate necesită adesea o re-autentificare. În plus, aplicația industrială poate solicita ca nodurile senzoriale ar trebui să fie confidențial protejate. Toate aceste preocupări ar trebui abordate de către soluțiile de securitate propuse, destinate IWSN. Provocările de securitate asociate cu IWSNs pot fi enumerate după cum urmează:

- Constrângeri legate de resurse;
- Scalabilitate;
- Suport pentru mobilitate;
- Conectivitate intermitentă;
- Confidențialitate.

4.3. STUDIU DE CAZ – ABORDAREA SECURIZĂRII UNEI REȚELE DE SENZORI WIRELESS INDUSTRIALE

Acest studiu de caz tratează implementarea unei o soluții-cadru de securitate în contextul rețelelor de senzori wireless industriale (IWSN). Un accent deosebit se pune pe utilizarea rețelelor bazate pe comunicații IPv6 și pe o serie de provocări de securitate asociate aplicațiilor industriale. Modul de implementare și analizele experimentale sunt descrise în [28]. Se prezintă, de asemenea, potențiale configurații de arhitectură pentru monitorizarea aplicațiilor industriale, cu scopul de a depăși provocările de securitate existente în astfel de aplicații. Se utilizează în continuare sistemul de operare Contiki pentru dispozitive cu resurse limitate, împreună cu substraturile de securitate link-layer și 6LoWPAN.

În studiile efectuate anterior, s-au analizat constrângerile de comunicare și de securitate într-un WSN bazat pe 6LoWPAN (vezi secțiunea 3.3), apoi atenția s-a concentrat asupra punerii în aplicare a unei soluții de securitate pentru o rețea 6LoWPAN (vezi secțiunea 3.4). În acest paragraf, se încearcă o abordare a soluțiilor de securitate studiate într-un context de

aplicabilitate IWSN, deoarece aceste au constrângeri specifice (de ex., interoperabilitatea, fiabilitatea, standardizare) peste WSNs generale bazate pe IPv6. Se oferă o scurtă descriere a provocărilor de securitate prezente în IWSNs și se încearcă definirea unui cadru de securitate pentru utilizarea în aplicații IWSN.

4.3.1. Modelarea sistemului

Mai multe elemente din spațiul de proiectare al IWSN trebuie să fie discutate, ca un pas preliminar pentru potențiale implementări fezabile ale unui substrat de securitate în stiva 6LoWPAN, considerată pentru acest tip de rețele. La proiectarea de mecanisme de securitate pentru IWSNs, obiectivele de securitate trebuie să fie adresate pentru toate nivelele din stiva de protocoale. De exemplu, stabilirea cheilor și managementul încrederii, autentificarea, confidențialitatea, rutare sigură, protecția integrității, prevenirea DoS, rezistența la nodurile compromise, etc. sunt doar câteva din sarcinile de securitate pe care ar trebui să le acopere. În plus, overhead-ul de securitate ar trebui să fie echilibrat împotriva tuturor celorlalte cerințe, din cauza limitărilor de resurse ale rețelelor IWSN. În acest context, sarcina proiectantului de rețele de senzori este, în primul rând, de a alege dintr-o gamă de algoritmi, protocoale și platforme disponibile care construiesc un sistem complet, în timp ce folosește instrumente hardware și software larg acceptate [27].

Următoarea arhitectură (Fig. 4.2) reprezintă o propunere de instrumente selectate pentru un design sigur de aplicație de monitorizare a mediului sau de monitorizare a stărilor unui IWSN. Selecția de protocoale se bazează pe cerințele de eficiență energetică, de precizie, latență și timp de sincronizare.

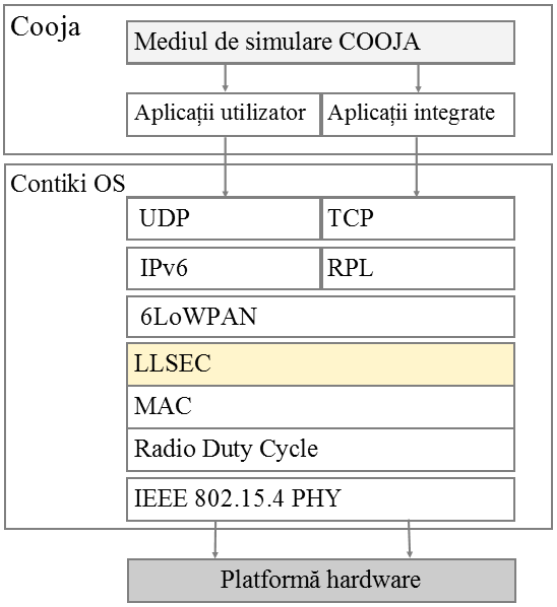

Fig. 4.2 Arhitectură de securizare propusă pentru o rețea de senzori wireless industrială. Mecanismul de securitate ales este LLSEC.

Ca sistem de operare ales să soluționeze problemele de scalabilitate, interoperabilitate și constrângeri hardware/software, s-a utilizat Contiki [29]. Acesta este proiectat special pentru dispozitive cu resurse limitate, și rulează pe o varietate de platforme hardware. De asemenea este ușor de implementat și adaptat. Acesta are o amprentă de memorie foarte mică, un sistem tipic poate rula cu mai puțin de 10K de memorie RAM și 30K de ROM. Pentru a sprijini dezvoltarea sistemelor low-power, Contiki prevede mecanisme pentru estimarea consumului de energie al sistemului și pentru a înțelege unde se cheltuie cea mai multă energie. În plus, Contiki oferă o stivă rețea IP completă, cu protocoale IP standard, cum ar fi UTP, TCP și HTTP, inclusiv suport pentru noile standarde de mică putere și comunicații IPv6, cum ar fi 6LoWPAN, CoAP, RPL etc.

Platforma hardware Tmote Sky aleasă este una dintre cele mai populare platforme WSN sub Contiki OS, folosite în rețele de senzori, în aplicații de monitorizare și prototipizare rapide ale aplicațiilor. Specificațiile Tmote Sky sunt: 16-bit MSP430 MCU, 10 KB de memorie RAM, 48 kB ROM, radio de emisie-recepție CC2420, o memorie flash externă, și diverse elemente sensibile [22]. S-a ales această platformă cu cost scăzut, ca și soluție hardware cu consum redus de energie, pentru a testa performanța arhitecturii cu adaos de securitate propusă. Tmote Sky permite o gamă largă de aplicații de rețea tip mesh și este, de asemenea, eficientă energetic [30].

Stratul IEEE802.15.4 MAC oferă controlul accesului la un canal partajat și încredere ridicată în livrarea de date. În rețelele low-power, radioul trebuie să fie oprit cât mai mult posibil pentru a economisi energie. Acest lucru este recomandat pentru majoritatea aplicațiilor în care nodurile operează pe baterii. În Contiki, consumul redus de energie poate fi realizat prin stratul RDC. Protocoalele configurate RDC și MAC pentru acest studiu de caz sunt ContikiMAC și CSMA-CA. Astfel sunt asigurate cerințele de eficiență energetică, fiabilitate și sincronizare în timp.

Substratul de securitate la nivelul legăturii de date (LLSEC) reprezintă un nou antet comprimat pentru stiva Contiki. Acest substrat depinde foarte mult de mecanismele de securitate IEEE802.15.4 existente și acceptă stabilirea de chei-pereche, astfel încât să atenueze efectul de compromitere a nodurilor. Motivul pentru care acest substrat poate fi adecvat unei aplicații IWSN este datorită eficienței energetice și rezistenței la atacuri DoS [23]. Mecanismul de stabilire a cheilor utilizat este cel propus în [23], numit Adaptable Pairwise Key Establishment Scheme (APKES). Rolul său este stabilirea perechilor de chei pentru sesiunile de comunicație cu nodurile vecine. Diferite scheme de pre-distribuție a cheilor pot fi configurate pentru ca APKES să se adapteze la diferite rețele 6LoWPAN (de ex., LEAP, schema completă a perechilor de chei, schema aleatoare a cheilor-pereche). În al doilea rând, este folosit un protocol ușor de implementat și rezilient la compromisuri, pentru autentificarea cadrelor broadcast. Împreună, aceste protocoale detectează noduri compromise, previn toate atacurile WSN cunoscute și sunt eficiente energetic. Mai mult, LLSEC previne nodurile neautorizate să adere la o rețea 6LoWPAN.

Din punct de vedere industrial, avantajele folosirii 6LoWPAN sunt abilitatea de a comunica direct cu alte dispozitive IP la nivel local sau prin rețeaua IP (de ex., Internet, Ethernet), arhitecturi existente și de securitate, model de date la nivel de aplicație stabilit și servicii (de ex., HTTP , HTML, XML), instrumente de management al rețelei stabilite, protocoale de transport, precum și suport pentru o opțiune IP în majoritatea standardelor wireless industriale.

4.3.2. Analiza experimentală și rezultate obținute

Acest studiu evaluează fezabilitatea implementării schemei propuse în conformitate cu cerințele de securitate ale IWSNs prezentate în secțiunea 4.3.2. Pentru a demonstra că soluția de securitate funcționează într-un scenariu industrial real și că sistemul îndeplinește cerințele specifice aplicației, s-au realizat diferite experimente cu ajutorul simulatorului de rețea Contiki / Cooja. Cooja are capacitatea de a emula platforme hardware WSN reale și oferă simulare în timp real. Acesta este capabil să imite nodurile Tmote Sky (printre alte platforme WSN) și să le conecteze. Codul executat pe nodul simulat este firmware-ul exact care rulează pe nodul fizic.

Pentru a afișa fezabilitatea și performanța substratului de securitate, am testat o rețea cu mai mult de zece noduri senzoriale, cu și fără criptare activată. Parametrii utilizați pentru simulare se bazează pe hardware-ul Tmote Sky. Rezultatele experimentale colectate sunt prezentate în Fig. 4.3-Fig. 4.5:

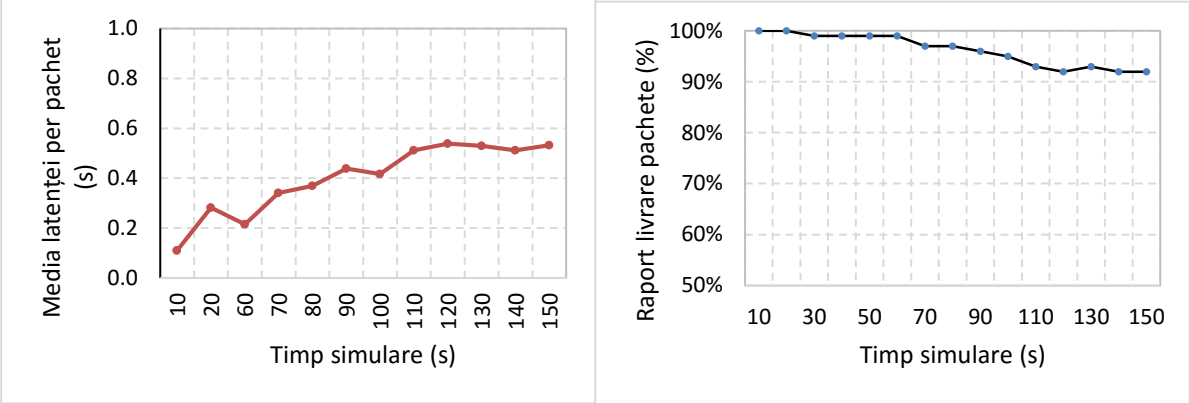

Fig. 4.3 Latența în timp calculată ca media tuturor pachetelor recepționate la un moment dat și raportul de livrare al pachetelor în timp, calculat ca media tuturor pachetelor recepționate la un moment dat

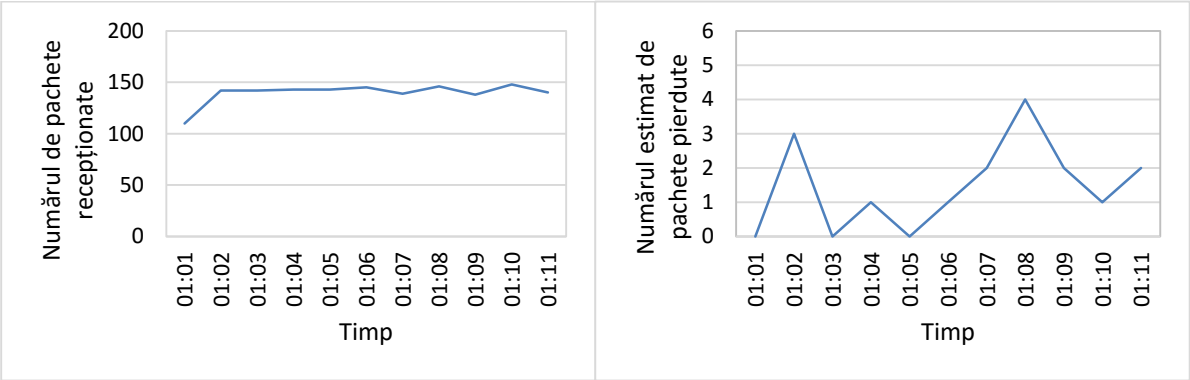

Fig. 4.4 Numărul de pachete recepționate și numărul estimat de pachete pierdute, în timp

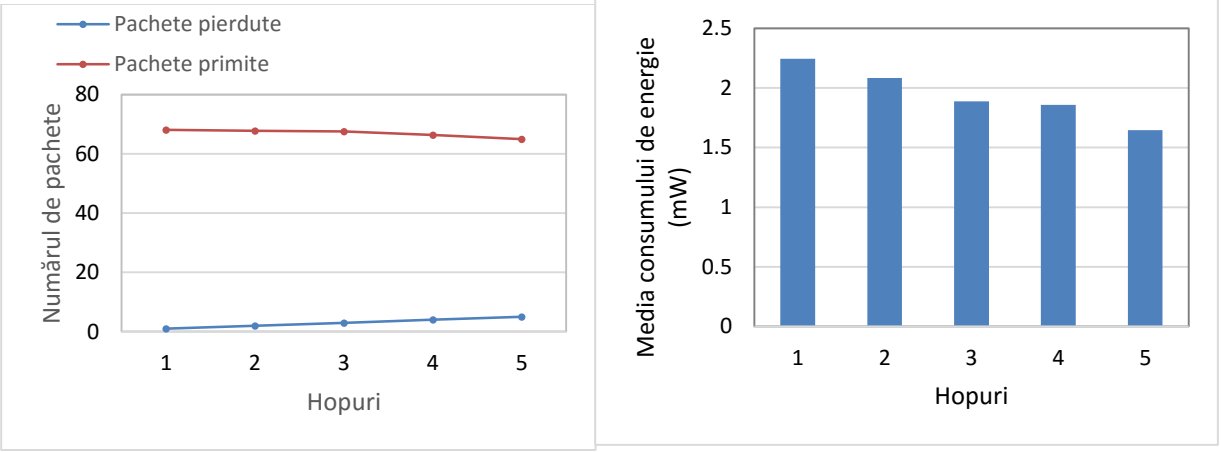

Fig. 4.5 Numărul de pachete transmise cu succes și numărul de pachete pierdute în timp, în funcție de numărul de hopuri. Media consumului de energie, în funcție de numărul de hopuri

Rezultatele prezentate sunt bazate pe topologia simulată pe o durată de 705 secunde, timp în care toate nodurile senzoriale generează pachete în cadrul unor intervale fixe (10s).

Rezultatele experimentale arată că implementarea modelului propus pe o rețea de 50 de noduri IWSN oferă o convergență a rețelei eficientă (44s), overhead al traficului de control (2841 pachete), consum de energie (15% de radio activ), latență (0.41s), raportul de livrare pachete (96%) în aceaste simulări de test, după o configurare atentă a razei de transmisie, ratei de succes a conexiunii (> 85%), timpul de funcționare radio, și frecvența mesajelor. Timpul în care radioul este în modul sleep este de 85%, și se datorează mecanismului ContikiMAC utilizat în toate simulările.

CAPITOLUL 5
INTEGRAREA REȚELELOR DE SENZORI WIRELESS ÎN INTERNET OF THINGS ȘI CYBER-PHYSICAL SYSTEMS

5.1. INTERNET OF THINGS

Internet-of-Things introduce o viziune a unui viitor Internet în care utilizatorii, sistemele computaționale și obiecte de zi cu zi ce dețin capabilități senzoriale și de acționare, cooperează pentru un confort fără precedent și beneficii economice. Ca și în cazul arhitecturii actuale Internet, protocoalele de comunicații bazate pe IP vor juca un rol-cheie care să permită conectivitate omniprezentă a dispozitivelor în contextul aplicațiilor IoT. Astfel de tehnologii de comunicare sunt dezvoltate în conformitate cu constrângerile platformelor senzoriale care ar putea fi utilizate de aplicațiile IoT, formând o stivă de comunicații în măsură să ofere raportul putere-eficiență necesar, fiabilitate, și conectivitate la Internet. Deoarece securitatea este un factor fundamental al celor mai multe aplicații IoT, o serie de mecanisme trebuie să fie concepute pentru a putea proteja comunicațiile activate de astfel de tehnologii.

În Fig. 5.1 se observă rolul senzorilor ca elemente fundamentale în aplicațiile inteligente de monitorizare și control din diverse domenii. S-a demonstrat în capitolul 3 că utilizarea comunicațiilor IPv6 în cadrul rețelelor WSN contribuie la integrarea acestora în Internet, prin urmare au o contribuție majoră în dezvoltarea și evoluția IoT.

Fig. 5.1 Modul de integrare al rețelelor de senzori wireless în IoT

5.2. HUMAN-IN-THE-LOOP CYBER-PHYSICAL SYSTEMS

Evoluția IoT împreună cu elemente din robotică și rețele de senzori wireless ne permit să creăm sisteme cyber-fizice (CPS) inteligente. Sistemele cyber-fizice se referă la sisteme cu capacități de calcul și fizice integrate care simt și controlează cu ușurință mediul din jurul nostru. Majoritatea sistemelor critice de securitate sunt interactive, adică, acestea interacționează cu o ființă umană, iar rolul operatorului uman este esențial pentru funcționarea corespunzătoare a sistemului. Astfel de sisteme de control interactive sunt denumite ca sisteme de control *human-in-the-loop* (HiTLCS).

Human-in-the-Loop Cyber-Physical System (HiTLCPS) este o paradigmă în care omul este parte a buclei de control, iar emoțiile sale afectează ieșirile sistemului. De exemplu, când o persoană este stresată, sistemul răspunde astfel încât starea emoțională a persoanei să se îmbunătățească; astfel, sentimentele unei persoane sunt responsabile pentru acționarea directă a sistemului.

HiTCCPS deduc stările psihologice și fiziologice umane prin intermediul senzorilor, ca feedback pentru bucla de control. Aceste sisteme sunt mult mai avansate, deoarece necesită detectare precisă și modelarea aspectelor comportamentale, psihologice și fiziologice ale naturii umane. Costurile de funcționare incorectă în domeniile de aplicare a acestor sisteme pot fi foarte severe. Pe de altă parte, includerea oamenilor ca o parte integrantă în bucla de control ar putea îmbunătăți foarte mult performanța și eficacitatea celor mai multe CPS. Ca o dovada a conceptului propus se prezintă, de asemenea, o aplicație conștientă emoțional care încearcă să influențeze pozitiv viața studenților, fără a compromite intimitatea acestora.

În prezent, asistăm la o creștere extraordinară în sisteme care sesizează diferite aspecte ale oamenilor și mediile din jurul acestora. În special, detectarea emoțiilor umane poate conduce la aplicații conștiente de emoții care utilizează aceste informații pentru a ajuta la îmbunătățirea vieții de zi cu zi ale oamenilor, și de asemenea oferind noi oportunități de afaceri. De obicei asociate cu consultațiile terapeutice, aceste sisteme au început să apară din ce în ce mai mult prin intermediul Internetului și smartphone-urilor. Utilizând senzorii smartphone-ului pentru a monitoriza indivizi, nu numai că ajută la primirea de feedback util în corectarea comportamentului dăunător, ci și la studiile aduse cercetătorilor în comportamentul afectiv. Această abordare pune problema menținerii vieții private pentru acest tip de aplicații. Așa cum s-a demonstrat în cercetări ulterioare [31], [32] achiziționarea stării emoționale a omului necesită conexiuni fiabile de rețea. Modelul teoretic evaluat (Fig. 5.2) abordează problema gestionării confidențialității și interfețelor de rețea bazate pe context uman.

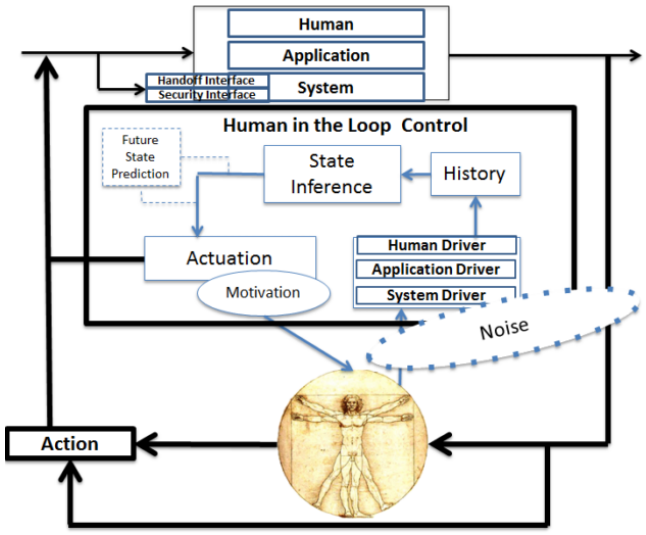

Fig. 5.2 Model general pentru procesul de control *Human-in-the-Loop*

Pentru a monitoriza și transmite în mod eficient contextul actual al omului în bucla de control, este adesea necesar să se păstreze o conexiune activă, cu respectarea cerințelor de calitate a serviciilor (QoS). Alte aspecte de rețea sunt la fel de importante, și anume informațiile de la senzori ar trebui să fie transmise și criptate doar atunci când este necesar, pentru a economisi lățimea de bandă, bateria și puterea de procesare. Managementul HiTL poate regla nivelurile necesare de confidențialitate, criptare, frecvența datelor, redundanță și interfețe de rețea în dispozitivele mobile.

5.3. STUDIU DE CAZ - DEZVOLTAREA UNUI MECANISM DE ASIGURARE A CONFIDENȚIALITĂȚII APLICAȚIILOR HITLCPS

5.3.1. Metode de asigurare a intimității utilizatorilor

Intimitatea (*privacy*) este dreptul pe care îl are o persoană de a controla ce se întâmplă cu identitatea sa și cu datele sale personale. Utilizarea Internetului și tranzacțiile online generează o cantitate mare de informații personale ce furnizează detalii despre personalitatea și interesele utilizatorilor. Probleme de invazie a intimității unei persoane apar în cazul proceselor de potrivire de date și de extracție a profilului personal, care folosesc aceste date singure sau în combinație cu alte date disponibile public. În [33] autorii introduc cinci principii de confidențialitate care ar trebui să permită designerilor să creeze rețele mobile care să adreseze neliniștile utilizatorilor individuali și a publicului larg prin minimizarea colectării de date cu caracter personal. Aceste principii sunt cuprinse pe scurt în **Tabelul 5.1**.

Tabelul 5.1 Cadru de proiectare a sistemelor confidențiale

	Principii	**Cerințe**	**Practici de proiectare**
1	Transparență în colectarea datelor	Descriere Irevocabilitate Inteligibilitate	Politici de confidențialitate Tehnologii de stocare privacy-aware
2	Obținerea consimțământului de a colecta date	Confirmare Cerințe de opțiuni	Licențiere Atestări software Notificări
3	Minimizarea colectării datelor personale	Cerințe funcționale pentru colectare Procesare distribuită	Eliminarea datelor personale Agregare Anonimizare Mascare
4	Minimizarea identificării datelor cu indivizii	Non-atribuire Stocare separată	Anonimizare Autentificare Permisiuni exclusive
5	Minimizarea și securizarea reținerii datelor	Cerințe funcționale pentru reținere Securitate Non-reutilizare	Securizarea bazei de date Ștergerea datelor după utilizare

Pentru a aplica aceste practici de confidențialitate în acest studiu de caz, trebuie luate în considerare două probleme. În primul rând, nevoia de autentificare a utilizatorului, în timp ce se face un efort pentru a minimiza identificarea datelor cu persoane fizice. Și în al doilea rând, un sistem de răspuns confidențial, în timp ce feedback-ul cu informații contextuale către utilizatorii individuali este necesar. De asemenea, se consideră că un singur mecanism nu este suficient pentru a îndeplini cerințele de confidențialitate, care pot fi îndeplinite în schimb de o integrare corespunzătoare a diferitelor mecanisme de confidențialitate, de exemplu, anonimizare, autentificare, filtrare de confidențialitate, etc. Studii similare pe această temă au fost făcute în [34], [35].

5.3.2. Modelarea sistemului de asigurare a confidențialității în HiTL

Se propune un model general care se concentrează pe mecanismele de conservare a vieții private, din punct de vedere emoțional-conștient. Arhitectura sistemului conține o aplicație Android, un server principal și un server web. Utilizatorii care interacționează cu sistemul sunt: studenții ca utilizatori obișnuiți și managerii punctelor de interes care pot adăuga, șterge sau modifica evenimentele asociate punctelor de interes. Sistemul colectează periodic datele de la senzori într-un mod anonim și combină aceste informații pe serverul principal. **Fig. 5.3** ilustrează arhitectura aplicației HappyStudent și modelul propus pentru asigurarea intimității utilizatorilor (al studenților, în cadrul acestei aplicații).

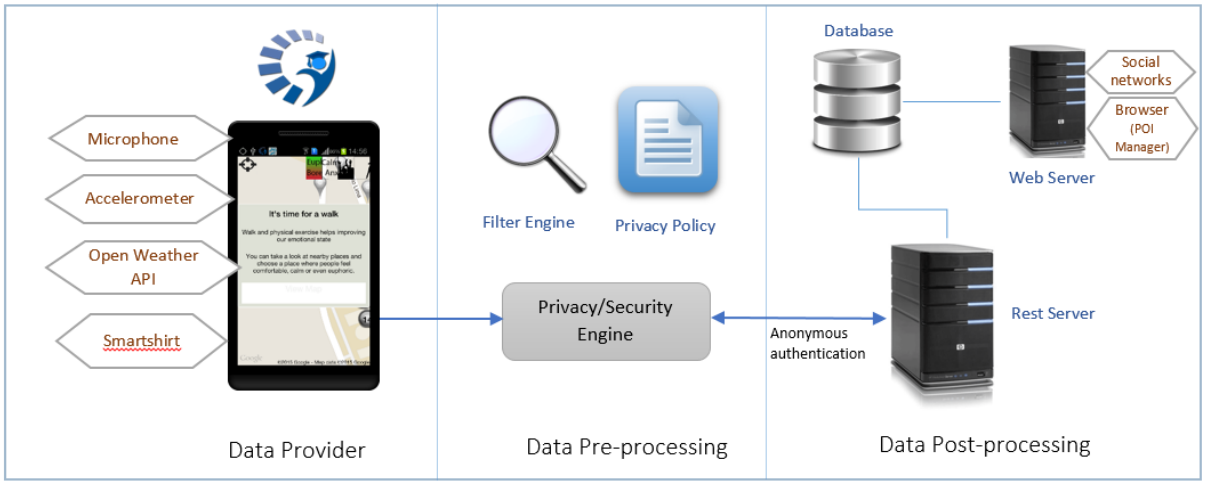

Fig. 5.3 Arhitectura HappyStudent

Motorul de confidențialitate/securitate constă în preprocesarea datelor primite de la senzori pentru a proteja viața privată a utilizatorilor. Datele sunt anonimizate, prin eliminarea informațiilor personale sensibile (de ex, număr de telefon, înregistrări telefonice, Bluetooth ID, nume sau adresă de email). Politicile definite de utilizatori (restricții în accesul la locație, dezactivarea notificărilor sau a urmăririi localizării) sunt considerate de către acest motor. Motorul de filtrare manipulează datele bazate pe politica de confidențialitate, care este disponibilă utilizatorilor în timpul înregistrării și conține următoarele informații:

- Informațiile individuale sunt furnizate la server în mod periodic. Informațiile de la toți utilizatorii sunt apoi agregate și actualizate periodic, în mod anonim.
- Locația utilizatorului nu este stocată în servere externe, servind pentru unicul scop de geolocalizare în hărțile prezentate și pentru calcule ale rutelor.
- Observațiile individuale de feedback nu sunt afișate public.
- Informațiile individuale sunt agregate, fără a expune orice asociere cu utilizatorii, pentru a calcula popularitatea de POI-uri.
- Toate datele cu caracter personal furnizate de către utilizator sunt stocate local pe telefon. Stocarea separată și autentificarea anonimă a utilizatorului previn stabilirea de legături între datele private și datele colectate.

Prin mecanismul de autentificare anonimă implementat, rețeaua nu cunoaște identitatea utilizatorului, în schimb se folosește de eticheta aleatorie generată pentru a contacta și oferi acces la echipamentul utilizatorului, după cum este necesar.

În funcție de rezultatul clasificării emoționale și a feedback-ului utilizatorului, controlul HiTL își asumă decizii diferite. Dacă este detectată o emoție pozitivă, nu se iau alte măsuri, iar sistemul reia starea de așteptare până la procedura de clasificare a emoției următoare. Cu toate acestea, în cazul în care o stare emoțională negativă este detectată (de ex., anxietate sau

plictiseală), sistemul ia măsuri directe pentru a îmbunătăți starea de spirit a utilizatorului. Acțiunile întreprinse de către sistem asociate cu fiecare profil de confidențialitate sunt specificate în **Tabelul 5.2**.

Tabelul 5.2 Definirea profilurilor de confidențialitate

Nivel de confidențialitate	Acțiuni
Low Level (Implicit)	Creștere frecvență de clasificare a emoției Urmărire localizare Activare a notificărilor POI Distribuire locație pe rețele de socializare
High Level	Scădere frecvență de clasificare a emoției Dezactivare a notificărilor POI

Nivelul scăzut (low-level) este legat de emoțiile negative, în timp ce nivelul înalt pentru emoții pozitive. Prin determinarea în mod automat a emoțiilor studentului, nivelurile de confidențialitate sunt adaptate în consecință. Aceste setări se pot modifica în conformitate cu regulile de confidențialitate, care sunt complet configurabile de către utilizator. Pe de altă parte, în cazul în emoția utilizatorului este pozitivă, sistemul aplică regulile pozitive și restabilește contramăsurile aplicate în starea emoțională negativă.

5.3.3. Implementarea aplicației de evaluare comportamentală

Pentru a urmări paradigma HiTLCPS, s-a conceput HappyStudent, o aplicație mobilă bazată pe un sistem de intervenție în schimbarea comportamentului (BCI), pentru a deduce starea emoțională curentă a studenților și pentru a folosi aceste informații pentru a genera feedback-uri sugestive, în scopul de a îmbunătăți bunăstarea fizică și mentală. Așa cum este prezentat în Fig. 5.2, studentul face parte din bucla de control și emoțiile sale afectează rezultatul sistemului. Având în vedere că emoțiile sunt introduse în sistem prin intermediul datelor primite de la senzori, HappyStudent urmează de asemenea, o paradigmă "people-centric-sensing" (detecție centrată pe oameni), în care senzorii de la smartphone-uri obțin date pentru a deduce contextul emoțional curent al utilizatorului.

Informațiile colectate de la senzori sunt procesate pentru a fi utilizate ca intrare a unui algoritm de "machine learning". Clasificatorii pentru determinarea emoțiilor sunt: valori prelucrate ale microfonului și accelerometrului de la smartphone, informațiile meteo de la un API extern care oferă temperatura, nebulozitatea și precipitațiile, și ritmul cardiac de la un semnal ECG primit cu ajutorul unui smartshirt. Emoția utilizatorului este dedusă o dată sau de două ori pe oră. Timpul dintre două achiziții senzoriale este determinat aleatoriu pentru a evita obișnuința utilizatorului. Rezultatul este afișat utilizatorului ca notificare pe telefon, și aplicația folosește corecția utilizatorului ca feedback pentru sistem. Emoția dedusă este apoi utilizată direct ca intrare la profilurile de confidențialitate și seturile de reguli pentru fiecare emoție. Utilizatorul este, prin urmare, responsabil pentru determinarea modului în care sistemul se adaptează la emoțiile sale.

În cercetări anterioare [36], s-a descoperit ca exercițiile de mers pe jos moderate și schimbarea mediilor poate declanșa emoții pozitive, deoarece activitățile fizice în aer liber oferă o serie de avantaje cognitive, cum ar fi îmbunătățirea memoriei, atenției și stării de spirit. Feedback-ul primit de la HappyStudent îi poate ajuta pe studenți să înțeleagă mai bine impactul pozitiv al interacțiunii lor sociale de zi cu zi și al activității fizice. Se consideră ca modelul propus se poate adapta și altor tipuri de utilizatori ai aplicațiilor HiTLCPS.

CONCLUZII FINALE ȘI CONTRIBUȚII PERSONALE. PERSPECTIVE

C 1. CONCLUZII GENERALE. DISCUȚII

Zi de zi se dezvoltă numeroase aplicații care au la bază rețelele de senzori. Acum și în viitorul apropriat rețelele de senzori vor ocupa un rol din ce în ce mai important în viața noastră de zi cu zi. Rețelele de senzori vor fi un element esențial în industrie, agricultură, medicină și aplicațiile casnice. De aceea rețelele de senzori trebuie sa fie din ce în ce mai robuste, mai economice, cu un timp cât mai mare de viață, rezistente la condițiile mediului și la schimbările permanente ale topologiei. Afirmațiile de mai sus se bazează pe faptul ca în momentul de față există o implicare intensă în cercetarea rețelelor de senzori, care aduc imense beneficii și totodată provocări.

Tot mai multe aplicații de detecție, monitorizare și control devin conectate la Internet, iar aceste comunicări trebuie să fie fiabile și sigure. Securitatea ocupă un loc foarte important în majoritatea aplicațiilor cu rețele de senzori wireless, de exemplu managementul dezastrelor, sistemul medical la domiciliu, aplicații de securizare a locuințelor sau a aplicațiilor implementate în medii ostile. Majoritatea atacurilor asupra securității în WSN sunt cauzate de inserarea informațiilor false de către nodurile compromise din interiorul rețelei. Pentru prevenirea includerii de rapoarte false de către un nod compromis, o metodă (schemă) este necesară pentru detectarea acestor rapoarte false. Dezvoltând un astfel de mecanism de detectare și implementându-l eficient este o adevărată provocare. În plus, există numeroase atacuri proiectate să exploateze canalele de comunicație nesigure și operațiunile nesupravegheate ale rețelelor de senzori wireless. Mai mult, datorită caracteristicii inerente de nesupraveghere a rețelelor de senzori wireless, se consideră că atacurile fizice asupra senzorilor joacă un rol important în operațiile cu rețele de senzori wireless.

Majoritatea schemelor de securitate propuse în ziua de azi se bazează pe modele de rețea specifice. Deși există o lipsă a unui model combinat care să asigure securitatea la fiecare nivel al rețelei, în viitor mecanismele de securitate vor deveni bine stabilite pe fiecare nivel, iar combinarea mecanismelor pentru a le face să lucreze în colaborare va atrage provocări științifice importante. Aplicațiile de rețele de senzori wireless reale au nevoie de un anumit grad de încredere în măsură să mențină o funcționalitate corectă.

Datorită creșterii rapide a cercetării în materie de creștere a performanțelor, eficiență energetică și așa mai departe, securitatea în WSNs poate deveni mai degrabă o opțiune decât o provocare. Studiile efectuate în evaluarea rețelelor WSN sub influența mecanismelor de securitate arată că aceasta este posibilă, cu limitările prezente ale WSNs, și contribuie la definirea noilor mecanisme care să permită integrarea în siguranță a rețelelor WSN în Internet. Se consideră că implementarea și validarea prin simulări a metodelor de securitate propuse pe diferite tipuri de rețele, conduc la crearea unui set de soluții pentru asigurarea securității transmiterii datelor între nodurile rețelei și îndeplinirea cerințelor de securitate dintr-o rețea specifică de senzori wireless.

Evident, există numeroase provocări când vine vorba de integrarea IPv6 în WSNs, care rezultă din diferențele structurilor generale ale rețelelor IEEE802.15.4 și IPv6. Aceste avantaje introduc, de asemenea, noi vulnerabilități de securitate și expun implementările existente la diverse tipuri de atacuri. O anumită entitate din Internet poate transmite informații rău intenționate sistemului, prin urmare să declanșeze acțiuni incorecte.

Sistemul de operare Contiki OS a fost ales pentru analiza și testarea aplicațiilor WSN dezvoltate din diferite motive. Acesta este deosebit de flexibil, ușor de implementat și furnizează puternice comunicații Internet de joasă putere. De asemenea, oferă suport pentru cele mai recente standarde wireless de joasă putere: 6LowPAN, RPL, CoAP. Realizarea unei aplicații în Contiki este descrisă în Anexa A1.

În cadrul tezei s-au analizat constrângerile de securitate și comunicații ale rețelelor WSN bazate pe IPv6, utilizând un set de instrumente software adecvate care facilitează sarcina proiectantului de WSNs de a alege dintr-o gamă largă de algoritmi, protocoale, și platforme disponibile. Astfel, prin intermediul mediului de simulare Contiki/Cooja, s-a proiectat o rețea tipică WSN de noduri distribuite, interconectate prin comunicații wireless IPv6, peste care s-a pus în aplicare un mecanism de securitate adaptat – ContikiSec. Datele din rețea s-au colectat și investigat, iar rezultatele obținute furnizează o soluție viabilă pentru rețele WSN de mici dimensiuni, cu cost scăzut, și cu limitări în ceea ce privesc capacitățile operaționale și de calcul. S-a demonstrat că soluția propusă este adecvată rețelelor WSN ale căror aplicații nu sunt critice sau nu presupun cerințe sporite (ca de ex., mobilitate, funcționare în timp real, consum mare de energie). De asemenea, s-a constatat că soluția propusă nu satisface toate cerințele de securitate, impuse prin folosirea comunicațiilor IPv6 în WSN. Rezultatele furnizate oferă o bază solidă pentru dezvoltarea în continuare de noi algoritmi și protocoale pentru implementări robuste WSN.

Pe baza analizei realizate anterior privind constrângerile de securitate ale rețelelor WSN bazate pe IPv6, se pot dezvolta în continuare noi algoritmi și protocoale care să satisfacă toate cerințele de securitate impuse de aplicațiile WSN cu resurse limitate, cu cost mic și de dimensiuni reduse. Se obține astfel nevoia de analiză și validare experimentală a soluțiilor de securitate de nivel înalt și protecția comunicațiilor end-to-end în contextul accesării rețelei WSN direct din Internet. Plecând de la această idee, a fost realizat un al doilea studiu de caz ce descrie și evaluează introducerea unui substrat de securitate în stiva 6LoWPAN și propune două mecanisme noi aplicabile aplicațiilor Contiki pentru medii 6LoWPAN. În acest studiu de caz, sunt subliniate vulnerabilitățile stivei 6LoWPAN și necesitatea introducerii unui substrat de securitate la nivelul legăturii de date (LLSEC). Alegerea acestui nivel este motivată de faptul că majoritatea mecanismelor de securitate de nivel înalt introduc complexitate și nu protejează împotriva tuturor tipurilor de atacuri cunoscute în rețele WSN. Substratul de securitate IEEE802.15.4 acționează ca un filtru pentru atacurile destinate protocoalelor de nivel înalt.

În cadrul aceste lucrări au fost selectate două soluții moderne de securitate aplicabile rețelelor cu resurse limitate, și anume APKES și EBEAP. Acestea se remarcă prin faptul că sunt eficiente-energetic și rezistente la atacuri DoS. În primul rând, se prezintă un mecanism adaptabil pentru managementul cheilor, și un protocol de autentificare și criptare a mesajelor de tip broadcast în cazul rețelelor 6LoWPAN. Aceste mecanisme au fost implementate în Contiki și testate pe diferite tipuri de topologii de rețele WSN, fără sau în prezența unor noduri compromise. Rezultatele obținute arată că soluțiile propuse sunt eficiente, aceste fiind capabile să protejeze rețeaua de atacuri venite din interior sau din exteriorul acesteia, și să asigure cerințele securității cum ar fi autentificarea, criptarea mesajelor unicast și broadcast, și non-repudierea. De asemenea, s-a demonstrat că impactul mecanismelor de securitate propuse asupra resurselor limitate ale rețelei, este foarte mic.

Introducerea securității în substratul legăturii de date prezintă o importanță deosebită. Datorită utilizării unui mediu wireless, atacatorii pot injecta și reda cadre 802.15.4. În cazul în care substratul de securitate IEEE802.15.4 nu le filtrează, astfel de atacuri pot avea consecințe grave. Pe nivelul de adaptare, atacatorii pot lansa atacuri de fragmentare, care distrug pachetele IPv6 parțial reasamblate sau memoria cache. La nivelul rețea, un atacator poate lansa atacuri DoS pe bază de cale (PDoS). Într-un atac PDoS, un atacator injectează pachete IPv6 fictive, care sunt dirijate prin intermediul rețelei 6LoWPAN, epuizând astfel bateria.

Substratul LLSEC propus protejează împotriva tuturor atacurilor cunoscute și este, așadar, mai eficient. În afară de asta, APKES previne nodurile neautorizate să se alăture unei rețele 6LoWPAN.

În Capitolul 4 se cercetează domeniul monitorizării și controlului industrial cu ajutorul rețelelor de senzori wireless, prin utilizarea mediului de operare Contiki si a comunicațiilor 6LoWPAN / IPv6 peste mediile IEEE802.15.4. Utilizarea aplicațiilor WSN în mediile industriale este motivată de următoarele beneficii: productivitate, eficiență energetică și protecție. Aplicațiile din acest domeniu se așteaptă să vizeze procese de monitorizare și control, supravegherea mașinilor, urmărirea activelor și monitorizarea stocului, printre altele. Utilizarea de comunicații de date sigure și limitate dintre dispozitivele IWSN va fi de importanță fundamentală în implementările critice în care aplicațiile wireless trebuie să înlocuiască dispozitivele cu fir existente. Pe de altă parte, multe din aceste aplicații pot beneficia de disponibilitatea comunicațiilor prin Internet sau dispozitive backend. Per ansamblu, proiectarea noilor mecanisme pentru comunicații wireless IWSN necesită eforturi atât din punct de vedere al securității cât și al serviciului calității.

În cadrul tezei, s-a propus un model de securitate în contextul IWSNs cu scopul de a studia integrarea lor în aplicații industriale. Aplicabilitatea în domeniul industrial este bazată pe un număr de provocări de securitate derivate asociate cu acest tip de aplicații. Modelul propus este flexibil, configurabil, și are potențialul de a se adapta la provocările de monitorizare și control wireless în medii industriale. Extensiile de securitate sunt definite luând în considerare provocările, caracteristicile și principiile de proiectare ale unui IWSN. La proiectarea de noi algoritmi, protocoale și arhitecturi de comunicare pentru IWSNs, o analiză corespunzătoare cu privire la performanțele, consumul de energie și interoperabilitatea trebuie să fie făcută. Utilizarea extensiilor de securitate în ceea ce privește performanța rețelei și cerințele de calcul se pot valida prin măsurători obținute experimental. Se consideră că această propunere oferă o contribuție validă spre adaptarea de măsuri de securitate într-un context IWSN 6LoWPAN. Din punct de vedere industrial, avantajele folosirii 6LoWPAN sunt: abilitatea de a comunica direct cu alte dispozitive IP la nivel local sau prin rețeaua IP (de ex., Internet, Ethernet), arhitecturi existente și de securitate, model de date la nivel de aplicație stabilit și servicii (de ex., HTTP , HTML, XML), instrumente de management al rețelei stabilite, protocoale de transport, precum și suport pentru o opțiune IP în majoritatea standardelor wireless industriale.

Integrarea rețelelor de senzori wireless în Internet contribuie de asemenea la o evoluție majoră a Internet-of-Things. IoT materializează o viziune a unui viitor Internet în care orice obiect cu capacități computaționale și senzoriale este capabil să comunice cu orice alt dispozitiv asemănător folosind protocoale de comunicații Internet. Multe din aceste aplicații sunt de așteptat să implice o cantitate mare de dispozitive de detectare și acționare, în consecință costul acestora este un factor important. Pe de altă parte, restricțiile de cost dictează constrângeri în ceea ce privește resursele disponibile în platformele senzoriale, cum ar fi memoria și puterea de calcul, în timp ce implementarea în mod nesupravegheat a multor dispozitive va necesita, de asemenea, utilizarea de baterii pentru stocarea energiei. În această viziune, aplicațiile WSN devin din ce în ce mai mult parte integrantă din aplicațiile IoT. Trecerea la IPv6 se realizează relativ ușor, ceea ce înseamnă că și aplicațiile WSN existente pot face parte din viitoare proiecte IoT de mare anvergură. În Capitolul 5 s-au definit și prezentat rolul rețelelor de senzori wireless în contextul IoT, punându-se accentul pe cerințele de securitate prezente în cazul aplicațiilor IoT. S-a analizat în principal problema confidențialității în aplicațiile ce implică accesarea din Internet, mai exact intimitatea utilizatorilor ce sunt implicați în tranzacții de date importante (și nu numai) între dispozitive aflate la distanță. Se pune accentul pe confidențialitatea datelor și a utilizatorilor într-un context Human-in-the-Loop Cyber-Physical System (HiTLCPS), o paradigmă în care

utilizatorul este parte integrantă din bucla de control, iar acțiunile sale afectează ieșirile sistemului.

În ultima parte s-a sugerat un model general care sprijină confidențialitatea în HiTLCPS și care a fost implementat pe HappyStudent, o aplicație care are o abordare BCI și urmează o paradigmă „student-centric-sensing" pentru a deduce și afecta pozitiv emoțiile unui student. Aplicația poate fi utilizată cu scopul de a îmbunătăți starea de spirit a studenților și nu numai, de a interacționa mai mult social și chiar performanțe mai bune la învățare și sarcini de lucru.

Folosind senzorii de la smartphone-uri pentru a monitoriza oameni, nu numai că ajută în furnizarea de feedback eficient pentru a ajuta utilizatorii în corectarea comportamentului lor, dar ajută de asemenea oamenii de știință în cercetarea comportamentală. Implementarea de HiTLCPS prezentată servește, de asemenea, ca o dovadă a conceptului de avantajele integrării diferitelor mecanisme de protecție a confidențialității.

Acest studiu a fost realizat în cadrul stagiului de cercetare realizat de autor, la Departamentul de Inginerie Informatică al Univerității din Coimbra[1], Portugalia. Parteneriatul s-a concretizat prin publicarea unui articol științific la o conferință internațională [35].

Concluzia care poate fi desprinsă la sfârșitul acestei lucrări este că, pentru o gamă largă de aplicații, rețelele WSN constituie soluții eficiente și performante în majoritatea domeniilor existente. Problematicile abordate în cadrul tezei (comunicații și securitate) sunt factori cheie care trebuie luați în considerare la proiectarea aplicațiilor cu rețele WSN în vederea asigurării unor performanțe ridicate. În viitor, datorită creșterii rapide a cercetării în materie de performanțe, eficiență energetică, minimizare a dispozitivelor electronice etc., securitatea în WSNs poate deveni mai degrabă o opțiune decât o provocare. Studiile efectuate în cadrul acestei lucrări arată că aceasta este posibilă, cu limitările prezente ale WSNs, și contribuie la definirea noilor mecanisme care să permită integrarea în siguranță a rețelelor WSN în Internet.

Problemele prezentate, precum și rezultatele obținute, conferă lucrării un real caracter de aplicabilitate practică, deschizând noi perspective cercetărilor în domeniul abordat.

Rezultatele furnizate oferă o bază solidă pentru dezvoltarea în continuare de noi algoritmi și protocoale pentru implementări robuste WSN în lumea reală. În principal, acest tip de abordare reduce în mod semnificativ timpul de dezvoltare și elimină eventuale erori, prevenind remedieri costisitoare și, uneori, inaccesibile pentru aplicații critice sau la distanță, în timp ce se construiește încredere în rândul viitorilor utilizatori ai tehnologiei de rețea încorporate.

C 2. CONTRIBUȚII PERSONALE

Pornind de la obiectivele declarate ale acestei lucrări, în continuare sunt prezentate principalele contribuții originale:

- Elaborarea unei sinteze asupra stadiului actual al domeniului rețelelor de senzori wireless, în ceea ce privește standardele existente, sistemele de operare și platformele hardware dedicate, și selectarea unor aplicații recente semnificative cu rețele WSN.
- Elaborarea unui studiu și a unor analize asupra unor problematici de bază vizând securitatea rețelelor se senzori wireless, utilizând tehnici de securitate existente.
- Elaborarea unui studiu comparativ al arhitecturilor de securitate recente, propuse pentru WSN, și identificarea constrângerilor legate de implementarea acestora în rețele wireless bazate pe IPv6.

[1] www.dei.uc.pt/

- Implementarea și validarea experimentală prin simulări, a algoritmului de securitate ContikiSec, utilizând o rețea de senzori Tmote Sky.
- Analiza calitativă și cantitativă a diferitelor structuri de rețele de senzori wireless, utilizând algoritmul ContikiSec.
- Elaborarea, implementarea și validarea unui program pentru măsurarea consumului de energie al rețelelor de senzori simulate.
- Elaborarea, implementarea și validarea unui program pentru simularea calitativă și cantitativă a securității rețelelor de senzori.
- Elaborarea unui studiu și a unor analize asupra vulnerabilităților stivei 6LoWPAN și necesitatea introducerii unui substrat de securitate la nivelul legăturii de date.
- Implementarea și validarea experimentală prin simulări, a unui substrat de securitate în stiva 6LoWPAN, împreună cu două mecanisme de securitate noi, aplicabile aplicațiilor Contiki pentru medii IEEE802.15.4.
- Definirea unor scenarii de atac și validarea rezilienței algoritmilor propuși.
- Analiza și validarea experimentală a soluțiilor de securitate de nivel înalt și de protecție a comunicațiilor end-to-end în contextul accesării rețelei de senzori wireless direct din Internet.
- Elaborarea unui studiu asupra cerințelor de securitate și a constrângerilor de bază în cazul implementării unei rețele de senzori wireless într-un mediu industrial.
- Particularizarea uneia din structurile propuse de securitate în cadrul unei rețele de senzori wireless industriale și validarea experimentală prin simulări cu diverse scenarii.
- Elaborarea unui studiu asupra tehnologiilor si protocoalelor specifice Internet-of-Things, precum și problematica securității în IoT.
- Sinteza și validarea unui model de asigurare a confidențialității datelor și intimitate a utilizatorilor unui sistem "Human-in-the-loop Cyber-Physical Systems" (HiTLCPS), prin implementarea unei aplicații mobile bazate pe HiTLCPS.

C 3. PERSPECTIVE DE DEZVOLTARE ULTERIOARĂ

Dintre principalele direcții de dezvoltare ulterioară care pot continua rezultatele obținute în cadrul acestei teze se pot enumera:

- Minimizarea și/sau optimizarea mecanismelor propuse de securizare a datelor din interiorul unei rețele WSN bazate pe IPv6. Definirea de noi mecanisme care să permită integrarea în siguranță a WSNs bazate pe IPv6 în Internet, respectiv în aplicații IoT.
- Dezvoltările de aplicații în Contiki au permis o familiarizare cu instrumentele hardware și software dedicate, ceea ce oferă o bază solidă pentru dezvoltări viitoare de noi algoritmi și protocoale, pentru implementări robuste WSN în lumea reală. De asemenea, se dorește aducerea de contribuții proiectului open-source Contiki prin adăugarea platformei IRIS[1] listei de platforme hardware WSN suportate.
- Contribuții la securizarea aplicațiilor Contiki se pot aduce prin implementarea de noi mecanisme de distribuție a cheilor aplicabile mecanismului APKES studiat.

[1] http://www.memsic.com/userfiles/files/Datasheets/WSN/IRIS_Datasheet.pdf

ANEXE

A1. CREAREA UNEI APLICAȚII ÎN CONTIKI OS

Se prezintă modul de instalare și configurare a mediului de dezvoltare Contiki, împreună cu realizarea unei aplicații specifice de rețea. Se explică modul în care se execută Contiki pe hardware.

A2. COLECTAREA DATELOR DINTR-O REȚEA WSN PRIN INTERNET

Se prezintă o aplicație de rețea 6LoWPAN, care generează date senzoriale și permite accesul la cele mai noi date printr-un webserver integrat. Datele din rețea sunt accesate prin HTTP dintr-un web browser. De asemenea, sunt prezentate programele pentru măsurarea consumului de energie și pentru pornirea/oprirea radioului.

A3. CONFIGURAREA PARAMETRILOR DE SECURITATE PENTRU COMUNICAȚII INTER-WSN ÎN CONTIKI

Configurarea diverșilor parametri de rețea necesari unei aplicații în Contiki se realizează prin crearea unui fișier de configurare în același director în care rezidă aplicația. Sunt prezentate fișierele de configurație pentru aplicarea mecanismelor de securitate sugerate în teză.

BIBLIOGRAFIE

[1] W. Dargie și C. Poellabauer, *Fundamentals of Wireless Sensor Networks*. Chichester, UK: John Wiley & Sons, Ltd, 2010.

[2] J. Solobera, „Detecting Forest Fires using Wireless Sensor Networks”, 2010. [Online]. Valabil la: http://www.libelium.com/wireless_sensor_networks_to_detec_forest_fires/.

[3] J. Sen, „A Survey on Wireless Sensor Network Security”, *Computer Networks*, vol. 52, nr. 12, p. 24, 2010.

[4] Y. Wang și M. Qin, „Security for Wireless Sensor Networks”, pp. 844-848, 2010.

[5] E. Cayirci și C. Rong, *Security in wireless ad hoc and sensor networks*. John Wiley & Sons, Ltd, 2009.

[6] M. V. Ramesh, A. B. Raj, și T. Hemalatha, „Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks”, *2012 Fourth International Conference on Computational Intelligence and Communication Networks*, pp. 783-787, nov. 2012.

[7] D. E. Burgner și L. a. Wahsheh, „Security of Wireless Sensor Networks”, *2011 Eighth International Conference on Information Technology: New Generations*, pp. 315-320, apr. 2011.

[8] C.-T. Li, „Security of wireless sensor networks: current status and key issues”, în *Smart Wireless Sensor Networks*, 2010, pp. 299-313.

[9] N. Kushalnagar, G. Montenegro, și C. P. P. Schumacher, „IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem statement, and Goals”, 2007.

[10] J. Hui și P. Thubert, „Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks”, *RFC 6282*, nr. Sept., 2011.

[11] E. Kim și D. Kaspar, „Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, *RFC 6568*, nr. April, 2012.

[12] C. Gomez, E. Kim, D. Kaspar, și C. Bormann, „Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing”, *RFC 6606*, nr. May, 2012.

[13] S. Chakrabarti, Z. Shelby, și E. Nordmark, „Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, *RFC 6775*, nr. Nov., 2012.

[14] C. Bormann, A. P. Castellani, și Z. Shelby, „CoAP: An application protocol for billions of tiny Internet nodes”, *IEEE Internet Computing*, vol. 16, nr. 2, pp. 62-67, 2012.

[15] Z. Shelby și C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, Ltd, 2009.

[16] M. Durvy, J. Abeillé, P. Wetterwald, C. O’Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne, și A. Dunkels, „Making sensor networks IPv6 ready”, *Proceedings of the 6th ACM conference on Embedded network sensor systems - SenSys ’08*, p. 421, 2008.

[17] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, și R. Alexander, „RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”, 2012.

[18] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, și K. Wehrle, „6LoWPAN fragmentation attacks and mitigation mechanisms”, în *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec ’13*, 2013, p. 55.

[19] L. Casado și P. Tsigas, „Contikisec: A secure network layer for wireless sensor networks under the contiki operating system”, în *Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age*, 2009, pp. 133-147.

[20] I. Halcu, G. Stamatescu, I. Stamatescu, și V. Sgarciu, „An analysis of security and communication constraints of IPv6-based Sensor Networks”, în *Proceedings of the 2014 6th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2014, pp. 55-60.

[21] I. Halcu, G. Stamatescu, și V. Sgarciu, „IPv6 Sensor Networks Modeling for Security and Communication Evaluation”, în *Systems, Decision and Control*, Springer, 2016, p. (accepted).

[22] ***, „Tmote Sky Datasheet.” [Online]. Valabil la: www.eecs.harvard.edu/.../tmote-sky-datasheet.pdf. [Data accesării: 01-mar-2015].

[23] K.-F. Krentz, H. Rafiee, și C. Meinel, „6LoWPAN security: Adding Compromise Resilience to the 802.15.4 Security Sublayer”, *Proceedings of the International Workshop on Adaptive Security - ASPI ’13*, pp. 1-10, 2013.

[24] I. Halcu, G. Stamatescu, și V. Sgarciu, „Enabling security on 6LoWPAN / IPv6 Wireless Sensor Networks”, în *2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2015, p. SSS-29-SSS-32.

[25] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, și T. Voigt, „Secure communication for the Internet of Things-a comparison of link-layer security and IPsec for 6LoWPAN”, *Security and Communication Networks*, vol. 7, nr. 12, pp. 2654-2668, dec. 2014.

[26] V. C. Güngör și G. P. Hancke, Ed., *Industrial Wireless Sensor Networks: Applications, Protocols and Standards*, Industrial. USA: CRC Press, 2013.

[27] V. C. Gungor și G. P. Hancke, „Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches”, *IEEE Transactions on Industrial Electronics*, vol. 56, nr. 10, 2009.

[28] I. Halcu, G. Stamatescu, și V. Sgarciu, „A Security Framework for a 6LoWPAN based Industrial Wireless Sensor Networks”, *UPB Scientific Bulletin*, nr. Series C Electrical Engineering and Computer Science, p. (accepted).

[29] A. Dunkels, N. Eriksson, F. Österlind, și N. Tsiftes, „The Contiki OS - The Operating System for the Internet of Things.” [Online]. Valabil la: http://www.contiki-os.org/.

[30] A. Dunkels, J. Eriksson, N. Finne, și N. Tsiftes, „Powertrace : Network-level Power Profiling for Low-power Wireless Networks Low-power Wireless”, *SICS Technical Report T2011:05*. Swedish Institute of Computer Science, 2011.

[31] D. Nunes, D. Raposo, D. Silva, P. Carmona, și J. S. Silva, „Achieving Human-Aware Seamless Handoff”, în *2015 International Conference on Distributed Computing in Sensor Systems*, 2015, pp. 254-259.

[32] D. Nunes, P. Carmona, P. Zhang, și J. Sá Silva, „Human-in-the-Loop management of networking in smartphones”, în *16th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2015), Boston, USA, Jun. 2015, (submitted).*

[33] S. B. Wicker și D. E. Schrader, „Privacy-aware design principles for information networks”, *Proceedings of the IEEE*, vol. 99, pp. 330-350, 2011.

[34] V. Sandulescu și I. Halcu, „Speaker Authentication for an Assistive Domotic System”, în *2015 20th International Conference on Control Systems and Computer Science*, 2015, pp. 337-340.

[35] I. Halcu, D. Nunes, V. Sgarciu, și J. Sa Silva, „New Mechanisms for Privacy in Human-in-the-loop Cyber-Physical Systems”, în *8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 2015, pp. 418-423.

[36] P. Carmona, D. Nunes, D. Silva, C. Raposo, C. Herrera, și J. Sá Silva, „Happy Hour - Improving Mood With An Emotionally Aware Application”, în *15th International Conference on Innovations for Community Services (I4CS)*.

LISTA DE LUCRĂRI PUBLICATE ÎN DOMENIUL TEZEI

1. Articole publicate în volumele unor manifestări științifice internaționale, cotate ISI sau BDI

[1] ***Halcu, I.***, *Nunes, D., Sgarciu, V., Sa Silva, J.*, "New Mechanisms for Privacy in Human-in-the-loop Cyber-Physical Systems", 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Sept. 24-26, 2015, Warsaw, Poland, 2015, pp. 418-423. [IEEExplore, ISI Proceedings]

[2] ***Halcu, I.***, *Stamatescu, G., Sgarciu, V.*, "Enabling Security on 6LoWPAN / IPv6 Wireless Sensor Networks", Proceedings of the 7th Electronics, Computers and Artificial Intelligence Conference, IWSSS Workshop, vol.7, no.2, Bucharest, June 25-27, 2015. [IEEExplore, ISI Proceedings]

[3] *Sandulescu, V.*, ***Halcu, I.***, "Speaker Authentication for an Assistive Domotic System", 20th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, May 2015, pp. 337-340. [IEEExplore, ISI Proceedings]

[4] ***Halcu, I.***, *Stamatescu, G., Stamatescu, I., Sgarciu, V.*, "An Analysis of Security and Communication Constraints of IPv6-based Sensor Networks", Proceedings of the 6th Electronics, Computers and Artificial Intelligence Conference, IWSSS Workshop, vol.6, no.6, Bucharest, Romania, October 23-25, 2014, pp. 73-78. [IEEExplore, ISI Proceedings]

2. Articole publicate în volumele unor reviste sau jurnale, cotate ISI sau BDI

[5] ***Halcu, I.***, *Stamatescu, G., Sgarciu, V.*, "A Security Framework for a 6LoWPAN based Industrial Wireless Sensor Networks", UPB Scientific Bulletin, Series C Electrical Engineering and Computer Science. (în curs de publicare)

3. Cărți/ Capitole de carte

[6] ***Halcu, I.***, *Stamatescu, G., Sgarciu, V.*, "IPv6 Sensor Networks Modeling for Security and Communication Evaluation", Recent Advances in Systems, Safety and Security, Springer series – "Systems, Decision and Control". (în curs de publicare)

LISTA DE LUCRĂRI PUBLICATE (EXCEPTÂND CELE DIN DOMENIUL TEZEI)

1. Articole publicate în volumele unor manifestări științifice internaţionale, cotate ISI sau BDI

[1] *Marinescu, M., Ciubancan, M., Dulea, M., Grigoriu, O.,* ***Halcu, I.****, et al.* "Software system for inventory and assessment of the wear of computing machines from a network of grid data centers", Proceedings of the 13th RoEduNet Conference: Networking in Education and Research Joint Event RENAM 8th Conference, Chișinău, Moldova, Sept. 2014. [IEEExplore]

[2] *Rusu, O.,* ***Halcu, I.****, Grigoriu, O., Neculoiu, G., Săndulescu, V., Marinescu, M., Marinescu, V.,* "Converting unstructured and semi-structured data into knowledge", Proceedings of the 11th RoEduNet International Conference – Networking in Education and Research, Sinaia, Romania, Jan. 16-19, 2013, pag. 85-88. [IEEExplore, ISI Proceedings]

[3] *Gârlașu, D., Săndulescu, V.,* ***Halcu, I.****, Neculoiu, G., Grigoriu, O., Marinescu, M., Marinescu, V.,* "A Big Data implementation based on Grid Computing", Proceedings of the 11th RoEduNet International Conference – Networking in Education and Research, Sinaia, Romania, Jan. 16-19, 2013, pag. 62-65. [IEEExplore, ISI Proceedings]

[4] *Ciubancan, M., Neculoiu, G., Grigoriu, O.,* ***Halcu, I.****, Săndulescu, V., Marinescu, M., Marinescu, V.,* Data Mining processing using GRID technologies, Proceedings of the 11th RoEduNet International Conference – Networking in Education and Research, Jan. 16-19, Sinaia, 2013, pag. 89-91. [IEEExplore, ISI Proceedings]

[5] *Bărbulescu, M., Grigoriu, O., Neculoiu, G., Halcu, I., Săndulescu, V., Marinescu, M., Marinescu, V.,* Integrating structured, semi-structured and unstructured data in natural and built environmental engineering, Proceedings of the 11th RoEduNet International Conference – Networking in Education and Research, Jan. 16-19, Sinaia, 2013, pag. 92-95. [IEEExplore, ISI Proceedings]

[6] *M. Barbulescu, M. Marinescu, V. Marinescu, O. Grigoriu, G. Neculoiu, V. Sandulescu,* ***I. Halcu***, "GNU GPL in studying programs from the systems engineering field", Proceedings of the 10th RoEduNet International Conference, Iași, Romania, June 23-25, 2011, pag. 215-218. [IEEExplore]

[7] *M. Ciubancan, M. Marinescu, V. Marinescu, O. Grigoriu, G. Neculoiu, V. Sandulescu,* ***I. Halcu***, "Computer aided learning with GRID technologies", Proceedings of the 10th RoEduNet International Conference, Iași, Romania, June 23-25, 2011, pag. 219-221. [IEEExplore]

2. Volume ale unor manifestări științifice naţionale

[8] *Niculescu-Faida O., Grigoriu O.,* ***Halcu I.****, Neculoiu G., Săndulescu V., Marinescu M., Marinescu V.,* "Big data and data mining collections in analogy with the data that measure status indicators of environmental factors", Proceedings of the 19th National Conference - Progress In Cryogenics And Isotopes Separation, Călimăneşti-Căciulata, Romania, Oct. 10-11, 2013, pg. 93-97, ISBN 978-973-750-249-0.

[9] *Grigoriu O.,* ***Halcu I.****, Sandulescu V., Neculoiu G., Marinescu M., Marinescu V.,* "Education for sustainable development", Proceedings of the 18th Conference – Progress in Cryogenics and Isotopes Separation, Călimăneşti-Căciulata, Romania, Oct. 25-26, 2012, ISBN: 978-973-750-228-5.