حماية آليات التوجيه في شبكات الاستشعار اللاسلكية ذات الكفاءة في استخدام الطاقة

ياسر رزيق سعيد السليهبي

الدكتور/ محمد حسيب ظفر

المستخلص

انتشرت في الالفية الجديدة شبكات الاستشعار اللاسلكية، وهي شبكة من أجهزة الاستشعار يتم استخدامها للأغراض العسكرية وتطبيقات المراقبة. وهي محدودة الموارد من حيث الطاقة وحجم الذاكرة والقدرة على إجراء الحسابات والاتصال مع بعضها البعض. وأهم مورد من هذه الموارد هو الطاقة لأنه استهلاكها بشكل حاد يؤثر على الشبكة ككل. آليات التوجيه في هذه الشبكة تنقسم إلى ثلاثة أقسام وهي الاليات المسطحة والاليات المجمعة والاليات المعتمدة على الموقع. وأفضلها من حيث عدم استهلاك الطاقة هي الاليات المجمعة. ويوجد العديد من آليات التوجيه المجمعة ولكنها معرضة إلى العديد من الهجمات وتفتقر إلى الحماية، ولذلك في هذه المقترح البحثي اقتراح عمل إصدار من هذه الآلية تحتوي على طبقة حماية مع الأخذ بالاعتبار مشكلة استهلاك الطاقة.

SECURE ROUTING MECHANISMS FOR ENERGY EFFICIENT WIRELESS SENSOR NETWORKS

Yasser Rozeq Alselehibi

Supervised By
Prof. Dr. Mohammad Haseeb Zafar

ABSTRACT

The technology revolution in wireless communications and micro-electro-mechanical systems (MEMS) has a direct impact on wireless sensor network (WSN) development. WSNs collect and process data from an area of interest. WSNs can be used for several application areas, such as the military, home, or environment. These devices typically have limited computing power and are designed to operate on batteries. Consequently, routing protocols that are applied to other networks cannot be used for WSNs. Many routing protocols for WSNs have been proposed, but none has made security a goal. This makes them easy targets for attacks. It is important to apply some level of security, so that WSNs are difficult to attack, especially when they are used in critical applications. One of the best categories of routing networks in WSNs is hierarchical protocols (cluster-based), where sensor nodes divided into small groups are an effective technique to achieve power savings, scalability, and routing. One of the well-known protocols in this category is the Low Energy Adaptive Clustering Hierarchy (LEACH). However, LEACH is vulnerable to many attacks. A LEACH protocol that achieves the desired security goals while keeping an acceptable level of energy consumption is a challenging task in WSN. The Enhancing Secure LEACH Protocol (MS-LEACH) is a modified version of LEACH with cryptographic protection against outsider attacks. MS-LEACH enhances security in LEACH but increases power consumption. To counter the power consumption in secure LEACH protocols, while keeping an acceptable level of security, we propose Secure Lightweight LEACH (SLW-LEACH). The simulation results of the proposed SLW-LEACH outperform MS-LEACH protocols, in terms of energy consumption, network lifetime, network throughput, and normalized routing load.