Teza de doctorat propune noi mecanisme si tehnici de securitate aplicabile in Sistemele Inteligente de Transport (ITS). Lucrarea contine referinte bibliografice specifice temei abordate, dintre care 8 referinte reprezinta cele mai semnificative lucrari realizate si publicate de autor in domeniul tezei.

Lucrarea este structurata in 8 capitole.

* **Capitolul 1**, *Abstract*, ofera o imagine de ansamblu a cercetarii abordate in teza, precum si a principalelor contributii aduse de catre autor.
* **Capitolul 2**, *Introduction*, prezinta intrebarile fundamentale la care se raspunde prin cercetarea inclusa in teza si ofera astfel o justificare pentru alegerea tematicii si a relevantei in contextul domeniului. Securitatea este una dintre cele mai mari provocari intalnite in ITS. Participantii din ITS au cerinte speciale de confidentialitate, astfel incat nu numai securitatea conventionala, dar si aspecte privind intimitatea si increderea in informatie, trebuie considerate atunci cand se proiecteaza mecanisme de securitate aplicabile in ITS. Din perspectiva securitatii, setul de mecanisme propus in teza acopera urmatoarele proprietati: confidentialitate, autentificare, non-repudierea, controlul integritatii. Capitolul ofera o imagine de ansamblu a tezei atat din punctul de vedere al contributiilor cat si al impartirii pe capitole. Fiecare contributie este discutata ulterior in urmatoarele capitole ale tezei.
* **Capitolul 3,** *Security Considerations in Intelligent Transportation Systems*, analizeaza tendintele actuale de securitate din ITS. Am identificat urmatoarele taxonomii care pot fi utilizate in analiza securitatii in ITS: taxonomia provocarilor de securitate in ITS, taxonomia adversarilor si atacurilor in ITS, taxonomia amenintarilor privind confidentialitatea in ITS, taxonomia mecanismelor de prevenire in ITS. Luand in considerare taxonomiile identificate, autorul propune in teza noi mecanisme de securitate care acopera urmatoarele arii: anonimitate, model securizat pentru schimbul de date in ITS, model de incredere pentru partajarea datelor in ITS, model de agregare pentru datele criptate in ITS. In incheierea capitolului, prezentam modul in care mecanismele de securitate propuse au fost implementate in platforma colaborativa MobiWay, folosita pentru testare si evaluare. MobiWay este o platforma colaborativa deschisa, standardizata care asigura interoperabilitatea intre echipamente mobile de colectare de date si o gama larga de aplicatii ITS.
* **Capitolul 4**, *ITS participant’s anonymity requirements in ITS*, prezinta contributiile din teza ce tin de propunearea unei solutii de securitate pentru a proteja anonimitatea utilizatorilor in ITS, si, in acelasi timp, propunerea mecanismului prin care se poate verifica legitimitatea informatiilor partajate in ITS. Pentru aceasta, prezentam o schema bazata pe folosirea pseudonimelor si semnaturilor partial oarbe aplicabila in ITS. Propunem ca utilizatorii sa interactioneze cu aplicatiile ITS folosind un pseudonim in loc de identitatea lor adevarata. Folosirea semnaturilor partial oarbe impiedica utilizatorii malitiosi sa trimita cantitati mari de date false care pot duce la analize si recomandari eronate. Comparam mecanismul propus cu alte abordari din literature de specialitate: schema Fiat-Schamir, schema RSA, schema Guillou si Quisquater in vederea evaluarii performantei unor operatii specifice: generarea de semnaturi, preprocesare si validare de semnaturi. Mecanismul propus ofera rezultate mai bune in ceea ce priveste generarea de semnaturi comparativ cu restul schemelor analizate, precum si rezultate similare cu schema RSA pentru verificarea semnaturii.
* **Capitolul 5**, *User Centric Model for Sharing Data in Intelligent Transportation Systems,* prezinta contributiile din teza ce tin de propunerea unei solutii de securitate care permite participantilor ITS sa isi partajeze datele colectate in functie de propriile nevoi de confidentialitate. Mecanismul propus bazat pe politici de securitate asigura faptul ca participantii au posibilitatea de a controla accesul la date sensibile inainte ca informatiile sa fie partajate cu diferite aplicatii ITS. In acelasi timp, ne dorim ca utilizatorii sa aiba optiunea de a-si adapta si modifica politicile de securitate oricand. Mecanismul bazat pe politici de securitate asigura protectia datelor si controlul accesului la informatiile stocate, mentinand flexibilitate in ceea ce priveste schimbarile contextuale. Pentru testare, autorul a dezvoltat un sistem de navigatie ITS in colaborare cu platforma MobiWay. In experimente, am verificat ca intr-adevar aplicatia ITS utilizeaza numai datele partajate specificate de catre politicile de securitate si nimic altceva. Prin experimente am demonstrat ca aplicarea politicilor de securitate la nivelul depozitului de date specific fiecarui utilizator nu implica deteriorarea performantei timpului de executie a procesului de colectare a informatiilor in ITS.
* **Capitolul 6**, *Trust in Intelligent Transportation Systems*, prezinta contributiile din teza ce tin de propunerea unei solutii de securitate pentru determinarea nivelului de incredere in informatia partajata in ITS. In ITS, increderea in informatie trebuie sa fie stabilita in raport cu datele partajate in sistem, si nu doar considerand reputatia surselor care partajeaza date. Mecanismul propus pentru determinarea nivelului de incredere in informatie este bazat pe urmatorii parametri de calitate care descriu informatia paratajata: precizia spatiala a sursei ITS in momentul furnizarii datelor despre evenimentul ITS, apropierea temporala in momentul furnizarii datelor despre eveniment, combinate cu reputatia sursei care transmite date despre eveniment. In experimentele propuse, un eveniment observat de catre un participant trebuie sa fie confirmat de catre un numar de participanti cel putin egal cu pragul minim specific pentru eveniment astfel incat acesta sa fie publicat in sistem. Am comparat mecanismul propus cu alte solutii: principiul majoritatii, principiul celei mai de incredere surse, inferenta Bayesiana, pentru a masura performanta in termeni de evenimente valide publicate in ITS. Mecanismul propus in teza ofera rezultate mai bune comparativ cu principiul majoritatii si principiul celei mai de incredere sursa, precum si rezultate similare cu inferenta Bayesiana.
* **Capitolul 7,** *Secure aggregation with privacy considerations,* prezinta contributiile din teza ce tin de propunerea unei solutii de securitate pentru agregarea informatiilor partajate in prezenta unui agregator de date care nu este considerat de incredere. O conditie obligatorie pentru agregatorul de date este ca acesta sa poate calcula si utiliza numai rezultatul agregat obtinut de la toti participantii (si nimic altceva, cum ar fi datele utilizatorilor individuali) fara alte interactiuni cu participantii. In mecanismul de securitate propus in teza, presupunem ca agregatorul de date poate fi compromis, astfel putand furniza rezultate incorecte sau false. Participantii care partajeaza date in ITS adauga colectiv zgomot la rezultatul agregat pentru a asigura confidentialitate diferentiata. Schema propune gruparea intercalata in structura de inele a participantilor pentru a adresa eficient intrarile si iesirile dinamice specifice participantilor din ITS. Agregarea datelor combinata cu criptografia ofera avantajul de a rupe conexiunea dintre identitatea participantilor si contributia acestora Pentru a evalua mecanismul de securitate propus, analizam rezultatele acestuia in comparatie cu alte scheme existente de agregare de date. Costul de comunicatie al schemei propuse nu se modifica in functie de numarul de participanti din ITS, prin urmare, mecanismul este scalabil in sisteme mari.
* **Capitolul 8**, *Conclusions*, prezinta principalele contributii ale tezei, impreuna cu rezultatele aferente, propunand spre cercetare problematici ramase deschise in lucrari viitoare