AVIS DE SOUTENANCE D'UNE THESE DE DOCTORAT

Le Doyen de la Faculté des Sciences a le plaisir d'informer le public qu'une soutenance de thèse de Doctorat en

«Mathématiques, Informatique et Applications»

aura lieu le 30/11/2023 à la Faculté des Sciences, Kénitra

La Thèse sera présentée par Mr EBOBISSE DJENE YVES FREDERIC

Sous le thème :

Contribution to Wireless Sensor Networks and IoT Security: Challenges and Energy Cost Assessment

Devant le jury composé de :

Nom et Prénom	Titre	Etablissement
ABOUCHABAKA JAAFAR	**Président**	**Faculté des sciences, Kénitra**
AMNAI MOHAMED	**Rapporteur**	**Faculté des sciences, Kénitra**
HICHAM GHENIOUI	**Rapporteur**	**FST, Fès**
EL HADDADI ANAS	**Rapporteur**	**ENSA AL-Hoceima, Abdelmalek Essaâdi University**
PIERRE MARTIN TARDIF	**Examinateur**	**Université de Sherbrooke**
EL BHIRI BRAHIM	**Co-Directeur de thèse**	**EMSI de Rabat**
FAKHRI YOUSSEF	**Directeur de thèse**	**Faculté des sciences, Kénitra**

قطب الدراسات في الدكتوراه
PÔLE DES ETUDES DOCTORALES

المملكة المغربية
وزارة التعليم العالي والبحث العلمي والابتكار

Nom et Prénom : EBOBISSE DJENE YVES FREDERIC
Date de soutenance : 30/11/2023
Directeur de Thèse : FAKHRI YOUSSEF

Sujet de thèse

Contribution to Wireless Sensor Networks and IoT Security: Challenges and Energy Cost Assessment

Résumé:

L'internet des objets et les réseaux de capteurs sans fil font de plus en plus partie intégrante de la vie quotidienne. Ils couvrent de nombreux domaines d'applications allant de l'agriculture à la médecine en passant par les maisons connectées, l'industrie 4. 0 et le domaine militaire entre autres. Ces technologies reposent sur des terminaux ayant des ressources limitées (capacité de calcul, de mémoire, batteries, etc..) les rendant ainsi vulnérables à de multiples attaques de la part de personnes mal intentionnées d'autant plus qu'elles sont davantage exposées à l'internet. Il est donc important de mettre en place des mécanismes de sécurité adaptés tenant compte des caractéristiques de ces environnements, ceci au travers d'algorithmes de cryptage, de hachage légers afin de garantir plusieurs objectifs sécuritaires tels que la confidentialité, l'intégrité et l'authentification. En comparant des algorithmes de chiffrement connus (DES, AES, etc..) et de hashage (MD5, SHA256), nos travaux étudient l'impact et les coûts induits par ces mécanismes de sécurité sur les réseaux de capteurs sans fils et IoT en terme d'énergie consommée et de durée de vie : premier nœud mort, dernier nœud mort, nombre de nœuds vivants, énergie moyenne consommée. Les simulations effectuées portent tour à tour sur des nœuds individuels, des réseaux centralisés (single hop) et des clusters de réseaux sans fils (multihop) sous Contiki Cooja puis MATLAB..

Abstract:

The Internet of Things and wireless sensor networks are becoming more commonplace. They span a wide range of applications, including agriculture, medical, linked homes, industry 4.0, and the military. These technologies are built on terminals with limited resources (computing capacity, memory, batteries, and so on), rendering them vulnerable to repeated attacks by malevolent individuals, particularly as they become more connected to the Internet. It is also critical to implement proper security mechanisms that take these environments' peculiarities into consideration, such as lightweight encryption techniques and hashing, to ensure many security objectives as confidentiality, integrity, and authentication. Our research compares the impact and costs of well-known encryption techniques (DES, AES, etc.) and hashing algorithms (MD5, SHA256) on wireless and IoT sensor networks in terms of energy spent and lifetime: first dead node, final dead node, number of living nodes, average energy consumed. Individual nodes, centralized networks (single hop), and clusters of wireless networks (multihop) were all simulated using Contiki Cooja and subsequently MATLAB.