جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes
Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THÈSE DE DOCTORAT

Madame Nada Mouchfiq

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Mercredi 10 Mai 2023 à 16h00 au Grand amphi à l'ENSIAS

Intitulé de la thèse

NOVEL COLLABORATIVE APPROACHES FOR MOBILE ENVIRONMENT'S SECURITY

Président :

Pr. Mohamed Essaaidi, PES, Ecole Marocaine des Sciences de l'Ingénieur

Directeur de thèse :

Pr. Ahmed Habbani, PES, ENSIAS, Université Mohammed V de Rabat

Rapporteurs :

Pr. Adnane Addaim, PES, EMI, Université Mohammed V de Rabat

Pr. Mohamed Sadik, PES, ENSEM, Université Hassan II, Casablanca

Pr. Ali El Moussati, PES, ENSA, Université Mohammed I, Oujda

Examinateurs :

Pr. Moulay Driss El Ouadghiri, PES, Faculté des Sciences, Université Moulay Ismail, Meknès

Pr. Hammadi Nait-Charif, Senior Lecturer, Bournemouth University, Dorset, UK

Pr. Alberto LaCava, Full Professor, Saint Peter's University, New Jersey, USA

UNIVERSITE MOHAMMED V - RABAT ★ ENSIAS

Résumé: L'objectif de notre thèse est d'apporter des solutions aux problèmes liés à la sécurité dans les réseaux mobiles ad hoc (MANETs). Comme première proposition, nous avons adapté le principe de la technologie blockchain pour sécuriser la communication entre ses composants. Par la suite, nous avons amélioré cette idée en fonction des limites détectées en concevant un nouveau protocole intelligent multitâche sécurisé pour les réseaux ad hoc (MSPA), assurant à la fois la protection des nœuds et des données échangées. Il se compose de trois étapes principales : l'initialisation, le filtrage et l'envoi. Pour prouver l'efficacité de notre approche, nous avons effectué des analyses formelles et informelles, et estimé la complexité en termes de temps d'exécution. Ensuite, pour tester l'aspect opérationnel de notre concept, nous avons créé une version sécurisée du protocole OLSR (Optimized Link State Routing) en intégrant les algorithmes MSPA de base. Nous avons modélisé la mise en œuvre du principe de fonctionnement du MSPA-OLSR à l'aide de UML en dressant les diagrammes de classe et de séquence reflétant la mise en œuvre des différentes étapes et scénarios de notre protocole dans le simulateur de réseau NS3. Les résultats de simulation indiquent une augmentation moyenne de 48% du taux de livraison des paquets (PDR) et une croissance de 59% du débit, selon la densité du réseau, et ce en scénario d'attaque par rapport à l'OLSR standard. Nous concluons que cette nouvelle version assure la sécurité au sein du réseau attaqué avec des métriques de QoS améliorées.

Mots-clés: Analyse formelle, analyse informelle, attaques, confidentialité, disponibilité, intelligent, intégrité, non-répudiation, protocole OLSR, réseau mobile Ad hoc, sécurité.

Abstract: The objective of our thesis is to provide solutions for the problems related to security in Mobile Ad hoc Networks (MANETs). As a first proposal, we adapted the principle of blockchain technology to it to secure communication between its components. Later, we improved this idea based on its detected limitations by designing a new secure multi-tasks intelligent protocol for ad hoc networks (MSPA), ensuring both the protection of the nodes and the exchanged data. It consists of three main steps: initialization, filtering, and sending. To prove the efficacy of our approach, we performed formal and informal analyses, and estimated complexity in terms of execution time. Afterward, to test the operational aspect of our concept, we created a secure version of the Optimized Link State Routing (OLSR) standard by integrating the basic MSPA algorithms. We modeled the implementation of the operating principle of the MSPA-OLSR protocol using UML by drawing class and sequence diagrams reflecting the implementation of the different steps and scenarios of our protocol under network simulator NS3. Simulation results indicate an average 48% increase in packet delivery ratio (PDR) and an 59% growth in throughput, depending on network density vs. standard OLSR in attack scenario. We conclude that this new version provides security within the attacked network with improved QoS metrics that are better than the original one.

Keywords: Attacks, confidentiality, disponibility, formal analysis, informal analysis, integrity, mobile ad hoc networks, non-repudiation, optimized link state routing protocol, security, smart systems.