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

Monsieur Otmane EL MOUAATAMID

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Lundi 31 Juillet 2023 à 11h00 au Grand Amphi à l'ENSIAS

Intitulé de la thèse

Cybersecurity and Reliability of the Internet of Things based on Combinatorial Designs and Error-Correcting Codes

Devant le Jury composé de:

Président:

Pr. Ahmed Tamtaoui, PES, Institut National des Postes et Télécommunications, Rabat

Directeur de thèse:

Pr. Mostafa Belkasmi, PES, ENSIAS, Université Mohammed V de Rabat

Co-Encadrant de thèse :

Pr. Mohamed Lahmer, PH, EST, Université Moulay Ismail, Meknès

Rapporteurs :

Pr. Ahmed Tamtaoui, PES, Institut National des Postes et Télécommunications, Rabat

Pr. Abdallah Rhattoy, PES, EST, Université Moulay Ismail, Meknès

Pr. Abdellatif Kobbane, PES, ENSIAS, Université Mohammed V de Rabat

Examinateur :

Pr. Moulay Ahmed Faqihi, PES, ENSIAS, Université Mohammed V de Rabat

UNIVERSITE MOHAMMED V - RABAT
ENSIAS

Résumé : Cette thèse de doctorat explore le potentiel des codes correcteurs d'erreurs et des designs combinatoires pour améliorer la cybersécurité et la fiabilité des systèmes de l'Internet des objets (IoT), en mettant l'accent sur les systèmes de communication de I'IoT. Alors que l'IoT continue de se développer dans des domaines tels que la santé, les maisons intelligentes et l'industrie, il apporte à la fois des opportunités et des défis, y compris des vulnérabilités en matière de sécurité, des problèmes d'évolutivité du réseau et de congestion du réseau.

Cette thèse étudie les défis de sécurité auxquels est confrontée l'infrastructure de l'IoT, en particulier dans les systèmes de communication de l'IoT tels que les réseaux de capteurs sans fil (WSN) et les technologies d'identification par radiofréquence (RFID). Différents vecteurs d'attaque et faiblesses inhérentes rendant ces systèmes susceptibles d'être violés sont identifiés. Pour relever ces défis, la thèse propose l'utilisation de One-Step Majority-Logic Decodable (OSMLD) codes basés sur les designs combinatoires.

Une analyse complète est présentée, mettant l'accent sur l'application des codes OSMLD pour atténuer les lacunes de sécurité au niveau de la couche physique des systèmes IoT et améliorer la fiabilité du système. De nouveaux codes OSMLD dérivés de designs combinatoires, en particulier les plans en bloc incomplets équilibrés (BIBDs) tels que les designs ovales, les designs unitaux et les designs de Denniston, sont construits et validés. Ces constructions servent de base pour développer un nouveau schéma d'authentification de groupe scalable qui prend en charge la tolérance aux pannes.

Les codes OSMLD dérivés sont connus par leur compromis entre performances et complexité, ce qui les rend adaptés aux appareils IoT en raison de leur faible complexité et de leur processus de décodage facile. Cette thèse contribue à la fiabilité et à la sécurité des systèmes IoT en construisant de nouveaux designs combinatoires, en particulier des BIBDs pour développer les codes OSMLD. Ces codes abordent efficacement les problèmes de sécurité et de fiabilité au niveau canal de communication dans les applications IoT, réduisant ainsi les lacunes de sécurité.

Les recherches de cette thèse fournit des solutions pratiques pour la mise en œuvre de ces codes dans les applications IoT. Les résultats offrent des indications précieuses aux personnes intéressées par la mise en œuvre et l'adoption de codes correcteurs d'erreurs et de designs combinatoires dans les systèmes IoT, ce qui permet d'avancer la fiabilité et la sécurité des systèmes IoT à l'avenir

Mots-clés: Codes correcteurs d'erreurs, Codes OSMLD, Designs Combinatoires, Plans en blocs incomplets équilibrés (BIBD), Internet des objets (IdO), Fiabilité de l'IdO, Sécurité de l'IdO, Authentification de groupe

Abstract: This Ph.D. thesis investigates the potential of error-correcting codes and combinatorial designs in enhancing the cybersecurity and reliability of Internet of Things (IoT) systems, specifically focusing on IoT communication systems. As the IoT continues to expand in domains like healthcare, smart homes, and industry, it brings both opportunities and challenges, including security vulnerabilities, network scalability issues, and network congestion.

The thesis explores the security challenges faced by IoT infrastructure, particularly in IoT communication systems such as Wireless Sensor Networks (WSNs) and Radio-Frequency Identification (RFID) technologies. It identifies various attack vectors and inherent weaknesses that make these systems susceptible to breaches. To tackle these challenges, the thesis proposes the utilization of One-Step Majority-Logic Decodable (OSMLD) codes based on combinatorial designs.

A comprehensive analysis is presented, focusing on the application of OSMLD codes to mitigate security gaps at the physical layer of IoT systems and enhance system reliability. New OSMLD codes derived from combinatorial designs, specifically Balanced Incomplete Block Designs (BIBDs) like Oval designs, Unital designs, and Denniston designs, are constructed and validated. These constructions serve as the foundation for developing a new scalable group authentication scheme that supports fault tolerance.

The derived OSMLD codes are known for their performance-complexity trade-off, making them suitable for IoT devices due to their low complexity and easy decoding process. This thesis contributes to the reliability and security of IoT systems by constructing new combinatorial designs, particularly BIBDs, and leveraging them to develop OSMLD codes. These codes effectively address security and reliability issues at the physical layer in IoT applications, thereby reducing security gaps.

Furthermore, the research provides practical solutions for implementing these codes in IoT applications. The findings offer valuable insights for individuals interested in implementing and adopting error-correcting codes and combinatorial designs in IoT systems, ultimately advancing the reliability and security of IoT systems in the future.

Keywords: Error-Correcting Codes, One-Step Majority-Logic Decodable (OSMLD) codes, Combinatorial designs, Balanced Incomplete Block Designs (BIBDs), Internet of Things (IoT), IoT Reliability, IoT security, Group Authentication