وزارة التعليم العالي والبحث العلمي
جـامعة الموصل
كلية علوم الحاسوب والرياضيات

نموذج مقترح لكشف العقد الخبيثة على أساس تقنية المناعة في شبكة الاستشعار اللاسلكية

حنان أنس قاسم

رسالـة ماجسـتير
علـــوم الحاســـوب

بإشراف

د.معن يونس عبد الله

مدرس

١٤٣٥هـ ٢٠١٤م

المستخلص

تُعَد شبكات الاستشعارات اللاسلكية مصدرا مهما لدراسة وتحليل البيانات. وفي كثير من الأحيان تنتشر هذه الشبكات في مناطق يصعب الوصول إليها بغرض رصد محيط كل منها، وتوليد القراءات المرصودة، لتسليمها إلى كيان مركزي ولتحليل المزيد من البيانات, العقد هي أجهزة استشعار صغيرة ذات موارد محدودة لتنفيذ جميع عملياتها التحسسية، وينبغي المحافظة على حياتها بأكملها, إن تطبيقات شبكات الاستشعار اللاسلكية مثل مراقبة ساحة المعركة، ومراقبة حرائق الغابات، هي من المهام الحرجة في الطبيعة, فإن التوقيت والدقة في إيصال البيانات الحسية تكون مهمة لغرض الكشف الناجح لحدث معين. ولذلك، فمن الضروري حماية هذه الشبكات من الهجمات الخبيثة التي يمكن أن يشنها الخصم، بقصد التقليل أو التعطيل من كفاءة الشبكة.

إن هجمات حجب الخدمة تعرف على انها الهجمات التي تنطلق من نهايات متعددة من شبكة الاستشعار اللاسلكية نحو مجموعة من عقد الاستشعار الطبيعية، بقصد إستنزاف موارد الطاقة المحدودة لها, هذه الهجمات لها تأثيرٌ كبيرٌ على أداء الشبكة، وتؤدي في النهاية إلى اختراق كافة عقد الاستشعار للشبكة. وعواقب مثل هذا الهجوم، إذا لم يتم كشفه فإنه يمكن أن يؤدي إلى توقف عمليات الشبكة بالكامل.

وفي هذه العمل قُدم نموذج للكشف عن هجمات حجب الخدمة بوصفها مشكلة لتمييز الأنماط، فضلا عن اقتراح أساليب للكشف عن مثل هذه الهجمات, وتم تنفيذ العمل بإستخدام خوارزمية ال LEACH بروتوكول وتطبيق المحاكاة بإستخدام الNS2. وبعدها تم تطبيق خوارزميات نظام التمييز المناعي الاصطناعي ومقارنتها مع خوارزميات إصطناعية أُخر بإستخدام تطبيق الweka من خلال عمل ستراتيجيات التدريب والإختيار في التصنيف. أثبتت التجارب إنه قد حصلنا على أفضل دقة تصنيف من خلال تطبيق خوارزمية AIRS Parallel. حيث حصلنا على دقة تصنيف ٨٨.٧٥٢٪ عند تطبيقها على بيانات التدريب و٨٩.٣٣١٪ عند تطبيقها على بيانات الاختبار.

Ministry of Higher Education
& Scientific Research
University of Mosul
College of Computers Sciences
and Mathematics

Proposed Model for Detection Malicious Node Based on Immunity for Wireless Sensor Networks

Hanan Anas Kasim

M.Sc./Thesis
Computer Science

Supervised By
Dr.Maan Younes Abdullah
Teacher

2013 A.D **1435 A.H**

Abstract

Wireless sensor networks have emerged as a significant source for the study and analysis of data from the environment. These networks are deployed in harsh and inaccessible environments with the purpose of monitoring their respective surroundings, and generating observed readings, for delivery to a centralized entity, for further data analysis. Sensors nodes are tiny devices with limit available resources for performing all their sensory operations, and be sustained for their entire lifetime. Applications of wireless sensor networks such as battlefield monitoring and bushfire monitoring are mission-critical in nature. The timeliness and accuracy in the delivery of the sensory data affects several mitigation efforts that may be launched upon successful detection of a particular event in the environment. Therefore, it is essential to protect such networks from malicious attacks that may be launched by the adversary-class, with the intent of causing loss to the network operations.

Denial of Service attacks are defined as attacks launched from multiple ends of a wireless sensor network towards a set of legitimate sensor nodes, with the intent of exhausting their limited energy resources. These attacks can be significantly affect the performance of the network, and eventually lead to complete compromise of all sensor nodes of the network. The consequences of such an attack, if left undetected, can be catastrophic to the operations of the entire network.

In this study, we model denial of service attack detection as a pattern recognition problem, and propose techniques for detecting such attacks. It is implemented in the Low Energy Adaptive Clustering Hierarchy protocol and applies simulation in NS-2. Artificial Immune Recognition System model and compared it with other artificial algorithm using WEKA by made training and testing strategy for classification. Experiment provided that we get best accuracy from applying AIRS Parallel algorithm. We get ٪۸۸,۷۵۲ accuracy when applying the algorithm on the training data and ٪۸۹,۳۳۱ when applying the algorithm on the testing data.