CAPITOLUL I

1. INTRODUCERE

1.1. Motivaţie şi scopuri

Scopul tezei de doctorat urmăreşte abordarea unui domeniu de cercetare care a atras atenţia în ultimii ani atât mediului academic cât şi celui industrial: securitatea reţelelor mobile ad-hoc (MANET). Cercetarea în domeniul securităţii reţelelor MANET rămâne activă, în ciuda anilor de cercetare. Acest lucru se datorează în primul rând faptului că încă nu există soluţii de securitate mature şi larg acceptate, şi în al doilea rând din cauza creşterii semnificative din ultimii ani a dispozitivelor mobile de comunicaţie P2P (*peer-to-peer*) prin intermediul canalelor wireless.

Creşterea considerabilă a dispozitivelor mobile de calcul şi comunicaţie (laptop-uri, telefoane mobile, tablete, dispozitive portabile digitale) conduce la o schimbare revoluţionară în societatea informaţională actuală, în care un utilizator poate folosi mai multe platforme electronice prin care are la dispoziţie toate informaţiile necesare ori de câte ori şi oriunde este nevoie. Dispozitivele mobile devin din ce în ce mai mici, mai ieftine şi mai puternice, dar în acelaşi timp acestea pot gestiona mai multe aplicaţii şi servicii de reţea, alimentând frecvent creşterea explozivă a pieţei de echipamente mobile de calcul.

Dintre toate aplicaţiile şi serviciile ce pot rula pe dispozitive mobile, conexiunile de reţea şi serviciile de date corespunzătoare, sunt, fără îndoială, cele mai solicitate servicii de către utilizatorii mobili. În prezent, conexiunile dintre aceste dispozitive sunt realizate prin intermediul furnizorului de servicii fixe bazate pe infrastructură, sau reţele private. Există, de asemenea, situaţii în care conexiunile de reţea nu sunt disponibile într-o anumită zonă geografică, iar furnizarea serviciilor de reţea în aceste cazuri devine o adevarată provocare. Recent, au apărut noi modalităţi alternative de oferire a

acestor servicii. Acestea sunt concentrate în jurul ideii de a conecta între ele dispozitivele mobile în domeniul lor de transmisie, prin crearea automată a unei reţele ad-hoc flexibilă şi puternică. În acest fel, nodurile mobile pot comunica între ele, dar pot primi de asemenea şi servicii de internet printr-un nod intermediar.

Cum reţelele wireless continuă să evolueze, se aşteaptă ca aceste capabilităţi ad-hoc să devină din ce în ce mai importante, iar soluţiile tehnologice utilizate pentru a sprijini viitoarele cercetări în domeniu, cât şi eforturile de dezvoltare vor creşte cu siguranţă în anii următori. Două tipuri speciale de reţele mobile ad-hoc ce prezintă interes sunt cele senzoriale şi vehiculare. Reţelele senzoriale sunt compuse dintr-un număr mare de noduri de senzori de mică dimensiune folosiţi pentru monitorizarea unui anumit fenomen, în schimb ce reţelele VANET aduc avantaje în dezvoltarea aplicaţiilor de optimizare a traficului şi de creştere a siguranţei rutiere.

Deşi reţelele MANET îşi găsesc aplicaţii în multiple domenii (servicii de urgenţă, reţele de senzori, reţele militare, aplicaţii educaţionale, divertisment, reţele vechiculare), ele nu sunt încă folosite pe scară largă în special datorită vulnerabilităţilor sale de securitate, dintre care se enumeră:

- vulnerabilitatea la interferenţe, deoarece toate semnalele împart aceeaşi lăţime de bandă (un nod poate transmite la un moment dat o anumită cantitate de informaţie);
- nu poate fi folosit un protocol de securizare static datorită mobilităţii nodurilor;
- nu are un dispozitiv central de decizie, depinzând în totalitate de participarea nodurilor la activitatea reţelei;
- nodurile nu au o sursă permanentă de energie, depinzând în cea mai mare parte de acumulatori, favorizând astfel atacurile de tip DoS (refuzul serviciului).

Astfel, pentru a putea profita de avantajele certe aduse de reţelele MANET, protocoalele sale de transmisie a datelor (rutare) trebuie îmbunătăţite cu elemente de securitate. În ultimii ani unele lucrări de cercetare au propus diverse soluţii pentru sporirea nivelului de

securitate, dar multe dintre acestea prezintă anumite dezavantaje care nu le fac foarte practice în realitate.

Teza prezintă lucrările de specialitate pentru a scoate în evidenţă avantajele şi dezavantajele aduse de acestea, dar în acelaşi timp propune şi realizează propriile metode de securizare a principalelor protocoale ale reţelelor ad-hoc din diverse domenii de aplicabilitate ale acestora.

1.2. Contribuţii originale

Lucrarea realizează diferite modificări în modalitatea de funcţionare a protocoalelor de rutare OLSR (*Optimezed Link State Routing*) şi AODV (*Ad-hoc On-Demand Distance Vector*) în vederea asigurării securităţii transmisiilor informaţiilor în funcţie de categoria şi caracteristicile particulare ale acestor protocoale.

În această teză au fost prezentate şi implementate trei modele principale de securizare a protocoalelor de rutare folosite în reţelele ad-hoc mobile:

- model de securizare a protocolului OLSR ce presupune numeroase îmbunătăţiri aduse modelului prezentat de R. Song şi P. C. Mason în lucrarea „ROLSR: A Robust Optimized Link State Routing Protocol for Military Ad-Hoc Networks" (Song and Mason, 2010);
- model de securizare a protocolului AODV, care are la bază sistemele de securitate propuse în lucrările: „Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" (Guerrero-Zapata, 2006) şi „Authenticated Routing for Ad hoc Networks" (ARAN) (Sanzgiri et. Al, 2005).
- model de prevenire a unor atacuri de securitate întâlnite îndeosebi în reţelele vechiculare.

Modelul de securizare al protocolului OLSR aduce îmbunătăţiri substanţiale faţă de protocolul ROLSR prezentat de R. Song şi P. C. Mason în (Song and Mason, 2010). Sunt implementaţi

de asemenea şi algoritmii corespunzători soluţiilor propuse pentru a facilita implementarea practică a modelului de securitate.

Printre cele mai importante avantaje ale sistemul propus în această lucrare se enumeră:

- folosirea criptografiei bazate pe verificarea identităţii – *Identity Based Encryption*, în care cheia publică este înlocuită cu informaţii publice legate de identitatea utilizatorului (precum numele sau adresa de reţea). Astfel se elimină necesitatea existenţei unei infrastructuri prestabilite pentru distribuirea cheilor publice;
- protecţie sporită pentru anumite tipuri de atacuri care nu sunt suficient securizate în protocolul ROLSR: falsificarea identităţii (*identity spoofing*), falsificarea mesajelor (*message forgery*), manipularea mesajelor (*message tampering*), refuzul serviciului (*denial of service*) şi altele;
- eliminarea complexităţii administrării cheilor de criptare corespunzătoare protocolului OLSR prin implementarea unui model simplificat şi mult mai eficient de încredere între nodurile vecine.
  Acesta are la bază doi factori de reputaţie care sunt direct corelaţi cu încrederea unui nod într-o reţea ad-hoc: nivelul de activitate şi comportamentul anterior.

Totodată, modelul propus adaptează şi extinde protocolul ROLSR pentru a putea fi complet utilizabil nu doar în cadrul aplicaţiilor militare, dar şi în domeniul educaţional, al serviciilor de urgenţă, al reţelelor vehiculare etc.

Modulele principale ale sistemului propus sunt:

- administrarea cheilor;
- autentificarea nodurilor vecine;
- schema de evaluare a reputaţiei nodurilor;
- schema de control a mesajelor de autentificare;
- monitorizarea nodurilor MPR.

În cadrul acestor module sunt proiectaţi şi implementaţi numeroşi algoritmi care au rolul de a eficientiza şi securiza comunicaţia dintre nodurile participante la schimbul de informaţie din cadrul reţelei.

Dintre aceşti algoritmi, cei mai importanţi sunt:

- algoritm pentru optimizarea modalităţii de generare a cheilor distribuite;
- algoritm pentru facilitarea extragerii cheilor private de prag folosite la autentificarea nodurilor vecine;
- algoritm pentru optimizarea calculului celei mai bune rute pentru expedierea unui mesaj care va lua în considerare factorii adiţionali propuşi pentru securizarea comunicaţiei, precum reputaţia nodurilor, integritatea conexiunii wireless etc.;
- algoritm pentru procesarea mesajelor folosite în cadrul schemei de autentificare;
- algoritm pentru rutarea pachetelor în interiorul reţelei în funcţie de coeficientul de încredere calculat pentru fiecare nod în parte.

Modelul de securizare al protocolului AODV combină şi extinde modelele propuse în lucrările „Secure Ad hoc On-Demand Distance Vector (SAODV) Routing" (Guerrero-Zapata, 2006) şi „Authenticated Routing for Ad hoc Networks" (ARAN) (Sanzgiri et. Al, 2005). Aceste protocoale nu acoperă suficient procesul prin care nodurile intermediare se pot alătura reţelei în cadrul procesului de rutare.

Se deschide astfel posibilitatea lansării unor atacuri de tip *wormhole* prin care un intrus poate genera informaţii de rutare necorespunzătoare care pot avea ca efect compromiterea reţelei prin conducerea acesteia într-o stare de inconsistenţă.

Folosind criptografia bazată pe identitate, funcţii hash înlănţuite cât şi algoritmi care să detecteze tiparele clasice de comportament ale nodurilor participante la un atac de tip *wormhole*, lucrarea

implementează un sistem complex dar foarte eficient de combatere a acestor tipuri de atacuri şi a vulnerabilităţilor asociate cu acestea.

În metoda propusă se elimină constrângerea legată de existenţa unei infrastructuri de administrare a cheilor.

Totodată, în această teză sunt realizate mecanisme de securizare a unor breşe de securitate care nu au fost tratate corespunzător în cadrul protocoalelor SAODV şi ARAN. Printre cele mai importante dintre acestea se enumeră:

- scăderea numărului de hop-uri în mesajele de tip RREQ şi RREP;
- creşterea numărului de secvenţă în mesajele RREQ şi RREP;
- falsificarea mesajului RRER;
- lansarea unor atacuri de tip refuzul serviciului (*DoS*) prin trimiterea continuă sau intermitentă de mesaje de cerere RREQ.

Mecanismul de protecţie are ca scop proiectarea unei scheme de autentificare punct-la-punct a mesajelor cu scopul garantării integrităţii şi a non-repudierii. Acesta conţine diverşi algoritmi pentru:

- primirea mesajelor RREQ de la nodul sursă;
- trimiterea pachetelor RREQ;
- primirea pachetelor RREP.

Modelul de securizare al reţelelor VANET are ca scop prevenirea unor atacuri de securitate întâlnite îndeosebi în reţelele vehiculare. Dintre acestea, se remarcă atacurile de tip eliminarea pachetelor şi *black hole*. Soluţia de protecţie propusă foloseşte o schemă bazată pe mesaje de confirmare pentru a diminua pierderea informaţiilor de topologie datorată aruncării mesajelor de tip TC de către posibili atacatori. Schema adaugă două noi tipuri de pachete de control şi implementează algoritmi pentru primirea în siguranţă a mesajelor de control HELLO şi TC.

Modificările aduse sunt validate din punct de vedere al performanţei sistemului prin intermediul implementării unor scenari de test pentru protocoalele AODV şi OLSR, folosind simulatorul OPNET Modeler. Astfel, soluţiile propuse se arată a fi adecvate protejării mesajelor transmise între participanţii la trafic.

1.3. Organizarea tezei

Conţinutul lucrării dezvoltă tematica securităţii în reţelele mobile ad-hoc pe parcursul a patru capitole urmate de concluzii şi bibliografie. În fiecare capitol sunt prezentate lucrările de specialitate cât şi contribuţiile originale aduse şi sunt evidenţiate referinţele bibliografice.

În **Capitolul 1**, intitulat "**INTRODUCERE**" sunt descrise motivaţiile, contribuţiile originale cât şi organizarea tezei.

Capitolul 2, denumit "**REŢELE AD-HOC MOBILE**" descrie modurile de operare folosite în reţelele wireless cât şi în cele ad-hoc, iar apoi sunt descrise mecanismele de funcţionare ale protocoalelor de rutare studiate în această lucrare – OLSR (*Optimezed Link State Routing*) şi AODV (*Ad hoc On-Demand Distance Vector*). Pentru fiecare protocol sunt detaliate informaţii precum formatul şi dirijarea pachetelor, metodele folosite pentru detecţia legăturilor şi a nodurilor vecine, descoperirea topologiei reţelei şi calcularea tabelei de rutare. Cele mai întâlnite breşe de securitate din cadrul reţelelor ad-hoc mobile sunt detaliate în funcţie de categoria din care acestea fac parte. Scopul este de a identifica breşele de securitate prin care se pot lansa atacuri asupra protocoalelor de rutare.

Totodată sunt descrise şi principalele funcţionalităţi ale simulatorului OPNET Modeler folosit pentru a testa performanţa protocoalelor prezentate în această lucrare.

Capitolul 3, denumit "**SOLUŢII DE SECURITATE PROPUSE ÎN REŢELELE AD-HOC**", prezintă în prima parte principalele soluţii de securitate care se pot aplica reţelelor ad-hoc