ABSTRACT

Wireless Sensor Networks (WSN) are becoming more and more popular everyday due to their increasing ability to monitor certain phenomenon over wide regions such as air pollution, natural disaster, industrial monitoring, underwater applications and medical care [1] [2].

The lack of a sophisticated security mechanisms for the nodes in the sensor network makes it a favourable target for external attacks, where an attacker can compromise some of the node(s) in the sensor network. Afterwards, the attacker may start altering the data received or sent by these nodes, before forwarding it to the other nodes in effort to prevent the destination from properly decoding or reading the received data.

These attacked nodes become compromised and will cause tremendous amount of unusable data to flow within the network, which will negatively impact the energy efficiency of the network and its overall performance.

This thesis proposes a technique that can detect and exclude these malicious nodes based on a *cooperative local voting approach with a dynamic centre* taking into consideration the aggressiveness of the attack, and it studies the impact of the technique on the amount of aggregated data by the network, and the time required to deliver the sensors data.

This thesis also studies the impact of the proposed technique on the total amount of energy consumption in the network, taking into consideration the different wireless technologies such as ANT, Low-Energy Bluetooth, Wi-Fi, etc…

The simulation of the proposed technique showed that the degree on which the efficiency of the network improved, depended mainly on the underlying wireless technology of the network and the timespan of which, the data is gathered from the network.

Arabic Abstract
الملخص العربي

تزداد شعبية شبكات الاستشعار اللاسلكية WSNs يوما بعد يوم نظرا لدورها المتصاعد على مراقبة بعد الظواهر على مساحات واسعه مثل تلوث الهواء، الكوارث الطبيعية، المراقبة الصناعية، التطبيقات تحت المائية والتطبيقات الطبية.

مقدرة الحماية البسيطة المتوافره للعقد في شبكة الاستشعار يجعلها هدف سهل للهجوم من قبل الغرباء حيث يستطيعون الاستحواذ على بعد العقد في الشبكه وتغيير المعلومات التي تقوم بإرسالها أو استقبالها مع باقي العقد في الشبك، بهدف منع مكان الوصول من ترجمة أو قراءة المعلومات بشكل صحيح.

هذه العقد التي تم مهاجمتها تؤدي إلى انتشار كم هائل من البيانات الغير صالحة للإستخدام عبر الشبكة مما يؤثر بشكل سلبي على كفائة الشبكة في استخدام الطاقة.

الرسالة تقدم تقنية تقوم بإكتشاف هذه العقد التي تم مهاجمتها وتقوم بعزلها من الشبكة باستخدام تقنية تصويت محلي مشترك بمركز متحرك. ثم يتم دراسة تأثيرها على كمية البيانات المجمعة في الشبكة والوقت المطلوب لتوصيلها إلى المكان المقصود.

يتم أيضًا بعد ذلك دراسة تأثير التقنية المقترحة على الطاقة الكلية المستخدمة من قبل الشبكة لأكثر من تقنية لاسلكية مثل ANT، Low-Energy Bluetooth، Wi-Fi

محاكاة التقنية المقترحة اظهر ان درجة تحسن كفاءة الشبكة اعتمدت في الأثاث على التقنية اللاسلكية المستخدمة في الشبكة والفتره الزمنية التي تقوم الشبكة فيها بجمع المعلومات .