**Nom et Prénom : SAIDI HANANE**
**Date de soutenance : 24/10/2020**
**Directeur de Thèse : A. ADDAIM**

***Sujet de Thèse :***

**Opportunistic routing and game theory for wireless sensor networks**

***Résumé :***

Les réseaux de capteurs sans fil (RCSF) sont des solutions intelligentes pour les applications de communication, telles que le suivi et la surveillance des comportements. Le RCSF est confronté à de nombreux défis qui ralentissent les performances de ces réseaux de capteurs. L'un des principaux défis est l'allocation des ressources et la sécurité, en particulier lorsque les capteurs sont utilisés pour surveiller les éléments sensibles. Afin d'améliorer l'allocation des ressources et la sécurité dans les réseaux de capteurs, nous suggérons d'utiliser un routage opportuniste où chaque capteur envoie des données ou des paquets sur un support dynamique vers la destination. Par conséquent, chaque paquet peut choisir un chemin différent vers la destination. Nous suggérons également une approche de théorie des jeux pour améliorer l'allocation des ressources et la prévention des noeuds malveillants. De plus, des simulations mathématiques ont été menées pour évaluer les performances de la théorie des jeux en termes de sécurité et d'allocation des ressources.

Nous allons d'abord passer en revue l'environnement des réseaux de capteurs sans fil ainsi que l'application des WSN dans différents domaines tels que les utilisations médicales, l'agriculture, les fins militaires, puis nous passerons en revue les protocoles de routage opportuniste et les différences par rapport aux protocoles de routage traditionnels. Le routage est une tâche délicate dans les réseaux de capteurs sans fil, la conception d'un protocole pour WSN est plus difficile que la conception d'un protocole pour un réseau normal. Dans WSN, cela nécessite une économie d'énergie des capteurs, la sécurité du réseau et la durée de vie. La prise en compte de nombreux paramètres et la gestion des ressources en fait partie. L'objectif principal du routage est de sélectionner le chemin pour transmettre les données d'un noeud à un autre. La sélection de la route signifie la meilleure route pour tous les noeuds. La transmission des données est basée sur la sélection du saut suivant. Dans le routage traditionnel, la sélection est effectuée de manière proactive au niveau du noeud émetteur avant la transmission. Ce type de routage ne tient pas compte de la nature du support réseau, alors que le routage opportuniste ou OR utilise la nature de diffusion de WSN pour transmettre des données, il est effectué par le noeud qui est le plus proche de la destination.

Deuxièmement, nous allons passer en revue la théorie des jeux qui est une branche des mathématiques appliquées, elle a différentes utilisations en économie militaire et en sociologie dans WSN, elle a montré des résultats importants en termes d'allocation des ressources, de gestion de réseau et de sécurité du réseau, ce qui a attiré notre attention de l'utiliser comme modèle pour l'associer à un routage opportuniste pour rendre le réseau plus fiable et plus sûr le routage opportuniste tracera le chemin pour transmettre les données d'une seule main La théorie des jeux fera coexister les noeuds avec des problèmes que le réseau peut rencontrer tels que des intrusions manque d'énergie Dans ce but, nous avons proposé un modèle pour minimiser le coût des noeuds en termes d'énergie et de transmission de données.

***Abstract :***

Wireless Sensor Networks (WSNs) are smart solutions for communication applications, such as behaviour tracking and monitoring. WSNs are facing many challenges that slow down the performance of these sensor networks. One of the main challenges is resource allocation and security, particularly when sensors are utilized to monitor sensitive items. In order to improve the resource allocation and the security in sensor networks, we suggest to use opportunistic routing where each sensor sends data or a packet over a dynamic medium to the destination. Therefore, each packet can choose a different path to the destination, we also suggest a game theory approach to improve resource allocation and malicious nodes

prevention. Moreover, mathematical simulations have been conducted to evaluate the performance of game theory in terms of security and resource allocation.

First we will overview the Wireless Sensor Networks environment as well as the application of WSNs in different areas such as medical uses, agriculture, military purposes then we will review the opportunistic routing protocols and the differences compared to traditional routing protocols. Routing is a delicate task in wireless sensor networks, designing a protocol for WSN is difficult than designing a protocol for a normal network in WSN, it requires energy saving of the sensors, network security and lifetime. Thus designing a routing protocol should take into consideration numerous parameters and resource management is one of them. The main goal of routing is selecting the path to transmit data from a node to another. Selecting the route means the best route for all the nodes. The data forwarding is based on selecting the next hop. In traditional routing the selection is done proactively at the sender node before the transmission; this type of routing doesn't consider the nature of the network medium, whereas opportunistic routing or OR uses the broadcasting nature of WSN to transmit data it is done by the node which is more close to the destination.

Second, we will overview game theory which is on the other hand a branch of applied mathematics, it has different uses in economics, military and sociology. In WSN It has shown important results in terms of resource allocation, network management and network security which has drawn our attention to use it as model to associate it with opportunistic routing to make the network more reliable and safe. Opportunistic routing will draw the path to forward data first then game theory will make nodes coexist with problems that the network may face such as intrusions lack of energy and others. For this purpose we have suggested a model to minimize the cost for nodes in terms of energy and data transmission and malicious intrusions sur DDoS attacks in perspective.