

ABSTRACTUL TEZEI DE DOCTORAT

Impactul securității asupra performanței rețelelor de comunicații. Distribuția cuantică a cheilor.

- Simulator de Rețele Hibride -

Impact of Security on Communication Networks Performance. Quantum Key Distribution.

- Hybrid Network Simulator -

Conducător de doctorat: Prof.dr.ing. Victor CROITORU

Doctorand: Ing. Laurențiu BOICESCU

Odată cu dezvoltarea rețelelor de comunicații, dar și datorită apariției criminalității informatice, securitatea informației a devenit unul dintre principalele domenii de interes ale prezentului. Progresele recente în domeniu sunt marcate de apariția criptografiei cuantice, prin sistemele de distribuție cuantică a cheilor, reprezentând și prima aplicație practică a teoriei informației cuantice. Teza de doctorat abordează, din punct de vedere teoretic și practic, problema analizei de performanță a proceselor de securitate și a impactului securității asupra performanței rețelelor de comunicații, în vederea optimizării raportului dintre securitate și performanță. Este subliniată necesitatea unei asemenea analize, în special în contextul apariției sistemelor de distribuție cuantică a cheilor, care impun utilizarea unor canale cuantice de comunicație caracterizate prin rate de transmisie inferioare sistemelor clasice. Teza de doctorat propune o nouă metodă formală de analiză de performanță a securității prin intermediul rețelelor hibride, care combină în cadrul aceluiași model atât rețele de servire cu așteptare, destinate descrierii caracteristicilor rețelelor de telecomunicații, precum și rețele Petri stochastice generalizate, destinate descrierii abstracte a proceselor de securitate. Spre deosebire de extensiile precedente ale celor două formalisme prezentate, rețelele hibride permit descrierea de rețele Petri și de servire cu așteptare care nu doar funcționează în paralel, dar pot și interacționa reciproc. Deși rețelele hibride sunt utilizate în cadrul tezei în scopul analizei cantitative, este posibilă utilizarea acestora și în cadrul analizei calitative (a validării proceselor modelate), dar această problemă poate fi abordată ulterior în cercetare. În baza rețelelor hibride propuse, teza prezintă proiectarea și implementarea completă, de către autor, a unui simulator hibrid de performanță a rețelelor (denumit *Hybrid Network Performance Simulator*). Simulatorul, se materializează prin aproximativ 5.500 de linii de cod scrise în limbajul obiect-orientat de programare Java și reprezintă un sistem independent de platformă creat pentru a favoriza analiza de performanță a securității și în special pentru a simplifica descrierea modelelor procesului de distribuție cuantică a cheilor. Simulatorul include un nucleu, format din planificatorul central și funcțiile de generare de numere aleatoare, de analiză a evenimentelor și stocare a rezultatelor, precum și capacitățile de descriere și analiză a modelelor de rețele cu așteptare, Petri și hibride. Pentru simplificarea procesului de descriere și stocare a modelelor, simulatorul include și un interpretor pentru un limbaj obiect-orientat de modelare propus de autor, cu o sintaxă similară limbajului Java. În final, teza prezintă implicarea autorului și primele contribuții în cadrul cercetării privind analiza impactului securității cuantice asupra performanței rețelelor de comunicații, folosind simulatorul implementat.

With the development of communication networks, and also due to the emergence of cybercrime, information security has become one of the main areas of interest of the present. Recent advances in the field are marked by the emergence of quantum cryptography, through quantum key distribution systems, which are also the first practical application of quantum computing. The Ph.D. thesis deals with the theoretical and practical aspects of the performance analysis of security and the impact of security on communication networks' performance, in order to optimize the security and performance relationship. The necessity of such analysis is underlined, especially considering the emergence of quantum key distribution systems that impose the use of quantum communication channels that have transmission rates inferior to those of classical systems. The Ph.D. thesis proposes a new formal method for performance analysis through *hybrid networks*, combining in the same model both queueing networks, describing the characteristics of communication networks, and generalized stochastic Petri nets, used in the abstract description of security processes. Unlike the previous extensions of the two formalisms presented, hybrid networks allow for the description of queueing and Petri nets that not only work in parallel, but also can interact with each other. Although hybrid networks are used throughout the thesis for quantitative, performance, analysis, their use in qualitative analysis (model-checking) is also possible, although this problem can be tackled in later research. Based on the proposed hybrid nets, the thesis also presents the design and complete implementation, by the author, of a *Hybrid Network Performance Simulator*. The simulator is materialized through roughly 5.500 lines of code written in the Java object-oriented programming language and represents a platform-independent system created in order to further the performance analysis of security and specifically to simplify the description of quantum key distribution models. The simulator includes a core, consisting of a centralized scheduler, random number generation functions as well as event analysis and result storage functions, along with the capabilities to describe and analyse Queueing, Petri and hybrid network models. In order to simplify the description and storage of models, the simulator also includes an interpreter for an object-oriented modelling language proposed by the author, with a syntax similar to Java. Finally, the thesis presents the author's involvement and the first contributions in the research on the impact of quantum security on communication networks' performance, using the implemented simulator.