Universitatea *POLITEHNICA* din București

Facultatea de Automatică și Calculatoare, Departamentul de Calculatoare

Teză de Doctorat

în Calculatoare și Tehnologia Informației

Security in Wireless Networks

Securitatea rețelelor mobile

Autor

Drd.ing. Alexandra-Elena MOCANU (MIHĂIȚĂ)

Coordonator

Prof.dr.ing. Florin POP

2020

București, România

Contents

List of Figures

List of Tables

1 | Introducere

1.1 Definirea problemei de cercetare și obiectivele tezei

Începând de la realizarea cu succes a primei conexiuni client-server, realizată de Sir Timothy John Berners-Lee în 1989, Internetul a evoluat cu rapiditate ajungând la 4,57 miliarde de dispozitive interconectate. Potrivit website-ului Statistica [Cle20], această valoare impresionantă include mai mult de 59% din populația mondială. Traficul de Internet efectuat utilizând dispozitive mobile reprezintă mai mult de 50% din traficul global de Internet, indiferent de multiplele tipuri de conexiuni fără fir, precum 2G, 3G, 4G, 5G, WiFi, Bluethooth, *etc*.

Creșterea substanțială a numărului de utilizatori, modificarea perpetuă a topologiei rețelelor și eterogenitatea dispozitivelor reprezintă principalele provocări pentru obținerea dezideratului de securitate în cadrul rețelelor mobile. Contracararea atacurilor precum Sybil [JZE+19], clonarea nodului [NSK+20], spoofing [GNF+20], interzicerea somnului [FFBY20], lipsa de acces la servicii [PS20], *etc*, reprezintă un obiectiv fundamental în cercetarea rețelelor mobile fără fir.

În această teză de doctorat ne concentrăm atenția, pe cercetarea în domeniul rețelelor vehiculare, senzoriale și a celor cu participare benevolă, în special pe securizarea fiecărui tip de rețea menționat anterior. Astfel, analizăm în profuzime fiecare caz în parte cu particularitățile sale: pornind de la topologii diferite și mergând până la protocoale de comunicație între noduri diferite. Această diversitate a determinat abordări diferite privind securitatea rețelelor cu rezultate distincte, specifice fiecărui studiu de cza. Rezultatele obținute în această teze se bazează pe întrebările și obiectivele de cercetare stabilite în Tabelul 1.1 și care stau la baza cercetărilor nostre.

Pentru a găsi cele mai bune soluții, am încercat să răspundem la câteva întrebări de cercetare precum:

1. **Cum putem securiza o rețea mobilă fără fir fără a afecta performanțele sale în ceea ce privește calitatea serviciilor? (RQ1)**

   Răspunsul la această întrebare este abordat în fiecare capitol al acestei teze. Pentru a propune securitatea unei rețele mobile fără fir, trebuie să definim în mod corespunzător principalele atribute ale rețelei și să analizăm restricțiile acesteia. După aceea, trebuie să luăm în considerare caracteristicile tipului de comunicație fără fir utilizat, cum ar fi protocoalele de rază și propagare. Aceste specificații ajută la alegerea unui

model de securitate.

2. **Care este impactul asupra performanței în ceea ce privește calitatea serviciului la adăugarea unui modul de securitate bazat pe criptare în rețelele mobile fără fir? (RQ2)**

   Un modul de securitate bazat pe criptare pentru rețelele mobile fără fir este o provocare atât din cauza supraîncărcării în rețea, cât și a constrângerilor de timp existente. Această teză încearcă să demonstreze că se poate face adăugarea unui astfel de model de securitate, dar cu prețul comunicării pierdute sau incomplete între nodurile rețelei.

3. **Putem defini un model de încredere pentru VANET pentru a asigura securitatea utilizatorilor implicați în rețea? (RQ3)**

   Au fost deja propuse diferite modele pentru modelul de încredere și reputație în VANET. Modelul pe care l-am propus este unul dintre cele mai comune: bazat pe cheie publică, folosind standardul de certificare .X509 pentru autentificarea utilizatorilor și dispozitive de monitorizare pentru a determina comportamentul bun sau rău al nodurilor din rețea. Eficiența modelului a fost testată prin simulare utilizând un simulator UPB VANET.

4. **Cum influențează diferitele scenarii ale rețelelor mobile fără fir definirea unui model de încredere și reputație? (RQ4)** Pentru a găsi răspunsul la această întrebare, am analizat mai multe rețele mobile fără fir și am propus diferite modele de securitate. Aceste modele au încercat să răspundă necesităților VANET, rețelelor de senzori fără fir și detectării participative.

5. **Ar trebui ca aspectul fără fir al comunicației în rețelele mobile fără fir să fie tratat ca o parte integrată a rețelei sau ar trebui abordat separat? (RQ5)**

   Când am studiat diferitele tipuri de rețele mobile fără fir și am propus diferite modele de securitate, am observat importanța aspectului wireless al rețelelor. Prin urmare, am propus un model pentru tratarea aspectului wireless separat și un alt model care îl consideră o parte a comportamentului nodului. Rezultatele acestei comparații sunt prezentate în continuare în teză.

Prin urmare, obiectivul principal al acestei teze de doctorat este cercetarea, dezvoltarea și evaluarea unui nou model de securitate pentru rețelele mobile fără fir.

Am identificat trei scenarii care pot beneficia de pe urma cercetării și soluțiilor noastre:

- rețele vehiculare ad-hoc,
- rețele fără fir pentru senzori,
- participatory sensing.

1.2 Prezentarea generală a tezei de doctorat

Această teză de doctorat abordează subiectul rețelelor mobile fără fir, aplicațiile acestora și cercetează modele noi și inovatoare pentru securizarea acestora în funcție de studiul de caz abordat. În capitolul 2 prezentăm principalele atribute și tehnologii care fac posibilă existența rețelelor mobile fără fir, împreună cu principalele protocoale de rutare precum și o serie atacuri cunoscute. În capitolul 3 descriem în detaliu atacurile existente și daunele acestora în cadrul rețelelor fără fir. De asemenea, am efectuat o serie de implementări comparative ale mai multor algoritmi criptografici simetrici. Implementările menționate au fost efectuare aât generic cât și în cazul real al rețelele mobile fără fir. Aceste experimente au arătat că performanțele algoritmilor criptografici depind în mare măsură de mediul în care sunt realizate. În capitolul 4 ne concentrăm atenția pe tipul special de rețele mobile fără fir numite rețele ad-hoc vehiculare. În capitolul 5 ne concentrăm un alt tip de rețea mobilă fără fir numită participatory sensing. Acest studiu de caz vizează reintegrarea vârstnicilor și, iar pe baza lui propunem un model de securitate în mai multe etape testat și evaluat stochastic. În capitolul 6 propunând o abordare generală bazată pe lanțuti Markov pentru securitate atît la nivel utilizator cât și la nivel legătură. În capitolul 7 prezentăm principalele concluzii ale cercetării care stă la baza acestei teze de doctorat. De asemenea scoatem în evidență avantajele și neajunsurile ale fiecărei abordări de securitate propuse.

Această teză de doctorat a fost bine documentată și ancorată în realitatea științifică actuală, fapt dovedit prin faptul că am utilizat 177 de referințele bibliografice relevante.

Întrebare de cercetare	Obiectiv de cercetare	Metodologie de cercetare	Caz de utilizare
RQ1	Pentru a sublinia importanța atributelor principale ale rețelelor mobile wireless, cum ar fi topologia în continuă schimbare, timpul limitat pentru interacțiuni și capacitățile limitate ale resurselor și faptul că fiecare adăugare la structura rețelei se reflectă în calitatea serviciului.	Dovedit stocastic și prin simulări	Răspunsul adecvat la această întrebare este în întregime această teză, accentul principal al cercetării noastre fiind asigurarea VANET, PS și WSN. Fiecare dintre modelele de securitate propuse în această teză a obținut unele proprietăți de securitate la un cost al performanței rețelelor în care a fost aplicat.
RQ2	Pentru a sublinia faptul că caracteristica unei metode de securitate și algoritmul utilizat variază foarte mult ca performanță în funcție de scenariul în care este aplicată.	Dovedit prin simulări	Pentru a răspunde la această întrebare, am implementat mai mulți algoritmi de criptare într-un mediu independent și apoi am implementat fiecare dintre acești algoritmi pentru criptarea mesajelor schimbate între utilizatori într-un VANET într-un mediu simulat. Timpul de criptare și decriptare a mesajelor între utilizatorii din VANET a determinat o scădere imensă a numărului total de pachete trimise în rețea. Detalii despre abordarea și rezultatele implementării sunt furnizate în capitolul 3 și în articolul [MDM+15].
RQ3	Pentru a sublinia importanța alegerii proprietăților de securitate pe care dorim să le acordăm. Dacă confidențialitatea este importantă, atunci un algoritm de criptare ar putea fi cea mai bună abordare, dar dacă autentificarea este obiectivul principal, atunci criptografia cu cheie publică ar putea face cel mai bine.	Dovedit stocastic și prin simulări	Răspunsul la această întrebare a implicat implementarea unui model de securitate complex pentru VANET care a vizat rezolvarea majorității atributelor de securitate, prin diferite metode, în detrimentul performanțelor rețelei. Mai multe detalii despre constrângerea crescută în rețea și performanțele acesteia după adăugarea unui model de securitate elaborat pot fi citite în capitolul 4 și în articolul [MDP+17b]
RQ4	Pentru a arăta corelația puternică dintre caracteristicile tipului de rețea mobilă fără fir și modelul de securitate bazat pe încredere și reputație ales.	Dovedit stochastic	Pentru a oferi un răspuns perspicace la această întrebare, am analizat diferite abordări și apoi am trecut la modele noi propuse pentru a aborda deficiența modelelor existente. Procedând astfel, am propus, implementat și testat diverse modele de încredere în mai multe scenarii, cum ar fi VANET, PS și WSN. Rezultatele acestor modele de securitate pot fi citite în continuare în capitolele 4, 5 și 6 și în articolul [MDP+17a]
RQ5	Pentru a arăta că încrederea în rețelele mobile fără fir poate fi văzută ca o acumulare de încredere bazată pe utilizatori și încredere bazată pe comunicare.	Dovedit stocastic și prin simulări	Pentru a aborda această întrebare, am propus un model de încredere exclusiv utilizatorului în detecția participativă ca parte a rețelelor mobile fără fir. Atunci am analizat variațiile de încredere ale utilizatorului atunci când au apărut probleme cu comunicarea. Aceste variații au condus la convingerea că încrederea în comunicare ar trebui abordată separat. Implementarea unui model de încredere bazat pe Markov pentru rețelele de senzori fără fir ca parte a rețelelor mobile fără fir a arătat importanța comunicării de încredere și a abordat deficiența abordării anterioare. Mai multe detalii pot fi citite în capitolele capitol 5 și 6 și în articolul [MPME20]

Table 1.1. Thesis objectives and methodology.

2 | Rețele mobile fără fir

În ultimul deceniu, comunicațiia wireless a trecut de la stadiul de noutate la standard. În zilele noastre, a nu fi conectat wireless la Internet sau a avea acces la alte dispozitive a devenit un lucru mai puțin întâlnit. Fie că este vorba de Bluetooth, WiFi, satelit sau 4G, 5G, cu toții ne dorim acces ușor la dispozitivele noastre și să putem controla totul de la distanță.

În acest capitol, prezentăm o analiză critică al tehnologiilor fără fir utilizate în rețelele mobile fără fir 2.1. Ulterior abordăm aspectele de securitate introduse de fiecare tip de comunicație fără fir 2.2. În secțiunea 2.3 prezentăm o serie de instrumente utilizate pentru validare prin simulare a condițiilor de comunicare fără fir în timp real în rețelele mobile fără fir. Rezultele acestor studii sunt prezentate în detaliu în secțiunea 2.4.

2.1 Tehnologii fără fir pentru comunicație pentru rețele mobile

În această secțiune motivăm importanța comunicației fără fir. Aceasta a fost standardizată pentru prima dată la nivel internațional în 1997 și de atunci a cunoscut o evoluție continuă.

Standardul inițial 802.11, considerat ieșit din uz, în zilele noastre prevedea două tipuri de rate de transfer 1 Mbps sau 2 Mbps folosind mediul de transmisie infraroșu și se bazează pe tehnologia spectrului împrăștiat. Ulterior, standardul a evoluat la versiunea 802.11a, care folosește frecvența de 5 GHz. Standardul 802.11b a permis obținerea unor rate de transfer de 11 Mbps folosind frecvența de 2.4 GHz. În continuare, standardul 802.11g a adus rate de transfer superioare, atingând teoretic viteza maximă de 54Mbps folosind aceesai frecvență de 2.4 GHz. Standardul 802.11n îmbunătățește substanțial ratele de transfer de la 54 Mbps până la 600Mbps folosind atât frecvențele de 2.4GHz și 5GHz. Tehnologia care a permis creșterea semnificativă a ratelor de transfer este MIMO (multiple input, multiple output), care presupune utilizarea mai multor antene pe dispozitivele utilizatorilor.

Revenind la actualitatea zilelor noastre, standardul 802.11ax cunoscut și sub numele de WiFi6 se află în faze incipiente ale utilizării. Acest standard utilizează o metodă inovativă pentru modularea semnalelor, metodă ce permite creșterea ratelor de transfer cu până la de 10 ori mai mult decât în cazul standardului 802.11n. În plus standardul

802.11ay, cunoscut și sub denumirea de NextGen, standard aflat în faze incipiente de utilizare, este considerat a fi primul standard real pentru comunicații fără fir folosind mmWave.

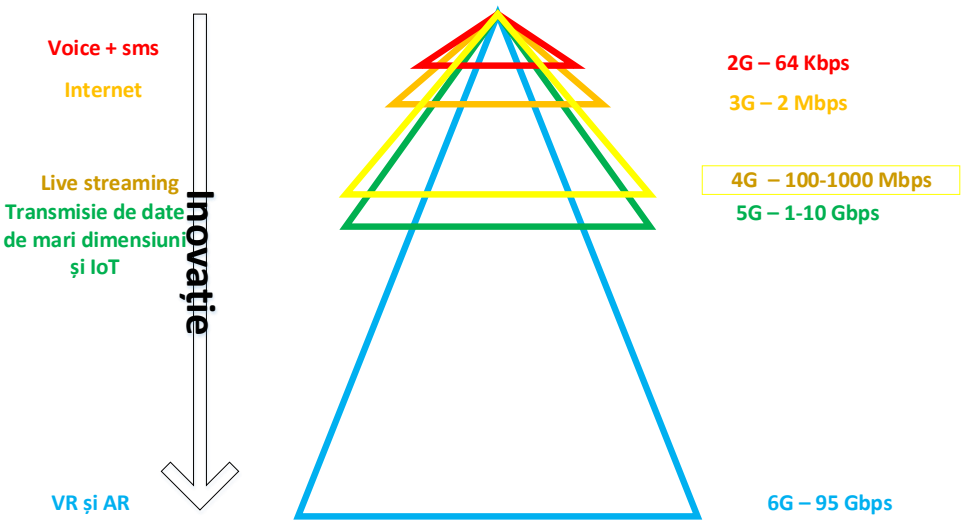

Figure 2.1. Comparație între versiunile standardului 802.11 privind frecvența și distanța de propogare.

În imaginea 2.1 observăm dependența inversă a frecvenței cu distanța de propagare a semnalului. Astfel, cu cât crește frecvența cu atât scade distanța de propagare. Avantajul fundamental a utilizării frecvențelor înalte este creșterea semnificativă a lățimi de banda.

2.2 Deficiențe ale stadardelor de comunicații mobile fără fir

Pentru securizarea comunicației în cadrul oricărui dintre standardele 802.11, sunt utilizate diverse protocoale de securitate precum Wired Equivalent Privacy (WEP), Wi-Fi Protected Setup (WPS), *etc.* Toate acestea s-au dovedit a fi vulnerabile, fapt ce a determinat Alința WiFi să împunătățească securitatea acestora.

Principala vulnerabilitate a protocolului WEP provine din construcția defectuasă a algoritmului criptografic RC4 utilizat. Acesta expune cheia criptografică, dacă mesajul cifrat este format din zerouri. Ulterior a fost dezvoltat, protocolul WAP, care deși rezolvă vulnerabilitatea WEP, prin adaugarea unui când de integritate, acesta este vulnerabil la atacuri tip Dicționar.

Observând aceste vulnerabilități, Alinața WiFi, a propus protocolul Protected Access II (WPA2), care introduce cifrarea folosidn algoritmul AES și o metodă de autentificare bazată pe înlănțuirea blocurilor de autentificare (counter cipher block chaining message authentication code protocol CCMP).

Protocol	Cifrare	Autentificare	Integritate Date	Vulnerabilități	Complexitate
WEP	RC4	WEP-Open și WEP-Shared	CRC-32	Chopchop, Bittau fragmentare, FMS, PTW, DoS	scăzut
WPA	TKIP	WPA-PSK și WPA-Enterprise	Michael	Chopchop, WPA-PSK, Reset, DoS	ridicată pentru WPA-Enterprise
WPA 2	CCMP și AES	WPA2-Personal și WPA2-Enterprise	CBC-MAC	DoS, MAC spoofing, Atac dciționar WPA2-Personal	ridicată pentru WPA2-Enterprise

Table 2.1. Comparație între protocoalele de securitate pentru comunicații fără fir.

2.3 Instrumente pentru simulare a rețelelor mobile fără fir

Când am încercat să determinăm cea mai bună modalitate de analiză a performanțelor modelelor de securitate propuse în această teză, ne-am confruntat cu provocarea multiplelor simulatoare existente pentru rețelele mobile fără fir.

Autorii, [MTC+11], prezintă un studiu critic aprofundat al celor mai utilizate instrumente de simulare pentru rețele mobile fără fir cu aplicabilitate directă în cazul VANET.

Studiul privind rețelele de senzori fără fir [MZ12] prezintă o serie de simulatoare din surse publice. Acesta clasifică instrumentele în funcție de obiectivul lor principal astfel:

- **simulatoare orientate la nivel de emulator și cod**. Aceste instrumente sunt axate nivelul fizic al rețelelor. În această categorie intră: ATEMU [PBM+04], Avrora [TLP05], EmSIm [TRJ02], Freemote Emulator [KMKW11], MSPSim [EÖF+09], TOSSIM [LLWC03] și VMNet [WLZN07];
- **orinetate pe topologie**. Această categorie se concentrează pe capacitatea de a testa algoritmi și protocoale de rutare. Singurul simulator din această categorie este prezentat în articolul [MZ12];
- **orientate pe mediul de comunicație fără fir**. Aceste simulatoare sunt axate pe aspectul wireless al rețelelor și emulează probleme de mediu care pot apărea în viața reală. În acest sens, autorii [Szt04] prezintă Prowler. Un alt exemplu este Wireless Sensor Network Localisation Simulator and WSNet [JYX+18];
- **simulatoare la nivel rețea și aplicație** . Aceste simulatoare fac posibil „transportul și prelucrarea datelor colectate". În această categorie menționăm AlgoSenSim [MF09], NetTopo [SWZ+08], SENSE [CBP+05], Sensor Security Simulator (S3), SHAWN [FKFP07], SIDnet-SWANS [GGD+07], Sinalgo [ANDK+18] și TRMSim-WSN [MP09];
- **transversal**. Aceste simulatoare fac posibilă simulări ale rețelei wireless la diferite grade de abstractizare. În această categorie menționăm: COOJA [EÖF+09], J-Sim [SHK+06] and Sensor Network Package [RKMC16], SENS [SKA04] și WSN-Sim [MZ12];
- **orintate spre protocoale de rutare și multicast**. În această categorie intră simulatoare bazate în principal pe simulatorul de rețea NS-2, cum ar fi: Mannasim

[PRG15], NRL Sensorsim [BE19] și RTNS [PCL07];

- **orientate pe mediul software**. Aceste simulatoare sunt bazate pe OMNeT ++ și includ: Castalia [Bou07], MiXiM [WSKW09], NesCT [VH08], PAWiS [MGH06] și SENSIM [LW82];
- **orinetate pe utilizatori finali**. Aceste simulatoare sunt bazate pe Ptolemy II, de exemplu: Viptos [CLZ05] și VisualSense [BKL+05].

Deși există mai multe opțiuni disponibile, simulatorul UPB VANET Sim2Car este, din câte cunoaștem la acest moment, primul care implementează securitatea în VANET. Un alt simulator utilizat în cadrul acestei teze de doctorat pentru validarea modelelor de securitate propuse este TRMSim-WSN. Acesta este un simulator specializat pentru modele de încredere și reputație în rețelele de senzori fără fir.

Simulatorul UPB VANET Sim2Car (Figura 2.2) este primul simulator utilizat pentru testarea datelor și emularea de securitate a modelelor propuse în teză. Simulatorul universității Politehnica București utilizează standardul 802.11b fără fir. Datele de intrare utilizate de acest instrument sunt modelele de mobilitate ale vehiculelor în funcție de care vehiculele sunt poziționate pe hartă. Poziția lor este actualizată periodic pentru a păstra o imagine realistă. Un aspect interesant este faptl că acesta ia în considerare diferite tipuri de comportament ale șoferilor.

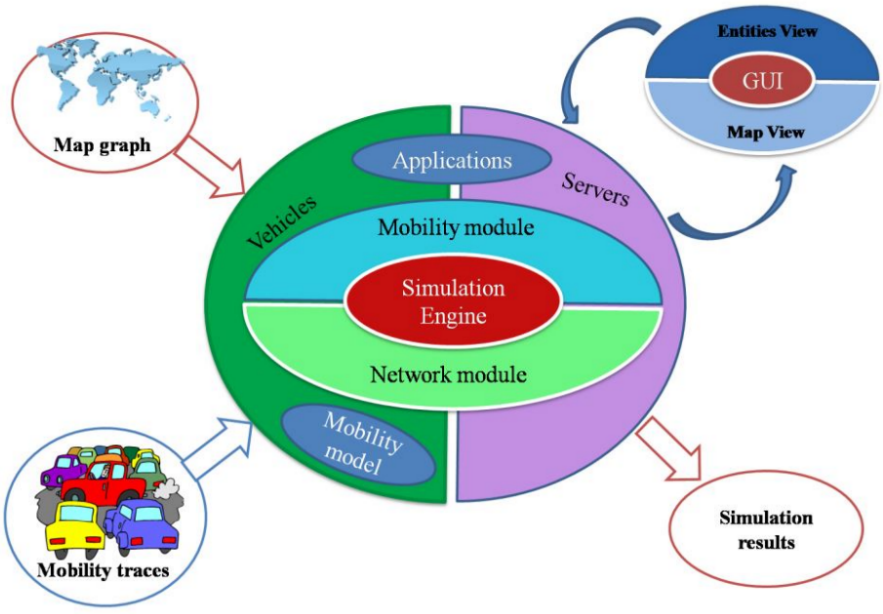

Figure 2.2. Arhitectura simulatorului UPB VANET Sim2Car [MD12].

TRMSim-WSN (Figura 2.3) reprezintă al doilea simulator pe care îl folosim pentru testarea și evaluarea modelelor de încredere și reputație propuse în această teză. Fiecare model de încredere și reputație are propriile sale caracteristici și particularități. Principalul avantaj al acestui simulator este arhitectura sa generică, care permite versatilitatea și asigură implementarea diferitelor modele de încredere și reputație în rețelele de senzori fără fir.

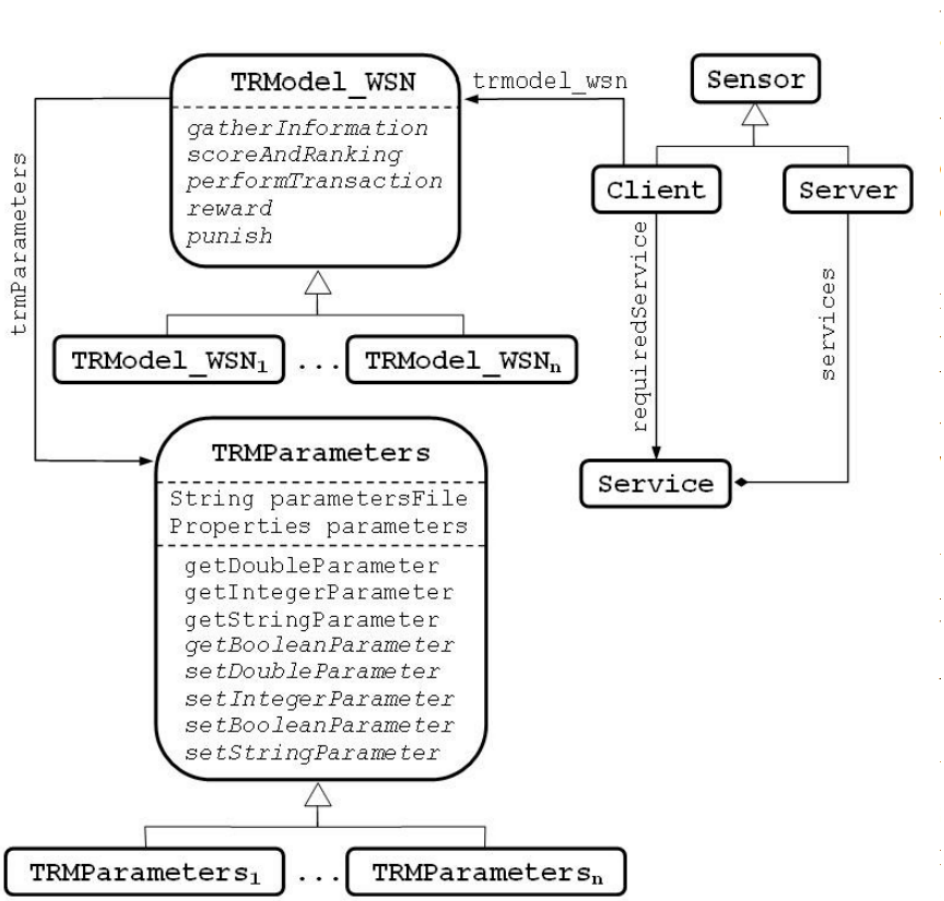

Figure 2.3. Arhitectura simulatorului TRMSim-WSN [GMMP09].

2.4 Concluzii

În acest capitol, am prezentat cele mai importante aspecte rețelelor mobile fără fir. În 2.1, am prezentat un sumar al tehnologiilor actuale în comunicațiile fără fir precum și metodelel actuale de securizare arețelelor fără fir 2.2. De asemenea am efectuat și o scurtă descriere a mai multor instrumente utilizate în simularea rețelelor mobile fără fir în secțiunea 2.3, cu analiza în detaliu a instrumentelor Sim2Car și TRMSim-WSN.

3 | Securitatea în rețele mobile fără fir

Acest capitol prezintă o serie de atacuri asupra rețelelor mobile fără fir și mai multe metode existente pentru mitigarea acestora. De asemenea efectuam o comparație între o serie de algoritmi criptografici în termeni de performanță. În plus, analizăm performanța acestora folosind o implementare reală în cadrul unui simulator de rețele mobile fără fir. În al doilea rând, analiză modele multiple de încredere și reputație aplicabile în rețelele mobile fără fir, subliniind punctele lor forte dar și minusirile acestora.

3.1 Atacuri în rețele mobile fără fir

Raya și Hubaux [RH05] prezintă o analiză critică a evoluției mecanismelor de securitate în rețele vehiculare, de la primele soluții concepute în corelație cu tahometrul, până la utilizarea dispozitivelor de urmărire tip GPS sau a aplicațiilor pentru dispozitive mobile smart.

În articolul [RPH06], autorii prezintă diferitele tipuri de atacuri specifice pentru sisteme inteligente de trafic (Intelligent Traffic Systems - ITS) și propun mai multe metode și mecanisme de de securitate pentru mitigarea acestora. În tabelul 3.1 prezentăm o comparație sumară a acestor metode.

Obiectiv principal	Atribute	Descriere
Obiectiv principal	Confidențialitate	capacitatea de a ascunde conținutul unui pachet de la terți.
	autentificare	abilitatea de a urmări fiecare pachet din rețea până la sursă
	integritate	capacitatea de a garanta faptul că un pachet primit este același cu cel trimis fără să fie modificat
	disponibiliate	capaciatatea de pune la dispoziție resursele deținute de nod
Obiectiv de securitate	prospețimea datelor	capacitatea de a decide acuratețea pachetelor primite deși obiectivele privind confidențialitatea și integritatea au fost îndeplinite.
	organizarea individuală	capacitatea de recuperare și de secoperire a unor rute alternative
	sincronizarea în timp	capacitatea de asigurare a faptului că toate nodurile funcționează sub aceeași coordonate temporare
	urmărire securizată	capacitatea de localizare cu acuratețe a nodurilor pentru a determina dacă este maliție, defect, sau dacă este victima unui atac.

Table 3.1. Prezentare sumară a atributelor de secruiate pentru sisteme fără fir.

În articolul [Che15], autorii prezintă o calsificare a atacurilor în (Wireless Sensor Networks - WSN). Acestea sunt prezentate pe scurt în tabelul 3.2.

Autorii articolului [DBFH09] afirmă că principala formă de abuz în rețea poate proveni de la un nod rău intenționat. Acest atac poartă numele de atac Sybil sau poluare și/sau fabricarea informațiilor. Soluția lor pentru mitigarea acestui atac este o abordare bazată pe asigurarea confidențialității și integrității datelor. Limitările soluției propuse provin din dependența ridicată de capacitatea de calcul a platformei.

Atacuri orientate spre obiectiv	Active	Jamming, Blackhole, Sybil, DoS, DDoS, Interceptarea pachetelor
	Passive	Monitorizarea traficului, Scurgerea de pachete, analiza traficului
Atacuri oreinatet spre acțiune	Inside	Mole, Blackhole, Grayhole, Atacuri malițioase, On-off attack
	Outside	Scurgerea de pachete, DoS, DDoS, Epuizarea resurselor
Atacuri orientate pe staturi	Fizic	Bruiaj, Scurgerea de pachete
	Legătura de date	Epuizarea canalului, Analiza traficuluis, Sybil
	Rețea	Blackhole, Epuizarea resurselor, Capturarea nodurilor, Scurgerea de pachete
	Transport	Desincronizare, DoS, Inundarea, Epuizarea pachetelor
	Aplicație	Coruperea datelor, Repudeierea, Nod malițios, BS path DoS

Table 3.2. Prezentare sumară a tipurilor de atacuri în WSN.

3.2 Securitate rețelelor mobile fără fir pe bază criptografiei

Securizaera rețelelor mobile fără fir prin criptografie implică cifrarea și descifraera datelor procesate în cadrul rețelei. Acest lucru asigură confidențialitatea pachetelor menționate. Având în vedre că resursle compuattționale sunt limitate în cadrul WSN am ales criptografia simetrică.

Atfel, in această teză am implementat și evaluat următorii algoritmi criptografici simetrici: AES, AES Fast, AES Light, Blowfish, Camellia, Camellia Light, Tea și Twofish. O prezentare sumară acestora se regăsește în tabelul 3.3.

Algoritm	**Dimensiune chei (biți)**	**Dimensiune bloc (biți)**	**Runde**
AES	128	128	10,12 sau 14
AES Light	128	128	10,12 sau 14
AES Fast	128	128	10,12 sau 14
Blowfish	32-448	64	16
Twofish	128,192 sau 256	128	16
Camellia	128, 192 sau 256	128	18 sa 24
Camellia Light	128, 192 sau 256	128	18
Tea	128	64	Variabil(64 recomandat)

Table 3.3. Sumar algoritmi criptografici simetrici evaluați în cadrul tezei de doctorat.

Advanced Encryption Standard (AES) este un algoritm de cifrare care are trei ver. Algoritmul **AES Fast** este o versiune optimizată a algoritmului AES în sensul că folosește tabele statice pentru tabelele de permutare cu dimensiune de 8 KB. Algoritmul **AES Light** este o versiune optimizată a algoritmului AES în ceea ce privește amprenta sa computațională. Nu are tabele statice și, prin urmare, este cea mai lentă versiune a algoritmului AES. Algoritmul **Blowfish** are 16 runde și folosește dimensiuni bloc de 64 de biți și chei criptografice cu lungime variabilă între 32 de biți și 448 de biți. **Twofish** este unul dintre succesorii lui Blowfish. Acesta are 16 runde și poate suporta trei dimensiuni posibile ale blocurilor cheie de 128, 192 și 256 biți, cu blocuri de date de 128 biți. Algoritmul **Camellia** este un alt algoritm simetric conceput de Mitsubishi. Are 18 sau 24 de runde și trei dimensiuni cheie posibile de 128, 192 și 256 de biți, cu blocuri de date fixe de

128 de biți. Cifrul **Light al algoritmului Camellia** este optimizat pentru dimensiune și, prin urmare, are o implementare mai mică. **Tiny Encryption Algorithm (TEA)** este unul dintre cele mai simple. Acesta are un număr variabil de runde, deși sunt recomandate 64 de runde pentru menținerea unui nivel de convidențialitate ridicat.

3.3 Abordări privind încrederea și reputațieia în rețelele mobile fără fir

Autorii din [FZC+20] abordează necesitatea securității în rețelele de senzori fără fir împărțind problemele în două mari categorii: atacuri externe și interioare. Aceștia afirmă că atacurile exterioare sunt ușor de atenuat utilizând autentificarea și criptarea mesajelor, dar atacurile din interior sunt cele care pot distruge complet rețeaua. Autorii menționează modelele de încredere și reputație ca fiind cea mai bună abordare de securitate împotriva atacurilor interioare, limitând impactul pe care un utilizator îl poate avea asupra întregii rețele.

Importanța rețelelor de senzori fără fir și necesitatea securității sunt subliniate și de autorii articolului [PA13]. Aceștia menționează atât aplicații militare, cât și civile și clasifică posibilele atacuri asupra rețelelor de senzori fără fir drept atacuri de rutare și atacuri de trafic de date.

În lucrare [AHR+17], este prezentat un interesant cadru de detectare participativă pe trei niveluri pentru monitorizarea poluării în regiunea urbană din Bangladesh. Autorii lucrării cite amintoosi2013trust, au propus un cadru de recrutare participativă de recrutare bazat pe participarea socială. Acest cadru a fost evaluat în funcție de simulare și a demonstrat eficiența în ceea ce privește selectarea unui număr mare de participanți cu încredere ridicată în comparație cu abordările arhitecturale one-hop. În capitolul de carte [SCN+16], autorii prezinta o priviere de ansamblu asupra rețelelor de detectare participativă (Participatory Sensing Networks - PSN), evidențiind provocările și oportunitățile unor astfel de rețele.

O altă abordare interesantă este bazată pe cluster, împărțind astfel încrederea în două: inter-cluster și intra-cluster [KSH+19]. În această lucrare, autorii fac o diferență clară între încrederea în date și încrederea în comunicare, o abordare similară cu cea propusă în această lucrare în care ne ocupăm de încrederea utilizatorilor și încrederea în comunicare.

Autorii articolului [SKS20] prezintă un studiu mai elaborat și o taxonomie asupra schemelor de gestionare a energiei în rețelele de senzori fără fir. Taxonomia prezintă atât abordări de gestionare a energiei, cât și algoritmi de conservare a energiei.

Securitatea bazată pe încredere și reputație pentru rețelele mobile fără fir a devenit mai populară și una dintre cele mai utilizate abordări. Utilizarea modelelor de securitate bazate pe criptografie pentru rețelele de senzori fără fir a devenit din ce în ce mai nepopulară, așa cum se menționează în [NMBG20], din cauza încărcării computaționale mari din rețea.

3.4 Rezultate experimentale a unor soluții de secritate distince

Algoritmii descriși în secțiunea 3.2 au fost implementați și testați folosind librăria Crypto++ 5.6.0 [com20] în limbajul de programare C++. Evaluarea s-a realizat folosind mediul de dezvoltare Visual Studio 2005 pe o stație de lucru având un procesor Intel la frecvența de 1.83 GHz. Această configurație este considerată a fi învechită, însă este similară cu puterea de calcul a dispozitivelor mobile tip wearables.

Luând în considerare caracteristicile simulatorului, precum și caracteristicile algoritmilor, am efectuat mai multe implementări ale modulelor de securitate, pentru fiecare algoritm criptografic menționat. Aceste implementări au fost realizate pentru a crea o analiză comparativă între performanțele algoritmilor atât în implementare individuala, cât și în cadrul simulatorului Sim2Car. Am realizat aceeastă analiză comparativă pentru a determina depedența dintre algoritmul ales și arhitectura aplicației în care acesta urmează să fie utilizat. Testele au arătat rezultate diferite în cazul abordării individale în comparație cu implementarea în simulator. Performanța algoritmilor a fost diferită în cele două cazuri.

Testele pentru cifraera celui mai mic bloc de date (1908 octeți) au arătat că cea mai bună performanță a avut-o algoritmului Blowfish, în timp ce cea mai proastă a fost cea a algoritmului Camellia Light. Criptarea celui mai mare bloc de date (2480400 octeți) a determinat AES ca fiind cel mai performant algoritm și algoritmul Tea ca cel mai ineficient 3.1.

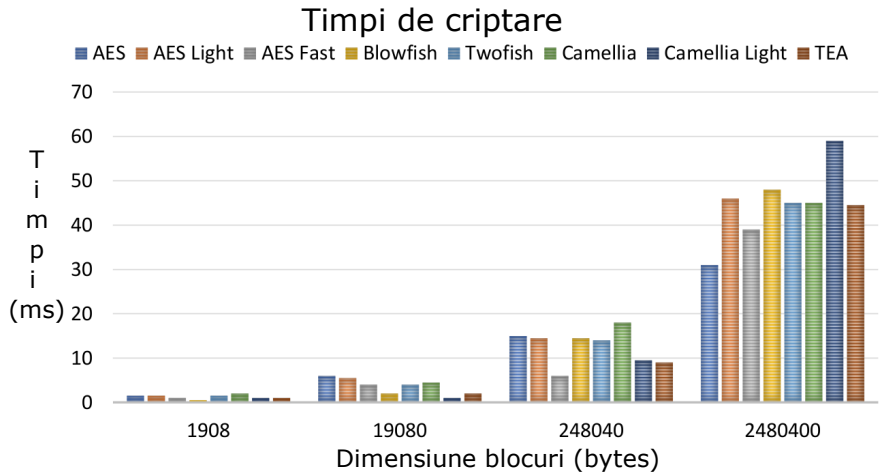

Figure 3.1. Timpul de cifrare în funcție de dimensiunea datelor procesate.

Testele pentru decriptarea celei mai mici dimensiuni a blocului de date (1908 octeți) au arătat că cea mai bună performanță a avut-o algoritmului Camellia, în timp ce cea mai proastă a fost cea a algoritmului AES. Decriptarea celui mai mare bloc de date (2480400 octeți) a determinat algoritmul AES ca fiind eficinet algoritm iar algoritmul AES Light ca cel mai ineficinet 3.2.

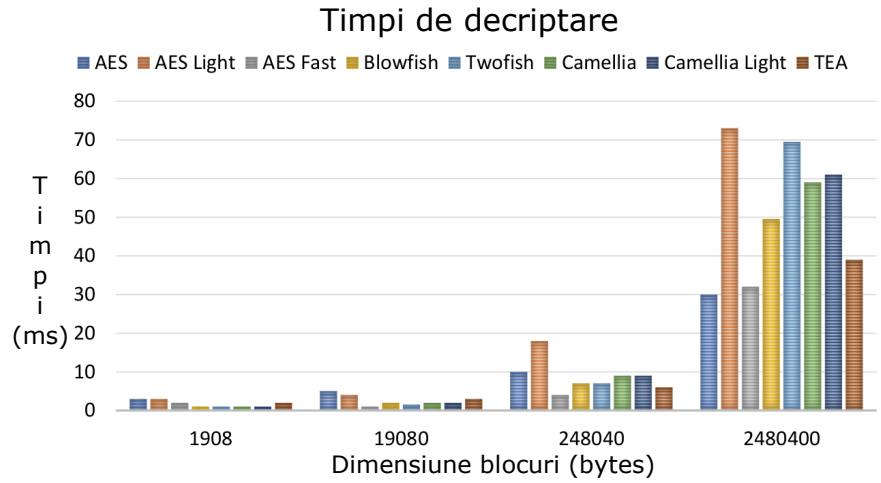

Figure 3.2. Comparison for decryption time between algorithmss.

Pentru pachetele mici de date, algoritmul Blowfish se dovedește a fi cel mai rapid, în timp ce pentru pachete mairi de date cel mai potrivit algoritm este AES. Aceste rezultate sunt de așteptat, deoarece Blowfish este cunoscut a fi un cod de blocare rapid pentru o cantitate mică de date, deoarece nu are nevoie să schimbe tastele atât de des. Schimbarea cheilor consumă mai mult timp în cifru, iar la criptarea unei cantități mari de date schimbarea cheilor aduce întârzieri.

Experimentul efectuat în simulatorul UPB Sim2Car a avut scopul de a monitoriza numărul de mesaje schimbate între mașini. Dimensiunea medie a pachetului mesajelor schimbate între mașini este de 220 de octeți. Rezultatul simulărilor a arătat ca pentru un număr ridicat de mesaje schimbate între vehicule, algoritmul cel mai eficient este TEA. Simularea utilizând algoritmul TEA a avut un numărul maxim de mesaje schimbate într-un anumit punct de aproape 4 ori mai mare decât numărul de mesaje schimbate în comparație cu ceilalți algoritmi. Cifrul cel mai puțin eficient a fost Camellia Light. Acest lucru arată dependența dintre algoritm și arhitectura aplicației unde este implmentat, astfel rezultatele obținute în implementările independente sunt diferite de rezultate obținute în implementarea reală în mediul de simulare Sim2car.

3.5 Concluzii

Î n acest capitol, am prezentat metode existente pentru mitigarea atacurilor în rețele mobile fără fir. În primul rând, în secțiunea 3 am efectuat o prezentare generală a principalelor atacuri în rețele mobile fără fir. În secțiunile 3.2 și 3.4, am efectuat o analiză a performanței unor algoritmi criptografici implementați atât în mod individual cât și în cadrul simulatorului Sim2Car, dezvoltat în cadrul UPB. comparație între ele în ceea ce privește performanțele și, de asemenea, analizează performanța acestora într-un simulator de rețele mobile fără fir.

4 | Securitate în VANET

În acest capitol, prezentăm conceptele teoretice și provocările. În secțiunea 4.1 sunt prezentate ecuația și modelele pentru gestionarea încrederii urmate de principalele rezultate obțin simulare în secțiunea 4.2. Modelul de încredere propus se bazează pe criptografie utilizând o infrastructură cu chei publice (PKI) pentru distribuirea și validarea vehiculelor în rețea. Comunicarea dintre fiecare două vehicule este asigurată prin cifrarea mesajelor folosind o cheie derivată obținută utilizând algoritmul de schimb de chei Diffie-Hellman. Comunicarea V2I este securizată utilizând certificate .X509. Capitolul se încheie cu avantajele și dezavantajele modelului de securitate propus, precum și cu posibilele îmbunătățiri din secțiunea 4.4.

4.1 Abordare bazată de încredere și reputației în VANET

Conceptul de încredere se referă la identificarea partneriilor dintr-un grup, pentru a putea deterina care dintre aceștia este de încredere. Primul element se referă la vehiculele sau utilizatorii din rețea, al doilea element este puțin mai dificil de definit. Într-o ierarhie subordonată există o autoritate de certificare principală care autorizează mai mulți descendenți și numai certificatele emise de aceste entități sunt recunoscute ca fiind de încredere.

Într-o rețea cu certificare încrucișată, există un număr diferit de CA care poate autoriza orice altă CA, "cu excepția cazului în care se aplică constrângeri de denumire" [Lin00]. Încrederea acestui tip de rețea nu este uniformă, și variază foarte mult în funcție de lungimea lanțului de certificare. Listele de încredere sunt un design de încredere în care nodului i se oferă un set inițial de chei publice ale CA-ului de încredere și pentru a fi validat cu succes.

În mod generic, modelele de gestionare a încrederii sunt mecanisme ale rețelor pentru asigurarea raportului încredere-riscuri optim. Cele mai comune modele de gestionare a încrederii sunt: sisteme cu cheie publică, resurrecting duckling și gestionarea încrederii în mod distribuit. Primul model implică existența unei autorități de certificare, astfel nodurile se pot autentifica între ele. Al doilea model se bazează pe conceptul de master-slave, unde masterul trimite comenzi iar nodurile trebuie să execute în tocmai setul de instrucțiuni transmis. Al treilea model se bazează pe ideea că trebuie încrederea se câștigă, iar apoi trebuie menținută, printr-un comportament adecvat în rețea.

Gestionarea încrederii în contextul rețelelor mobile ad hoc are mai multe provocări

având în vedere comunicarea oportunistă și natura ad hoc a rețelei. Rețelele ad hoc se bazează pe cooperarea activă dintre toate nodurile pentru rutare și redirecționarea pachetelor. Distanța de comunicare, lățimea de bandă sau pragul sunt parametri care influențează direct conportamentul nodurilor pentru acțiuni egoiste în sensul că va asculta datele doar din apropierea sa fără a le transmită mai departe.

Abordarea de securitate propusă în această teză implementează o formă hibridă de model de încredere între sistemele cu cheie publică și managementul încrederii distribuite. La început, infrastructura oferă fiecărui nod avantajul unei încrederi neutre, deci toate nodurile sunt considerate „amabile și dezinteresate". Folosind informațiile colectate de dispozitivele de monitorizare, se face o listă a comportamentului necorespunzător. Odată ce un nod depășește un prag dat, așa cum a spus Friedrich Nietzsche, încrederea lui scade.

Protocolul Cooperative MAC este un protocol al standardului 802.11 compatibil cu mai multe valori ale ratelor de transfer pe baza ideii că utilizatorii dintr-un sistem VANET au efectuat schimburi de mesaje cu diferite viteze de trasfer. În cazul unui canal de comunicații cu viteză redusă între un expeditor și un receptor, dacă există un al treilea nod între cei doi care are viteze de transmisie mai mare, atunci acel utilizator va acționa ca expeditor pentru a accelera transmisia generală și a reduce overheadul general.

Utilizarea generală presupune că fiecare nod trebuie să afle în proximitatea nodurilor vecine și să funcționeze în baza unui canalul de comunicație potrivit. Prin urmare, cererile de trimitere (RTS) și Clear to Send (CTS) trebuie să fie introduse în sistem pentru evitarea coliziunilor și rezervarea canalului (NAV).

Să presupunem că există un nod care dorește să trimită date (expeditor), un nod căruia îi sunt destinate datele (receptor) și două noduri din proximitate (Helper1 și Helper2) ca în figura 4.1. Transmiterea datelor urmează modelul de mai jos:

- expeditorul trimite un pachet RTS;
- fiecare nod din zonă primește pachetul RTS și verifică dacă adresa expeditorului există în tabelul de proximitate. Dacă nu este, va fi adăugat. Apoi, fiecare coleg calculează rata de transfer la care ar putea transfera date și le stochează împreună cu adresa MAC în tabelul de proximitate;
- dacă un nod primește pachetul RTS fără erori, acesta devine un posibil ajutor. Fiecare asistent evaluează dacă ratele lor de trasnsfer pot îmbunătăți transferul. Dacă se poate, va trimite un pachet de asistență (HTS). Asistentul cu cea mai bună apropiere este ales ca intermediar. Notă: HTC este identic cu un tip de mesaj CTS;
- receptorul trimite un CTS pentru a rezerva canalul. Dacă există un ajutor, acesta rezervă canalul pentru timpul necesar pentru un transfer, în caz contrar, acesta rezervă canalul pentru timpul necesar comunicării directe;
- expeditorul începe să trimită datele. Dacă acestea sunt primite fără erori, receptorul transmite pachetul ACK. Acest pas se repetă până la finalul transmisiei.

Protocolul Cooperativ Mac (CoopMAC) prezintă avantaje precum diversitate spațială mai mare, deoarece orice daune în comunicațiile dintre două noduri pot fi preluate de un al treilea cu o putere mai mare a semnalului și rate de transnfer mai bune.

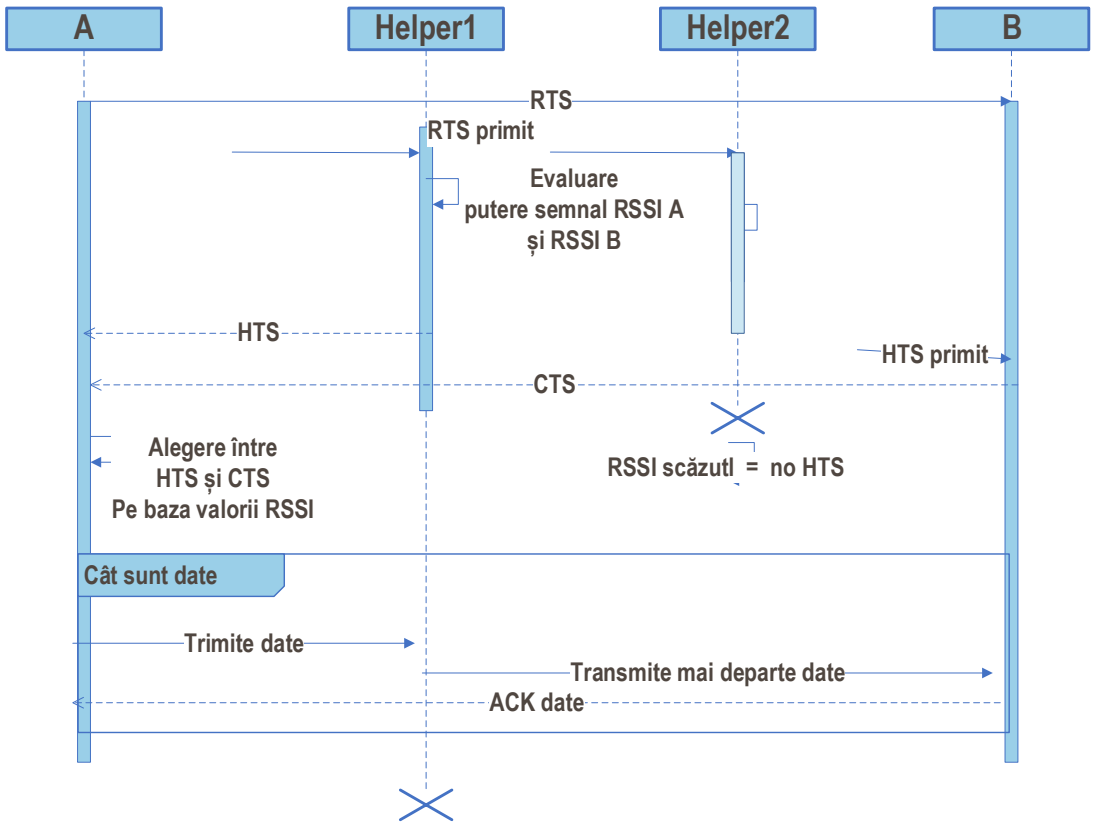

Figure 4.1. Transfer de date prin protocolul CoopMAC.

Protocolul are deficiențe, cum ar fi faptul că asistentul ar putea să nu dorească să fie atât de util și să refuze redirecționarea pachetelor. În acest caz, expeditorul trebuie să observe lipsa de ajutor și să găsească un alt intermediar sau, dacă nu există, să trimită datele singur, în ciuda ratei reduse de trasnsfer.

O altă potențială problemă care ar putea veni de la un nod asistent asistent, este faptul că acesta poate să devină rău intenționată. Nodul asistent devenit malițios ar putea ajunge să modifice payloadul mesajelor și să le transmită. Acest lucru este foarte greu de detectat din punctul de vedere al expeditorului, deoarece acesta nu cunoaște mesajul inițial.

4.2 Aspecte ale modelului de securitate bazat pe criptare în VANET

Acest capitol prezintă validarea mecanismului de securitate propus prin simulare folosind Sim2Car. Algoritmii utilizați pentru testare sunt AES, AES Light și AES Fast.

Versiunea clasică este o implementare a algoritmului AES (Rijndael) din FIPS-197 care utilizează un tabel static de 256 de cuvinte tabel pentru fiecare criptare și decriptare

pentru un total de 2KBytes. Se adaugă astfel 12 operații de rotație per rotunjiți valorile conținute în celelalte tabele din conținutul primului.

Versiunea „rapidă" este o implementare a algoritmului AES (Rijndael) de la FIPS-197 optimizat de Dr. Brian Gladman în ceea ce privește consumul de timp prin utilizare 8 KBytes de tabele statice pentru precompilare rapidă.

Dat fiind faptul că dimensiunea pachetului variază între 9 octeți și 614 octeți, iar dimensiunea medie a pachetului este de 177 octeți și faptul că pentru dimensiuni relativ mici de intrare, versiunea „rapidă" are cele mai bune performanțe se recomandată utilizarea AES Fast. Această decizie a fost consolidată si de numărul crescut de mesaje schimbate în rețea.

Valorile ratelor maxime de trasnfer $r_{11}, r_{5.5}, r_2$ și Sr_1 sunt definite pentru următoarele valori de 11 Mbps, 5,5 Mbps, 2 Mbps și 1 Mbps.

Timpul trasnmisiei al unui pachet de date pentru o rată de tranziție de date fixă de x Mbps se calculează folosind ecuațiile curente:

$$T_{11} = T_{count}(n) + T_{overhead} + \frac{8L}{R_{11}}$$
$$T_{5.5} = T_{count}(n) + T_{overhead} + \frac{8L}{R_{5.5}}$$

unde $T_{overhead}$ se defineste astfel

$$T_{overhead} = T_{PLCP} + T_{DIFS} + T_{RTS} + T_{CTS} + 3T_{SIFS} + T_{TACK}$$

și $T_{count}(n)$ se definește ca fiind timpul total necesar pentru realizaera unei conexiuni cu succes.

În plus, pentru rata de trasnfer de 2 Mbps, dacă nu există un nod asitent definim timpl de trasnfer conform ecuației următoare:

$T_2 = T_{count}(n) + (P_{11,11} + P_{5.5,11} + P_{5.5,5.5})T_{CoopOH} + \frac{16P_{11,11}L}{R_{11}} + \frac{8P_{5,11}L}{R_{11}} + \frac{8P_{5,11}L}{R_{5.5}} + \frac{16P_{5.5,5.5}L}{R_{5.5}} + (1 - P_{11,11} - P_{5.5,11} - P_{5.5,5.5})(T_{overhead} + \frac{8L}{R_2})$
where $R_x = xMbps$ și $T_{CoopOH} = 2T_{PLCP} + T_{DIFS} + 5T_{SIFS} + T_{RTS} + 2T_{CTS} + T_{ACK}$.

Pe baza ecuațiilor prezentate mai sus, pot fi scris în mod similar ecuații pentru timpul mediu de transmisie T_1.

Protocolul CSMA/CA garantează faptul că fiecare stație din rețea are același număr de pachete pentru o perioadă lungă de timp. Prin urmare, media timpul de transmisie pe pachet este calculat ca:

$$T = f_{11}T_{11} + f_{5.5}T_{5.5} + f_2T_2 + f_1T_1 \quad (6)$$

unde

$$f_{11} = \frac{r_{11}^2}{r_1^2} \quad (7)$$
$$f_{5.5} = \frac{(r_{5.5}^2 - r_{11}^2)}{r_1^2} \quad (8)$$
$$f_2 = \frac{(r_2^2 - r_{5.5}^2)}{r_1^2} \quad (9)$$
$$f_1 = \frac{(r_1^2 - r_2^2)}{r_1^2} \quad (10)$$

Ținând cont de ecuația (6) și de faptul că distanța maximă este dată de $r_{11} \simeq 36m < r_{5.5} \simeq 45m < r_2 \simeq 48m < r_1 \simeq 51m$ putem afirma timpul mediu în cazul CoopMac este mai bun decât T_1 și T_2 dar inferior decât în cazul T_{11} și aprope de T_{55}.

4.3 Rezultate experimentale privind implementarea soluției bază pe criptografie în VANET

Pentru a demonstra validitatea mecanismului de securitate propus, am efectuat mai mult experimente pe paza simulatorului Sim2Car. Am utilizat standardul 802.11 p cu două secanrii de test date de 2 hărți diferite: San Francisco ($121km^2$) and Beijing ($16.807.8km^2$).

Testul a avut în vedere un număr de 500 de vehicule și 10 infrastructuri punct pe hartă. Un număr de 50 de vehicule a fost ales aleatoriu.

Numărul scăzut pachete este motivată de creșterea încărcarii payloadului datorită mecanismului de securitate introdus în rețea. Lungime medie a mesajului fără mecanismul de securitate propus a fost calculat ca fiind de 100 de octeți, în timp ce cu mecanismul de secruitate bazat pe criptografie acesta a crescut numărul de octeți ai mesajului la 177 de octeți.

Un studiu al modului în care atacurile anterioare sunt abordate de mecanismul de securitate prezentat în acest capitol, îl rezumăm după cum urmează:

- atacurile de modificare apar atunci când mesajele schimbate sunt diferite de la receptor la destinație, creând astfel o imagine falsă a traficului. Acest tip de atac a fost rezolvat prin introducerea unui câmp suplimentar pentru hash al mesajului împreună cu mesajul care este verificat la destinație. Dacă hashul calculat al mesajului este diferit de hash-ul trimis, atunci mesajul este abandonat. Această soluție a considerat că erorile de comunicare sunt de cel mult 2 biți și pot fi rezolvate automat de transmițătorul fără fir;
- atacurile de reluare sunt cele care colectează date într-un interval de timp doar pentru a reutiliza acele date ulterior, pentru a obține anumite privilegii. Acest atac a fost rezolvat prin introducerea unei perechi de poziții GPS în datele criptate depuse și ID-ul pachetului de mesaje, prin urmare, dacă un asistent dorește să retrimită informații, datele criptate GPS vor arăta că locația este diferită de locația receptorului diferența dintre marcajul de timp al mesajului și ora curentă este mai mare de un minut. Astfel mesajele vor fi abandonate;
- atacul Sybil fac parte din atacurile de imitare și se întâmplă atunci când un atacator folosește un set diferit de identificare în același timp. Acest atac a fost mitigat prin impunerea faptului că toate mesajele ar trebui să fie semnate, iar datele mesajului să conțină informații despre locația GPS a emițătorului;
- divulgare identității adaugă prejudicii confidențialității utilizatorilor, dezvăluind datele lor secrete. Acest tip de atac este posibil numai dacă atacatorul se află în permanență în apropierea victimei și stabilește legături cu acesta în etapa de descoperire;

- scurgerea pachetelor apare atunci când un atacator ascultă comunicațiile din rețea pentru a obține informații confidențiale. Acest atac este inutil în rețea în faza de schimb de mesaje din cauza algoritmului de cheie partajată impus care determină utilizarea unei chei diferite la fiecare sesiune.

De assemenea am luat în considerare atacurile menționate mai jos și am prezentat și soluția găsită.

- refuzul de serviciu (Dos) sau refuzul de serviciu distribuit (DDoS) sunt atacuri menite să facă rețeaua indisponibilă și astfel utilizatorii neinformați cu privire la starea traficului. Acest atac este foarte greu de atenuat, deoarece nu afectează securitatea sistemului, ci disponibilitatea acestuia. Nu se bazează pe punctele slabe ale criptografiei sistemului, ci pe mediul de comunicații fără fir;
- atacurile de fabricație apar atunci când un utilizator creează informații false pentru a obține anumite privilegii. Aceste informații false inserate în sistem sunt atenuate la nivelul infrastructurii atunci când aceasta corelează informațiile provenite din diverse surse.

Soluția propusă pentru reducerea atacurilor precum DoS, DDoS sau Fabrication este introducerea dispozitivelor de monitorizare în rețea care ar trebui să detecteze comportamentul necorespunzător și să semnaleze acest lucru infrastructurii. Dezavantajul soluției propuse este că eliminarea nodurilor rău intenționat se realizează în același timp și, prin urmare, acțiunile lor pot afecta rețeaua pentru o perioada mai lunga de timp.

4.4 Concluzii

Mecanismul de securitate descris în teză se bazează pe dispozitive fără fir de comunicare în care vehiculele acționează ca și clienți. Aceștia trimit informații privind locația lor GPS. Imaginea de ansamblu a relțelei este oferită de inrastructură. În acest capitol am propus un model de securitate pentru VANET bazat pe certificate .X509 pentru autentificarea utilizatorului în rețea, un algoritm denumit CoopMac pentru îmbunătățirea ratelor de trasnfer folosind noduri partenere, stabilierea unei chei unice per sesiune folosind algoritmul Diffie-Hellman pentru ca fiecare pereche de doi utilizatori să partajeze o cheie secretă pentru criptarea mesajelor schimbate. Principalul dezavantaj pentru rețea este faptul că nu poate asigura anonimitatea, iar infrastructura cunoaște poziția nodurilor în sistem. De asemenea, constrângerile în timp reale ale mecanismului de securitate au fost abia îndeplinite, deoarece numărul de pachete transferate în rețea a scăzut drastic. Această problemă nu a putut fi rezolvată, dar s-a găsit o soluție alternativă prin adăugarea unui model de cooperare în rețea care crește distanța și, prin urmare, și intervalul de timp.

În cazul unui atac asupra infrastructurii sau a autorității de certificare, atacatorii vor obține informații privind participanții din sistem.

5 | Model de securitate în cadrul rețelelor mobile fără fir bazat pe participatoty sensing

Când se vorbește despre reintegrarea vârstnicilor ca un studiu de caz particular pentru încredere și reputație în detectarea participativă (participatory sensing), trebuie clarificate mai multe aspecte: de ce folosim detectarea participativă, de ce este importantă încrederea în aceste aplicații și mai mult, de ce reintegrarea vârstnicilor.

Aplicațiile participatory sensing reprezintă o comunitate în care utilizatorul alege să adune și să partajeze date de la senzorii săi pentru agregarea lor și și oferirea unor informații relevante celorlalți mebrii. Spre deosebire de rețelele oportuniste, utilizatorii sunt conștienți de aplicația activă și partajarea datelor senzorilor se face nu atunci când condițiile se potrivesc, ci atunci când utilizatorii o permit. Abordarea oportunistă are dezavantajul partajării necontrolate a datelor, în timp ce aplicația de detectare participativă are dezavantajul multor întreruperi ale utilizatorilor. Pentru a răspunde mai bine nevoilor utilizatorilor de zi cu zi, a fost propus un model hibrid între aceste două modele de aplicație: utilizatorii decid când și unde partajează datele fără ca aplicația să verifice în permanență acordul utilizatorului.

Managementul încrederii este o tehnică cheie pentru protejarea soluțiilor distribuite de atacuri interne. Acesta constă în determinarea gradului de încredere al unui furnizor de opinii și evaluarea încrederii opiniilor furnizate. Propunerea noastră oferă o nouă abordare pentru gestionarea încrederii prin monitorizarea atât a celor declarate de utilizator cât și a celor cunoscute (cunoștințe existente).

Capitolul este structurat în următoarele secțiuni: în secțiunea 5.1 descriem în detaliu managementul încrederii cu problemele sale și soluțiile propuse. Mai departe, în secțiunea 5.2 prezentăm abordarea propusă pentru gestionarea încrederii într-un sistem participativ. Rezultatele experimentale privind abordarea propusă sunt prezentate în secțiunea 5.3. în secțiunea finală 5.4 prezentăm principalele concluzii ale soluție noastre.

5.1 Abordare de securitate pentru încredere și reputație pe baza participatory sensing

Abordarea propusă încearcă să rezolve problemele de gestionare a încrederii în aplicațiile de detectare participativă bazate pe experiența umană: reintegrarea vârstnicului.

Abordarea actuală ia în considerare recomandările vârstnicilor pentru turiști în ceea ce privește traseele cele mai rapide, cele mai scurte sau cele mai interesante din punct de vedre turistic. De multe ori un traseu mai puțin cunoscut print-un oraș nou poate dezvăluii obiective arhitecturale, culturale, parcuri, etc, deosebite. Acest lucru poate determina o experiență profund îmbunătățită.

Principalele componente ale arhitecturii propuse sunt utilizatorii sistemului, informațiile inițiale formate dintr-un set de obiective și hărți turistice predefinite și cunoștințele utilizatorului despre aceste obiective. Sistemul se bazează la cererea unor utilizatori și răspunsurilor acestora. Acestea reprezintă recomandări reale bazate pe experiența reală a unor persoane.

Arhitectura propusă ia în considerare două tipuri de utilizatori: furnizorii și receptorii. Furnizorii sunt persoanele vârstnice care aleg să-și împărtășească cunoștințele: căi rapide, căi scurte și, mai mult, cele mai relevante obiective turistice dintr-o zonă de interes. Receptorii sunt vizitatorii care au nevoie de asistență atunci când vizitează un oraș străin. Un utilizator poate fi fie un receptor, fie un furnizor, dar nu ambele în același timp.

Reintegrarea vârstnicilor are o paradignă peer-to-peer în care utilizatorii comunică folosind principiul cerere-ofertă. Activitatea de la egal la egal se realizează prin intermediul aplicației mobile dedicate TERI - Trust Elder ReIntegration. Sistemul se bazează pe premisele că receptorul deține un smartphone cu serviciul de localizare activat. Monitoarele GPS ale fiecărui furnizor calculează cât de mult urmează utilizatorul o cale sugerată și, la sfârșitul căii sau când aplicația este închisă, trimite înapoi la furnizor procentul rezultat. Furnizorii completează își pot ajusta recomandările în funcție de feedbackul primit sau de alte informații deținute.

Fiecare recomandare dată de un vîrstnic unui turist poate fi orientată în timp, distanță sau locație. Pe baza acestei orientări, profilul furnizorului și profilul destinatarului li se atribuie un scor. Cu cât scorul este mai mare, cu atât compatibilitatea dintre furnizor și receptor este mai mare.

Schimbul de informații este împărțit în 4 etape: fază de inițializare, învățare, recomandare și ajustare. Fiecare etapă este importantă pentru colectarea datelor și pentru calculul încrederii utilizatorului. Etapele reprezintă fluxul real de informații pe care un utilizator îl aduce aplicației: mai întâi un utilizator trebuie să declare ceea ce știe și care sunt interesele sale. Apoi, sistemul descoperă cât de mult știe utilizatorul cu adevărat despre interesele sale. După crearea unui profil, furnizorii pot începe să sugereze căi vizitatorilor. Faza finală este aceea de corectare a recomandării. Fiecare dintre aceste faze este descrisă în detaliu în continuare.

Fiecare utilizator al sistemului are o încredere cu valori cuprinse între 0 și 1, unde 0 înseamnă lipsa încrederii și 1 înseamnă încredere totală. Fiecare feedback reprezintă un scor pe care receptorul îl împărtășește cu privire la calitatea recomandării. La intrarea în sistem, fiecare utilizator primește o valoare care reprezintă încrederea sa inițială. De asemenea, fiecare furnizor stochează o listă a receptorilor cu care a fost în contact, împreună cu procentul lor de disponibilitate pentru a urma calea sugerată, în timp ce fiecare receptor stochează lista tuturor furnizorilor cu care a fost în contact, împreună cu încrederea rezultată . În acest fel, fiecare utilizator poate calcula încrederea celorlalți, dar nu a sa. De asemenea, neștiind dacă celălalt utilizator a dat un feedbak pozitiv sau nu, nu se poate modifica valoarea de încredere asociată fără a-și influența propria încredere.

Principalul avantaj al abordării propuse este capacitatea de a face sugestii pentru turiști nu numai în ceea ce privește calea cea mai rapidă sau cea mai scurtă, ci și pentru vizitarea obiectivelor turistice, împreună cu o nouă abordare de gestionare a încrederii. Aplicația mobilă aduce o mobilitate ridicată în partea utilizatorului.

5.2 Model pentru gestiunea încrderii și reputației prin reintegraera vârstnicilor folosind participatory sensing

Modelul de încredere propus este analizează următoarele perspective: monitorizează încrederii în sine a utilizatorului, încrederea sistemului în cunoștințele utilizatorului și încredrea utilizatorilor în cunoștințele sistemului. Aceste perspective corespund diferitelor faze ale sistemului și sunt prezentate în continuare.

În faza de inițializare, fiecare utilizator trebuie să completeze un profil de utilizator care să precizeze unde locuiește, ce orașe cunoaște și în ce grad, timpul petrecut în fiecare oraș și, de preferință, cartierele sau zonele cele mai familiare. Aceste informații creează un nivel inițial de încredere al utilizatorului în ceea ce privește credibilitatea nodurilor. Aceste informații ajută la crearea încrederii inițiale a furnizorilor și interesul principal al receptorilor pentru sugestii ulterioare.

În faza de învățare, fiecare donator trebuie să completeze un set de provocări. Inițial aceștia își declară interesele și apoi avestea sunt evaluate. Categoriile de interese pot fi muzee, teatre, spitale, restaurante, florării *etc.* Al doilea grad de încredere trebuie să fie suficient de influent pentru a reflecta cunoștințele utilizatorilor, dar fără a elimina importanța feedback-ului. Provocările reprezintă o hartă virtuală a orașului în care trebuie utilizatorii donatori trebuie să identifice cât mai multe obiective turistice din zona lor de interes și ulterior să aleagă dintr-un set de cai de acces spre acel loc. Numărul de obiective recunoscute din numărul total cunoscut de sistem din acea zonă de interes determină un al doilea grad de încredere a donatorilor. Abaterea de la calea sugeratăde către furnizor poate determina gradul de cunoștințe în ceea ce privește călătoria rapidă a nodurilor furnizore. Aceasta reprezintă, de asemenea, o parte a celui de-al doilea grad de încredere al furnizorului. Receptorul trebuie, de asemenea, să completeze un set de provocări cu privire la interesele acestora și să completeze un set de provocări cu privire la aceste interese.

Această fază contribuie la calcularea scorului unei recomandări. Încrederea rezultată după faza unu și doi reprezintă încrederea inițială (TI) reprezentată de Ecuația 5.1. Procentele fiecărui element din ecuația calculului de încredere au fost evaluate stocastic.

$$TI = \beta \times TInitialize + (1 - \beta) \times TLearning, unde \quad \beta = 0.1 \tag{5.1}$$

După faza de învățare începe faza de comunicare efectivă. În acest moment, sistemul acceptă cererile primitorilor și răspunsurile vârstnicilor. De asemenea, sistemul acceptă un profil de urgență în care oferă utilizatorului informații de bază despre spitale sau stații de transport public.

Fazele de recomandare și feedback funcționează corelat, în sensul că pentru fiecare recomandare se oferă și feedback. Dar, feedback-ul dat trebuie să ia în considerare și profilul receptorului. Pe baza gradului de similitudine, feedback-ul poate avea o importanță mai mare sau mai mică asupra rezultatului final. Dacă o conformitate totală a căii sugerate înseamnă 100% opinie validă din partea receptorului, atunci 50% conformitatea acesteia ar trebui să aibă doar jumătate din importanța feedback-ului. Având în vedere faptul că încrederea are o valoare cuprinsă între 0 și 1 în timp ce feedback-ul (F) are o valoare între 0 și 10, trebuie făcută o împărțire la 10 pentru a rămâne în intervalul de încredere declarat. Mai explicit, luând în considerare feedback-ul (F) o valoare între 0 și 10 reprezentând satisfacția receptorului față de o cale sugerată și un procent de obedientă (OP), o valoare între 0 și 1, reprezentând gradul cu care receptorul a urmat calea sugerată, ecuația pentru comunicarea de încredere între doi utilizatori este menționată în ecuația 5.2.

$$TrustFeedbackperRequest/Response = 0.1 \times OP \times F \tag{5.2}$$

Calcularea încrederii utilizatorilor trebuie să reflecte cât mai bine cunoștințele lor, astfel încât să fie cel mai bine împărțit între fazele sistemului. De exemplu, dacă faza inițială are un procent mai mare decât faza de învățare, utilizatorii care au trăit pentru o perioadă mai lungă de timp într-un anumit loc, dar nu au cunoștințe aprofundate, ar avea un scor mai mare decât un utilizator cu cunoștințe solide, dar care nu a trăit în acel loc o perioadă mai scurtă de timp. De asemenea, trebuie să menținem echilibrul între încrederea pe care sistemul o acordă utilizatorului și încrederea calculată prin feedback-ul primit. De exemplu, dacă procentul de feedback este mic, un furnizor cu un nivel ridicat de încredere poate trimite recomandări proaste, deoarece nu afectează rezultatul general. Pe de altă parte, un utilizator cu o încredere bună a sistemului, care îndeplinește receptorii rau intenționați, poate fi distrus dacă procentul de feedback este prea mare. Prin urmare, fazele inițiale și de învățare trebuie să contracareze faza de feedback. În mod generic, încrederea unui utilizator este compusă din încredere inițială de 55% (TI), care este colectată în prima și a doua fază, și 45% încredere rezultată din feedback-ul dat de utilizatori (TF). Calculul încrederii feedback-ului altor utilizatori este dat în Ecuația 5.3.

$$TF = \frac{\sum_{I=1}^{n} 0.1 \times OP_{IR} \times F_{RI}}{|G|} \tag{5.3}$$

unde |G| este cardinalul listei de oferitori care au avut anterior contact cu acesta . Această ecuația poate fi rescrisă astfel:

$$TF = 0.1 \times \frac{\sum_{I=1}^{|G|} OP_{IR} \times F_{RI}}{|G|} \tag{5.4}$$

Abordarea propusă pentru calculul încrederii unui utilizator depinde, așadar, de ceea ce crede că știe (5,5%), de ceea ce știe sistemul că știe (49,5%) și de încrederea acordată de ceilalți utilizatori (45%), rezumându-l în ecuația 5.5:

$$TotalTrust = \alpha \times TI + (1 - \alpha) \times TF, where \quad \alpha = 0.55 \tag{5.5}$$

Procentele nivelurilor de încredere după fiecare fază din ecuație 5.5 au fost evaluate stocastic pe baza presupunerii că majoritatea rău intenționată nu trebuie să influențeze decisiv încrederea totală a unui utilizator onest.

5.3 Rezultate experimenatale

În scopul testării abordării computaționale pentru încrederea în detectarea participativă, a fost luat în considerare un eșantion de 12 utilizatori și modelat matematic. Dintre acești utilizatori, 7 au fost considerați donatori și 5 au fost considerați receptori. Pentru fiecare dintre acești utilizatori a fost desemnată o valoare inițială de încredere și au fost stabilite mai multe rute generate aleatoriu pentru a calcula încrederea de feedback a utilizatorilor.

A doua fază denumită faza de învățare reprezintă un set de provocări pe care utilizatorul trebuie să le îndeplinească. A doua fază a fost, de asemenea, modelată matematic, iar profilurile utilizatorilor au fost generate aleatoriu.

Pentru faza a treia și a patra, au fost efectuate recomandări și feedback, solicitări și răspunsuri aleatorii. Aceste solicitări și răspunsuri au fost făcute în 3 pași iterativi pentru a determina exactitatea influenței utilizatorilor în raport cu alți utilizatori.

O evoluție a încrederii totale a utilizatorilor după fiecare etapă este prezentată în diagrama 5.1. Fazele sistemului prezentate sunt: inițializarea, învățarea, prima iterație a interacțiunilor, a doua iterație a interacțiunilor și a treia iterație a interacțiunilor. În această diagramă se poate observa că prima fază introduce un punct de plecare slab, dar nu poate fi eliminată deoarece este necesară pentru stabilirea provocărilor fazei a doua. După cum se poate observa în diagramă, faza a doua are un rol de catalizator pentru echilibrarea încrederii generale a utilizatorilor fără a lăsa să fie puternic influențată de recenziile bune sau rele. Următoarele trei faze reprezintă iterații în care utilizatorul interacționează și se evaluează reciproc. Faptul că celălalt utilizator nu cunoaște evaluarea celuilalt ajută la menținerea unui echilibru al încrederii. Acest lucru se realizează prin faptul că un receptor nu știe cât de mult influențează gradul său asupra încrederii totale a iterației, la fel ca și cel care oferă.

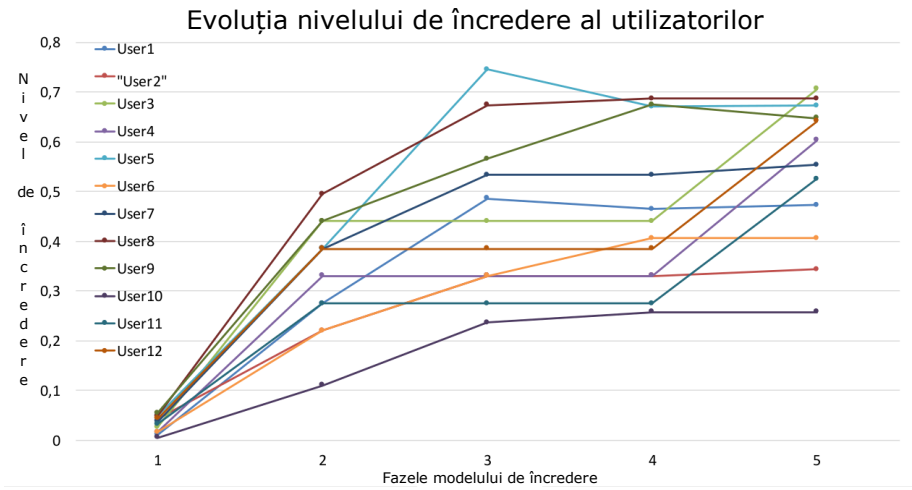

Figure 5.1. Evoluția încredrii la nivel utilizator după fiecare etapă a modelului de securitate propus.

5.4 Concluzii

În acest capitol am prezentat un nou tip de aplicație pentru optimizarea căilor folosind servicii bazate pe cloud în sisteme de detectare participativă folosind studiul de caz al reintegrării vârstnicilor. O evoluție a încrederii totale a utilizatorilor după fiecare etapă este prezentată în diagrama 5.1 unde se poate observa că prima fază introduce un punct de plecare slab, dar nu poate fi eliminată deoarece este necesară pentru stabilirea provocărilor din faza a doua. Faza a doua este importantă pentru a crea o încredere generală echilibrată a utilizatorilor. A treia și a patra fază reprezintă iterații ale interacțiunii cu utilizatorii și se evaluează reciproc, oferind feedback reciproc.

Modelul de management al încrederii propus a fost evaluat statistic. Diagrama principală arată o rețea echilibrată în care feedback-ul puternic este atenuat de istoricul utilizatorilor.

Acest capitolul a fost structurat după cum urmează: în secțiunea 5.1 am descris în detaliu managementul încrederii cu problemele sale și soluțiile propuse. Mai departe, în secțiunea 5.2 am prezentat abordarea propusă pentru gestionarea încrederii într-un sistem participativ. Rezultatele experimentale privind abordarea propusă au fost apoi discutate în secțiunea 5.3. Secțiunea finală 5.4 prezintă principalele concluzii ale soluției propuse.

6 | Securitatea în WSN

Autorii articolului [ARH19] susțin că una dintre principalele probleme ale rețelelelor de senzori fără fir este costul de calcul ridicat al nodurilor. Acest lucru, împreună cu resursele lor limitate, determină un nivel crescut de vulnerabilitate la atacuri și chiar la impactul asupra mediului.

Acest capitol introduce o metodă inovativă pentru gestionarea încrederii bazată pe lanțurile Markov pentru rețelele de senzori fără fir (Section 6.1) și o metodă adaptivă pentru managementul încrederii care ia în considerare calitatea serviciilor (Section 6.2).

6.1 Model pentru încredere și reputație bazat pe lanțuri Markov în rețele de senzori fără fir

Modelul pentru încredere propus ajută la emularea comportamentului comunicării dintre utilizatori. Această defecțiune apare ca urmare a faptului că un nod poate fi offline pentru o perioadă de timp nedefinită. Fiecare nod se defectează conform unei sume de funcții distribuite exponențial cu parametrul α și se reoperaționalizează în funcție de o sumă de funcții distribuite exponențial cu parametrul β. În sistem, fiecare nod poate avea una din cele trei stări: online, offline și volatil în care nodul s-a reactivat din starea offline, dar încă nu este disponibil pentru comunicare. Starea volatilă poate fi asimilată stării de diagnosticare a erorilor după oprirea bruscă a unui nod.

Modelul propus reprezintă o abordare optimistă și, prin urmare, acordă fiecărui nod încredere deplină atunci când intră în sistem. Valoarea de încredere și reputație a oricărui nod din sistem, la punctul de plecare, este 1.

Valoarea de încredere și reputație a unui nod din sistem pentru acest model propus este calculată numai pe baza informațiilor de primă mână. Lucrările ulterioare la modelul propus vor include analiza dacă informațiile second hand adaugă robustețe sistemului, așa cum sugerează referințele [BB03] și [MGLB00].

Pentru acest model de încredere și reputație, sugerăm utilizarea unei abordări hibride, atât de declanșare a evenimentelor, cât și de timp, pentru actualizarea încrederii unui nod. Actualizarea declanșatorului de evenimente se referă la starea oscilantă a nodului între online și offline și între stările offline și volatile. Aspectul bazat pe timp al modelului propus se referă la faptul că, dacă un nod este în starea volatilă pentru o perioadă de timp mai mare decât un prag stabilit τ, atunci acesta va fi plasat automat din nou în starea online. Împreună cu resetarea stării nodului de la volatil la online, valoarea de încredere și

reputație a nodului va fi restabilită la 1, permițând astfel unui nod să răscumpere dintr-un comportament rău. Acel comportament rău în acest model propus este reprezentat de o conexiune proastă, fie din cauze subiective, cum ar fi drenarea bateriei, fie una obiectivă, cum ar fi evenimentele meteorologice.

Timpul în care nodul este offline este considerat timp de nefuncționare. Considerăm că timpul de oprire al unui nod este conform unei sume de funcții distribuite exponențial cu parametrul β.

Parametrii β și α, pot avea fie valori fixe pe tot parcursul vieții nodului, astfel am creat două scenarii de lucru (Figure 6.1). Aceste două scenarii pot fi asimilate în viața reală cu sursa de alimentare pe care o poate avea un nod. De exemplu, parametrul fix poate fi utilizat pentru cartografierea, de exemplu, a unui nod care este alimentat în mod constant și, prin urmare, are variații mici sau nule în timpul duratei sale de viață, în timp ce un nod bazat pe baterie poate varia în funcție de curba de utilizare a bateriei.

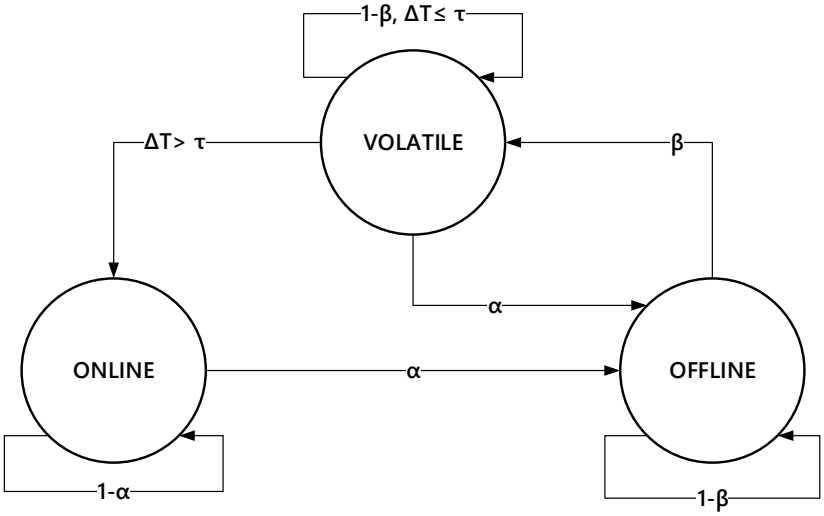

Figure 6.1. Abordarea mecanismului de securitate multi-stare. Fiecare nod se defectează cu probabilitatea bazată pe parametrul α și se reoperaționalizează cu o probabilitate bazată pe parametrul β.

În scopuri de cercetare, considerăm că doar un singur nod se recuperează odată, precum și faptul că variațiile nodurilor între starea online, offline și volatilă sunt independente și că starea unui nod nu influențează pe cea a celor din jur . Prin urmare, pentru fiecare nod i din N de noduri existente în rețea există parametrii α și β denumiți generic α_i și β_i. Premisele menționate anterior reprezintă o adaptare a unui model prezentat în [Gla14].

Având în vedere premisele anterioare, unul dintre principalele obiective ale acestui capitol este de a descoperi care este probabilitatea ca un anumit număr de noduri i, mai mic decât N, să fie online la un moment dat t în WMN. În acest sens, în primul rând am modelat WMN-ul propus ca un sistem markovian. Introducem

$$\gamma_i = \frac{\alpha_i}{\beta_i} \tag{6.1}$$

unde α_i și β_i reprezintă coeficienții funcției exponențiale distribuite, care reprezintă stările online, respectiv offline a nodurilor.

Dat fiind ecuația 6.1 și cunoscând nuărul total de noduri N din rețea, afirmăm că probabilitatea a unui nod dat i de noduri mai mic decât N, să fie online la un moment dat de tip t în conformitate cu ecuația 6.2.

$$P_i = \frac{\gamma_i}{i! \sum_{j=1}^{N} \frac{\gamma_j}{j!}} \tag{6.2}$$

Un alt obiectiv al acestei teze este de a estima care este rata medie a timpului de nefuncționare (adică numărul mediu de noduri care se defalcă pe unitate de timp), precum și rata medie de eșec pentru WMN-ul nostru dat.

Având în vedere P_N probabilitatea ca toate nodurile din rețea să fie online, atunci putem afirma că rata medie a timpului de nefuncționare ($P_{down.rate}$) poate fi calculată ca improbabilitatea ca P_N să se întâmple. Cunoscând valoarea P_N, atunci probabilitatea ca întreaga rețea să fie nefuncțională poate fi calculată folosind ecuația 6.3.

$$P_{down.rate} = 1 - P_N \tag{6.3}$$

Pentru a estima rata medie de eșec ($\lambda_{fail.rate} \epsilon [0; 1]$) a unei rețele cu un număr de noduri de N, trebuie să luăm în considerare atât timpul de nefuncționare al fiecărui nod în sistem, precum și probabilitatea de a avea i noduri online în WMN. În acest sens, folosim ecuația 6.4.

$$\lambda_{fail.rate} = \sum_{i=1}^{N} i \times \alpha_i \times P_i \tag{6.4}$$

Dacă cunoaștem procentul de timp când nodurile nu sunt disponibile, atunci putem calcula numărul mediu de noduri online din WMN așa cum se menționează în ecuația 6.5.

$$N_{avg} = \sum_{i=1}^{N} i \times P_i \tag{6.5}$$

Încercând să găsim ecuația pentru rata medie de nefuncționare, a apărut o nouă provocare. Dacă putem determina care este numărul mediu de noduri online dintr-o rețea, am putea aborda problema invers și să aflăm care ar fi numărul minim de noduri pe care ar trebui să le aibă un WMN pentru a se asigura că la un moment dat există cel puțin N noduri online? Ecuația matematică care poate estima cel mai mic număr M de noduri care pot garanta cel puțin N noduri online poate fi enunțată după cum urmează $N_{avg}(M)$
$geq N$. Calculul extins al acestei inegalități poate fi observat în ecuația 6.6.

$$\sum_{i=1}^{M} \frac{i \times \gamma_i}{i! \sum_{j=1}^{M} \frac{\gamma_j}{j!}} \geq N. \tag{6.6}$$

În continuare alegem variabila w pentru a exprima probabilitatea ca un nod offline să nu poată intra online imediat, rămânând astfel în starea volatilă. Valoarea sa poate fi calculată ca raportul ratei defalcărilor nodurilor care nu pot intra online imediat, peste rata medie totală a defalcărilor nodurilor, așa cum se arată în ecuația 6.7.

$$w = \frac{\sum_{j=1}^{N-1} \alpha_j \times P_j}{\sum_{j=1}^{N} \alpha_j \times P_j}. \tag{6.7}$$

Putem defini încrederea unui nod i într-un WMN cu M noduri, un număr mediu de N_{medie} noduri online cu o probabilitate w că, după o defalcare, nu pot deveni imediat online, după k numărul de tranziții după cum urmează în ecuația 6.8.

$$T_i^k = \frac{1}{k} \times \left((1-w) \times T_i^{k-1} + w \times \frac{N_{avg}}{M} \right) \tag{6.8}$$

6.2 Rezultate experimentale

Pentru scopul cercetării considerăm o rețea de senzori fără fir cu 10 noduri care își pot schimba starea între online și offline independent. Considerăm că fiecare dintre noduri au încredere inițială a nodului egală cu 1 ($T_0 = 1$). Adică toate nodurile pornesc de la prezumția de a fi pe deplin corecte, cu capacități de a face parte din rețea (online). Fiecare tranziție către offline și online afectează din nou fiabilitatea nodului și, prin urmare, este încrederea.

Ecuațiile propuse în secțiunea 6.1 au fost testate și validate matematic și în simulare folosind TRMSim-WSN.

În timpul validării am observat că o rată scăzută a unui eșec, indicată de o valoare scăzută a parametrului $alfa$, împreună cu o rată ridicată de recuperare, tradusă într-o valoare ridicată a parametrului $beta$, crește probabilitatea numărului de i de noduri care să fie online în rețea. Aceste rezultate ale simulării pot fi observate în Figura 6.3.

În imaginea 6.2 arătăm dependența probabilității de a avea un anumit număr de noduri online în rețea în funcție de numărul existent de noduri eșuate. După cum s-a văzut, valoarea probabilității P scade semnificativ odată cu numărul de noduri offline.

În Figura 6.4 prezentăm rezultatele obținute unde se poate observa că valoarea de încredere pentru fiecare nod scade în același mod ca și valoarea probabilității P de a avea un anumit număr de noduri online în rețeaua.

Dacă după un anumit număr de tranziții în timpul stării volatile, un nod va rămâne stabil, modelul de încredere și reputație permite posibilitatea răscumpărării prin restabilirea valorii sale de încredere la cea inițială, $T_0 = 1$. Lucrările ulterioare vor determina cât timp trebuie să fie τ pentru a reprezenta corect că un nod a devenit stabil și disponibil.

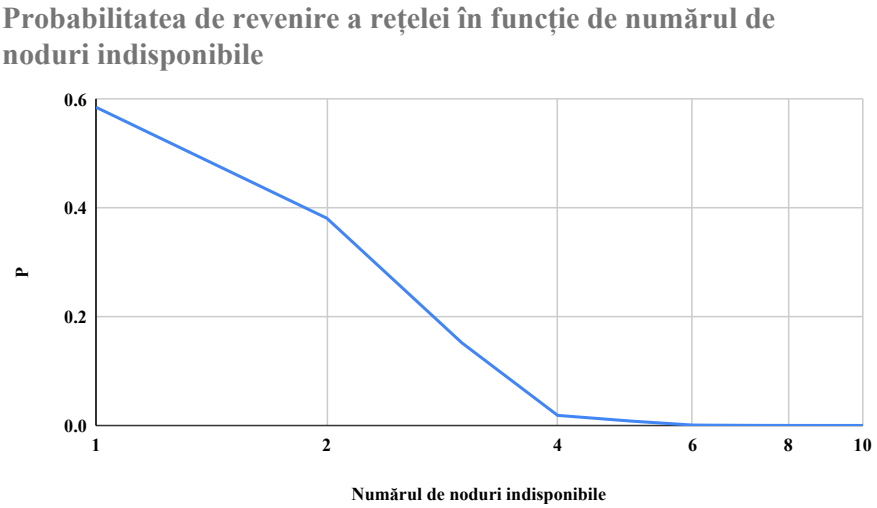

Figure 6.2. Valorile probabilității P de a avea un anumit număr de noduri disponibile în rețea ținând cont de numărul de noduri defecte.

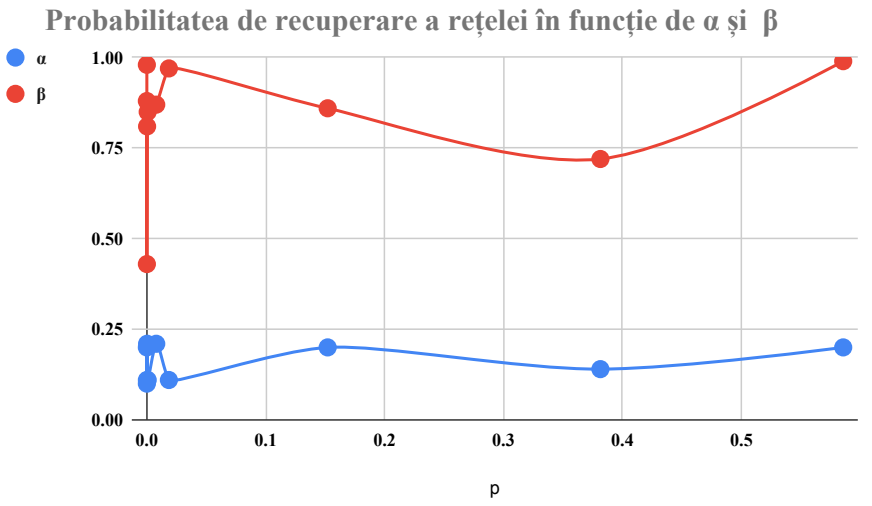

Figure 6.3. Valorile probabilității P de a avea un anumit de număr de noduri disponibile în rețea ținând cont de parametrii α și β.

6.3 Concluzii

Luând în considerare dispozitivele eterogene dintr-o rețea, împreună cu diferitele sisteme de operare și topologia în schimbare, devine dificil și consumator din punct de vedere al resurselor (timp, bani *etc.*) Implementarea modelelor clasice de securitate în ceea ce privește QoS.

În acest capitol, am demonstrat că o nouă paradigmă de securitate bazată pe încredere și reputație poate fi capabilă, astfel încât să rezolve aceste probleme într-un mod eficient. Abordarea bazată pe Markov pentru încredere și reputație în WMN propusă în această teză reușește să calculeze valorile de încredere ale nodurilor care sunt dinamice, asimetrice,

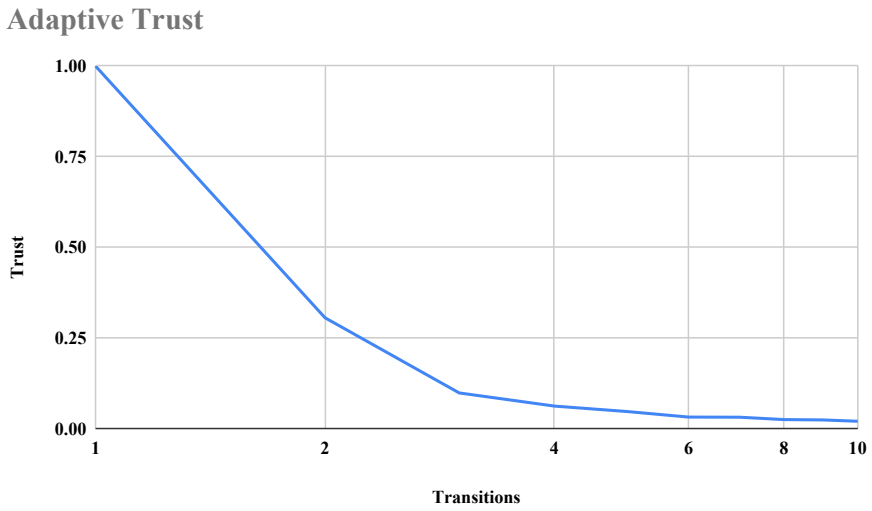

Figure 6.4. Evoluția încrederii în raport cu numărul de noduri defecte din rețea.

sensibile la context, subiective și tranzitive parțiale. Fiecare nod din sistem poate avea una din cele trei stări: online și disponibil pentru comunicare, offline și inexistent și volatil în care nodul s-a recuperat dintr-o stare offline, dar încă nu este disponibil pentru comunicare. Starea volatilă poate fi asimilată stării de diagnosticare a erorii după oprirea bruscă a unui nod. Modelul de încredere și reputație propus reprezintă o abordare optimistă și, prin urmare, acordă fiecărui nod încredere deplină atunci când intră în sistem. Valoarea de încredere și reputație a oricărui nod din sistem, la punctul de plecare, este 1. Fiecare actualizare a valorii de încredere și reputație este calculată numai pe baza informațiilor de primă mână, utilizând o abordare hibridă atât de declanșare a evenimentelor, cât și bazată pe timp pentru actualizare încrederea unui nod. Rezultatele obținute ale modelului de încredere și reputație propuse prezintă un mare potențial în ceea ce privește simulările ulterioare și determinarea acurateței algoritmului propus.

Concluziile noastre sunt următoarele: modelul de încredere este definit în secțiunea 6.1 și testat cu rezultatele prezentate în 6.2. Modelul de încredere propus consideră că factorul de adaptare, w, se schimbă în timp și acest fapt se reflectă în calculul de încredere al unui nod.

7 | Concluzii și direcții viitoare de cercetare

7.1 Concluzii

Pe parcursul anilor de cercetare al acestei teze de doctorat, am îndeplinit obiectivul fundamental și am cercetat, propus și validat unu nou model de securitate pentru rețelele mobile fără fir. Am prezentat într-un mod analitic și obiectiv o serie de soluții precum și avantajele și dezavantajele acestora.

7.2 Contribuții originale

CO1 Am propus un model de securitate bazat pe criptografie. Astfel efectuat implementarea reală și testarea a ueni serie de algoritmi criptografici în mod independent dar și în Simulatorul Sim2Car dezvoltat în cadrul Departamentului de Sisteme Distribuite din Universitatea Politehnica din București;

CO2 Am propus, implementat și testat într-un mediu simulat un model de securitate bazat pe criptografie pentru VANET;

CO3 Am propus, implementat și testat stocastic un model de încredere și reputație la nivel utilizator pentru rețelele folosind comceptul de participatory sensing. Acest model abordează încrederea utilizatorilor;

CO4 Am propus, implementat și testat stocastic și simulat un model de încredere și reputație la nivel legătură de date pentru rețelele de senzori fără fir. Acest model abordează încrederea în comunicare.

CO5 Am propus, implementat și testat stocastic și simulat un model de încredere și reputație general bazat pe un sistem markovian rețelele de senzori fără fir.

7.3 Lista publicațiilor

Rezultatele obținute în această teză de doctorat au fost prezentate comunității științifice în cadrul unor conferințe, jurnale și capitole de carte. Am publicat un număr de 7 lucrări științifice, dintre care patru ca prim autor și trei ca autor secundar. Lista

publicațiilor constă într-un capitol de carte (Advances in Mobile Cloud Computing and Big Data in the 5G Era), un articol în reviste internaționale (Information Sciences) și cinci articole în conferințe internaționale bine stabilite (International Conference on Green, Pervasive și Cloud Computing; P2P, Parallel, Grid, Cloud și Internet Computing; Conferință internațională de Testare a Software-ului și Sistemelor).

Articole științifice publicate:

1. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Pop, Florin; Mavromoustakis, Constandinos X; Mastorakis, George; "Secure Opportunistic Vehicle-to-Vehicle Communication", "Advances in Mobile Cloud Computing and Big Data in the 5G Era",229-268,2017,Springer;

2. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Mocanu, Bogdan; Pop, Florin; Cristea, Valentin; "Analysis of security approaches for vehicular ad-hoc networks", "P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on",304-309,2015,IEEE;

3. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Cristea, Valentin; "Spider: A bio-inspired structured peer-to-peer overlay for data dissemination", "P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2015 10th International Conference on",291-295,2015,IEEE;

4. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Castiglione, Aniello; "Data fusion technique in spider peer-to-peer networks in smart cities for security enhancements", "Information Sciences",479,607-621,2019,Elsevier;

5. Mocanu, Bogdan; Pop, Florin; **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Cristea, Valentin; Castiglione, Aniello; "Flaw Recovery in Cloud Based Bio-inspired Peer-to-Peer Systems for Smart Cities", "International Conference on Green, Pervasive, and Cloud Computing",338-352,2017,Springer;

6. **Mocanu (Mihăiță), Alexandra-Elena**; Dobre, Ciprian; Pop, Florin; Mocanu, Bogdan; Cristea, Valentin; Esposito, Christian; "A trust application in participatory sensing: Elder reintegration", "International Conference on Green, Pervasive, and Cloud Computing",596-610,2017,Springer;

7. **Mocanu (Mihăiță), Alexandra-Elena**; Mocanu, Bogdan; Esposito, Christian; Pop, Florin; "Trust is in the air: a new adaptive method to evaluate mobile wireless networks","IFIP International Conference on Testing Software and Systems",135–149,2020, Springer;

7.4 Lista proiectelor

Pe parcursul anilor de doctorat am participat la o serie de proiecte. Acestea mi-au oferit contextul pentru realizarea studiilor de caz reale de utilizare pentru această teză și de

asemenea, posibilitatea de a colaborare cu cercetători valoroși din acest domeniu. Acestea sunt:

1. *DataWay*: Real-time Data Processing Platform for Smart Cities: Making sense of Big Data in romanian: Platforma de procesare a datelor in timp real pentru Orase Inteligente: Dand sens Big Data., Cod proiect: PN-II-RU-TE-2014-4-2731, Perioada: Octombrie 2015 - Septembrie 2017, Director: Prof.dr.ing. Florin POP;

2. *MobiWay* - Mobility Beyond Individualism: an Integrated Platform for Intelligent Transportation Systems of Tomorrow, Cod proiect: (PN-II-PT-PCCA-2013-4-0321), Director: Prof. Dr. Ing. Ciprian Dobre

3. *Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU 187 1.5 S 155536*

Bibliography

[AHR+17] Al Amin Neaz Ahmed, HM Fazlul Haque, Abdur Rahman, Md Susam Ashraf, Sanjay Saha, and Swakkhar Shatabda. A participatory sensing framework for environment pollution monitoring and management. *arXiv preprint arXiv:1701.06429*, 2017.

[ANDK+18] Phan Minh Linh An, Thang Nguyen-Duc, Taejoon Kim, Taehong Kim, Jae-Seang Lee, and HyungSeok Choi. An enhancement of sinalgo simulator for mobile network scenario. *Wireless Networks*, pages 504–505, 2018.

[ARH19] Usama Ahmed, Imran Raza, and Syed Asad Hussain. Trust evaluation in cross-cloud federation: Survey and requirement analysis. *ACM Computing Surveys (CSUR)*, 52(1):1–37, 2019.

[BB03] Sorav Bansal and Mary Baker. Observation-based cooperation enforcement in ad hoc networks. *arXiv preprint cs/0307012*, 2003.

[BE19] BI Bakare and JD Enoch. A review of simulation techniques for some wireless communication system. *International Journal of Electronics Communication and Computer Engineering*, 10(2), 2019.

[BKL+05] Philip Baldwin, Sanjeev Kohli, Edward A Lee, Xiaojun Liu, Yang Zhao, CT Ee, Christopher Brooks, NV Krishnan, Stephen Neuendorffer, Charlie Zhong, et al. Visualsense: Visual modeling for wireless and sensor network systems. Technical report, Citeseer, 2005.

[Bou07] Athanassios Boulis. Castalia: revealing pitfalls in designing distributed algorithms in wsn. In *Proceedings of the 5th international conference on Embedded networked sensor systems*, pages 407–408, 2007.

[CBP+05] Gilbert Chen, Joel Branch, Michael Pflug, Lijuan Zhu, and Boleslaw Szymanski. Sense: a wireless sensor network simulator. In *Advances in pervasive computing and networking*, pages 249–267. Springer, 2005.

[Che15] Kahina Chelli. Security issues in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the World Congress on Engineering*, volume 1, 2015.

[Cle20] J. Clement. Mobile internet usage worldwide - statistics & facts, 2020.

[CLZ05] Elaine Cheong, Edward A Lee, and Yang Zhao. Viptos: a graphical development and simulation environment for tinyos-based wireless sensor networks. In *SenSys*, volume 5, pages 302–302, 2005.

[com20] Crypto++ community. Crypto++ library 5.6.0 release 2020, 2020.

[DBFH09] Akshay Dua, Nirupama Bulusu, Wu-Chang Feng, and Wen Hu. Towards trustworthy participatory sensing. In *Proceedings of the 4th USENIX conference on Hot topics in security*, pages 8–8, 2009.

[EÖF+09] Joakim Eriksson, Fredrik Österlind, Niclas Finne, Nicolas Tsiftes, Adam Dunkels, Thiemo Voigt, Robert Sauter, and Pedro José Marrón. Cooja/msp-

sim: interoperability testing for wireless sensor networks. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, pages 1–7, 2009.

[FFBY20] Reza Fotohi, Somayyeh Firoozi Bari, and Mehdi Yusefi. Securing wireless sensor networks against denial-of-sleep attacks using rsa cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, 33(4):e4234, 2020.

[FKFP07] Sándor P Fekete, Alexander Kroller, Stefan Fischer, and Dennis Pfisterer. Shawn: The fast, highly customizable sensor network simulator. In *2007 Fourth International Conference on Networked Sensing Systems*, pages 299–299. IEEE, 2007.

[FZC+20] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. Trust-based attack and defense in wireless sensor networks: A survey. *Wireless Communications and Mobile Computing*, 2020, 2020.

[GGD+07] Victor Gradinescu, Cristian Gorgorin, Raluca Diaconescu, Valentin Cristea, and Liviu Iftode. Adaptive traffic lights using car-to-car communication. In *2007 IEEE 65th vehicular technology conference-VTC2007-Spring*, pages 21–25. IEEE, 2007.

[Gla14] Ioannis Glaropoulos. Queuing theory 2014-exercises, 2014.

[GMMP09] Felix Gomez Marmol and Gregorio Martinez Perez. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. In *ICC IEEE*, pages 1 – 5, 07 2009.

[GNF+20] Ning Gao, Qiang Ni, Daquan Feng, Xiaojun Jing, and Yue Cao. Physical layer authentication under intelligent spoofing in wireless sensor networks. *Signal Processing*, 166:107272, 2020.

[JYX+18] Xiaojie Jin, Yingzhen Yang, Ning Xu, Jianchao Yang, Nebojsa Jojic, Jiashi Feng, and Shuicheng Yan. Wsnet: Compact and efficient networks through weight sampling. In *International Conference on Machine Learning*, pages 2352–2361. PMLR, 2018.

[JZE+19] Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Aso Mohammad Darwesh, and Mohammad Reza Meybodi. A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. *Wireless Personal Communications*, 105(1):145–173, 2019.

[KMKW11] Raphaël Kummer, Timothée Maret, Peter Kropf, and Jean-Frédéric Wagen. Freemote: A wireless sensor networks emulation system. In *Proceedings of 7th MINEMA workshop*, 2011.

[KSH+19] T. Khan, K. Singh, L. Hoang Son, M. Abdel-Basset, H. Viet Long, S. P. Singh, and M. Manjul. A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access*, 7:58221–58240, 2019.

[Lin00] John Linn. Trust models and management in public-key infrastructures. *RSA laboratories*, 12, 2000.

[LLWC03] Philip Levis, Nelson Lee, Matt Welsh, and David Culler. Tossim: Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 126–137, 2003.

[LW82] Ki-Won Lee and Kensall D Wise. Sensim: A simulation program for solid-state pressure sensors. *IEEE Transactions on Electron Devices*, 29(1):34–41, 1982.

[MD12] Alexandra Mihaita and Ciprian Dobre. Securing opportunistic vehicle to vehicle communication. In *Master thesis*, 2012.

[MDM+15] A. Mihaita, C. Dobre, B. Mocanu, F. Pop, and V. Cristea. Analysis of security approaches for vehicular ad-hoc networks. In *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pages 304–309, 2015.

[MDP+17a] Alexandra Mihaita, Ciprian Dobre, Florin Pop, Bogdan Mocanu, Valentin Cristea, and Christian Esposito. A trust application in participatory sensing: Elder reintegration. In *International Conference on Green, Pervasive, and Cloud Computing*, pages 596–610. Springer, 2017.

[MDP+17b] Alexandra-Elena Mihaita, Ciprian Dobre, Florin Pop, Constandinos X Mavromoustakis, and George Mastorakis. Secure opportunistic vehicle-to-vehicle communication. In *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, pages 229–268. Springer, 2017.

[MF09] A Marculescu and J Fontignie. Algosensim: an algorithm oriented sensor networks simulator. *Retrieved May*, 3:2009, 2009.

[MGH06] Stefan Mahlknecht, Johann Glaser, and Thomas Herndl. Pawis: towards a power aware system architecture for a soc/sip wireless sensor and actor node implementation. In *Fieldbus Systems and Their Applications 2005*, pages 129–134. Elsevier, 2006.

[MGLB00] Sergio Marti, Thomas J Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–265, 2000.

[MP09] Félix Gómez Mármol and Gregorio Martínez Pérez. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. In *2009 IEEE International Conference on Communications*, pages 1–5. IEEE, 2009.

[MPME20] Alexandra Mihaita, Florin Pop, Bogdan Mocanu, and Christian Esposito. Trust is in the air: a new adaptive method to evaluate mobile wireless networks. In *INTERNATIONAL CONFERENCE ON TESTING SOFTWARE AND SYSTEMS*. Springer, 2020.

[MTC+11] Francisco J Martinez, Chai Keong Toh, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. A survey and comparative study of simulators for vehicular ad hoc networks (vanets). *Wireless Communications and Mobile Computing*, 11(7):813–828, 2011.

[MZ12] Bartosz Musznicki and Piotr Zwierzykowski. Survey of simulators for wireless sensor networks. *International Journal of Grid and Distributed Computing*, 5(3):23–50, 2012.

[NMBG20] Henry Nunoo-Mensah, Kwame Osei Boateng, and James Dzisi Gadze. Pstrm: Privacy-aware sociopsychological trust and reputation model for wireless sensor networks. *Peer-to-Peer Networking and Applications*, pages 1–21, 2020.

[NSK+20] Muhammad Numan, Fazli Subhan, Wazir Zada Khan, Saqib Hakak, Sajjad Haider, G Thippa Reddy, Alireza Jolfaei, and Mamoun Alazab. A systematic review on clone node detection in static wireless sensor networks. *IEEE Access*, 8:65450–65461, 2020.

[PA13] M. M. Patel and A. Aggarwal. Security attacks in wireless sensor networks: A survey. In *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, pages 329–333, 2013.

[PBM+04] Jonathan Polley, Dionysus Blazakis, Jonathan McGee, Daniel Rusk, and John S Baras. Atemu: a fine-grained sensor network simulator. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, pages 145–152. IEEE, 2004.

[PCL07] Paolo Pagano, Mangesh Chitnis, and Giuseppe Lipari. Rtns: an ns-2 extension to simulate wireless real-time distributed systems for structured topologies. In *Proceedings of the 3rd international conference on Wireless internet*, pages 1–8. Citeseer, 2007.

[PRG15] Rodolfo Miranda Pereira, Linnyer Beatrys Ruiz, and Maria Luisa Amarante Ghizoni. Mannasim: A ns-2 extension to simulate wireless sensor network. *ICN 2015*, page 107, 2015.

[PS20] M Premkumar and TVP Sundararajan. Dldm: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocessors and Microsystems*, 79:103278, 2020.

[RH05] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21. ACM, 2005.

[RKMC16] Madhupreetha L Rajaram, Elias Kougianos, Saraju P Mohanty, and Uma Choppali. Wireless sensor network simulation frameworks: A tutorial review: Matlab/simulink bests the rest. *IEEE Consumer Electronics Magazine*, 5(2):63–69, 2016.

[RPH06] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing ve-

hicular communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(LCA-ARTICLE-2006-015):8–15, 2006.

[SCN+16] Thiago H Silva, CSFS Celes, J Neto, V Mota, F Cunha, A Ferreira, AIJT Ribeiro, P Vaz de Melo, J Almeida, and A Loureiro. Users in the urban sensing process: Challenges and research opportunities. *Pervasive Computing: Next Generation Platforms for Intelligent Data Collection*, pages 45–95, 2016.

[SHK+06] Ahmed Sobeih, Jennifer C Hou, Lu-Chuan Kung, Ning Li, Honghai Zhang, Wei-Peng Chen, Hung-Ying Tyan, and Hyuk Lim. J-sim: a simulation and emulation environment for wireless sensor networks. *IEEE Wireless Communications*, 13(4):104–119, 2006.

[SKA04] Sameer Sundresh, Wooyoung Kim, and Gul Agha. Sens: A sensor, environment and network simulator. In *37th Annual Simulation Symposium, 2004. Proceedings.*, pages 221–228. IEEE, 2004.

[SKS20] Jaspreet Singh, Ranjit Kaur, and Damanpreet Singh. A survey and taxonomy on energy management schemes in wireless sensor networks. *Journal of Systems Architecture*, page 101782, 2020.

[SWZ+08] Lei Shu, Chun Wu, Yan Zhang, Jiming Chen, Lei Wang, and Manfred Hauswirth. Nettopo: beyond simulator and visualizer for wireless sensor networks. *ACM SIGBED Review*, 5(3):1–8, 2008.

[Szt04] J Sztipanovits. Probabilistic wireless network simulator (prowler), 2004.

[TLP05] Ben L Titzer, Daniel K Lee, and Jens Palsberg. Avrora: Scalable sensor network simulation with precise timing. In *IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005.*, pages 477–482. IEEE, 2005.

[TRJ02] TK Tan, A Raghunathan, and Niraj Kumar Jha. Emsim: An energy simulation framework for an embedded operating system. In *2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353)*, volume 2, pages II–II. IEEE, 2002.

[VH08] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 60. ICST (Institute for Computer Sciences, Social-Informatics and ..., 2008.

[WLZN07] Hejun Wu, Qiong Luo, Pei Zheng, and Lionel M Ni. Vmnet: Realistic emulation of wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 18(2):277–288, 2007.

[WSKW09] Karl Wessel, Michael Swigulski, Andreas Köpke, and Daniel Willkomm. Mixim: the physical layer an architecture overview. In *Proceedings of the*

2nd International Conference on Simulation Tools and Techniques, pages 1–8, 2009.