Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Monsieur SALMI SALIM

Discipline : Sciences de l'Ingénieur
Spécialité : Informatique

Sujet de la thèse

Mécanismes et techniques de sécurité à base de Deep Learning pour les attaques par déni de service dans les réseaux de capteurs sans fil

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique "

Thèse présentée et soutenue **le samedi 11 mai 2024 à 10h** à l'Ecole Nationale des Sciences Appliquées de Fès, devant le jury composé de :

NOM ET PRÉNOM	TITRE	ETABLISSEMENT	
Zakariae CHALH	PES	Ecole Nationale des Sciences Appliquées de Fès	Président
Fatima AMOUNAS	PH	Faculté des Sciences et Techniques d'Errachidia	Rapporteur
Youssef FARHAOUI	PH	Faculté des Sciences et Techniques d'Errachidia	Rapporteur
Faycal MESSAOUDI	PH	Ecole Nationale de Commerce et de Gestion de Fès	Rapporteur
Anass EL AFFAR	PH	Faculté Polydisciplinaire de Taza	Examinateur
Nabil EL AKKAD	PH	Ecole Nationale des Sciences Appliquées de Fès	Examinateur
Mohamed BENSLIMANE	PH	Ecole Supérieure de Technologie de Fès	Examinateur
Lahcen OUGHDIR	PES	Ecole Nationale des Sciences Appliquées de Fès	Directeur de Thèse

Laboratoire de recherche : Ingénierie, Systèmes et Applications
Etablissement : Ecole Nationale des Sciences Appliquées de Fès

Résumé de la thèse

Les réseaux de capteurs sans fil (RCSF) sont essentiels à l'écosystème de l'internet des objets (IoT). Cependant, ils sont confrontés à d'importants problèmes de sécurité, en particulier la menace d'attaques par déni de service (DoS). Dans ce réseau complexe, chaque capteur contribue à un écosystème dynamique, et le risque croissant d'attaques par déni de service met en évidence la nécessité de stratégies innovantes pour renforcer la sécurité des RCSF à l'ère des connexions intelligentes. Dans un premier temps, nous nous sommes attachés à relever les défis uniques posés par la rareté des données au sein des RCSF. Nous avons créé un ensemble de données réelles simulées dans un environnement RCSF et lancé divers scénarios d'attaque pour classer les paquets de données. Ce travail préparatoire a jeté les bases d'une étude approfondie des attaques DoS. Pour améliorer nos systèmes de défense, nous avons incorporé des modèles avancés d'apprentissage profond tels que les réseaux neuronaux profonds, les réseaux neuronaux récurrents et un modèle hybride qui combine des données spatiales et séquentielles. Ces protecteurs numériques, soutenus par une approche robuste d'ingénierie des données, peuvent détecter et neutraliser efficacement les menaces potentielles pour la sécurité. Grâce à nos recherches approfondies, nous avons développé un cadre de méta-apprentissage pour améliorer l'adaptabilité et la réactivité de notre système de sécurité. Cette approche innovante permet aux systèmes de procéder à des ajustements intelligents malgré des données limitées. Nos méthodes ont fait l'objet d'une évaluation rigoureuse basée sur des critères académiques établis tels que les taux de détection et la précision, et les résultats ont mis en évidence la robustesse et l'efficacité de notre approche. En conclusion, notre thèse contribue de manière significative au domaine en constante évolution de la sécurité des réseaux de capteurs sans fil (RCSF). Elle joue un rôle crucial dans l'élaboration et l'avancement des cadres de sécurité au sein des réseaux de capteurs sans fil.

Mots clés : Réseaux de capteurs sans fil, attaques par déni de service, rareté des données, modèles d'apprentissage profond, menaces de sécurité, cadre de méta-apprentissage.