وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

تطوير نموذج تصنيف لنظام كشف التطفل في شبكات الاستشعار اللاسلكية

رسالة مقدمة

الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل

كجزء من متطلبات نيل شهادة ماجستير علوم في

علوم الحاسوب

من قبل

سرى صباح ابراهيم الشريفي

بأشراف

أ.د. مفاز محسن خليل العنزي

1444هـ 2023م

الخلاصة:

حظيت شبكات الاستشعار اللاسلكية (WSNs) باهتمام كبير، مما أدى إلى تطبيقها في العديد من المجالات، بدءًا من التطبيقات العسكرية إلى حماية البيئة. تتكون شبكات WSN من العديد من عقد الاستشعار التي ستتواصل عبر قناة لاسلكية وتقوم بمعالجة البيانات ومهام الاستشعار الموزعة للعديد من التطبيقات المهمة. سيؤدي استخدام هذه المستشعرات إلى زيادة سلامة الطرق السريعة وبقاء الحياة البرية وتقليل وقت الاستجابة للكوارث. يمكن أيضًا نشرها كشبكات استشعار مخصصة للعديد من التطبيقات لتوفير مراقبة مستمرة وكثيفة مكانيًا للأنظمة البيئية والبيولوجية والاصطناعية.

شبكات الاستشعار اللاسلكية (WSNs) عرضة لأنواع مختلفة من التهديدات الأمنية التي يمكن أن تقلل من أداء الشبكة بأكملها؛ والتي قد تؤدي إلى مشاكل قاتلة مثل هجمات رفض الخدمة (DoS) وهجمات التوجيه وما إلى ذلك. لا يمكن لبروتوكولات إدارة المفاتيح وبروتوكولات المصادقة والتوجيه الآمن توفير الأمان لشبكات WSN لهذه الأنواع من الهجمات. ولكن يعتبر نظام كشف التطفل (IDS) هو الحل لهذه المشكلة. يقوم بتحليل الشبكة عن طريق جمع كمية كافية من البيانات ويكتشف السلوك غير الطبيعي لعقدة المستشعر.

تحلل هذه الرسالة التحديات، والقضايا الأمنية الرئيسية، والانتهاكات الأمنية في شبكات الاستشعار اللاسلكية بناءً على تحليل بروتوكول التسلسل الهرمي للتكتل التكيفي منخفض الطاقة (Leach)، وهو بروتوكول توجيه قائم على الكتلة عن طريق تغيير عدد المجموعات لمراقبة التأثير على أداء شبكة الاستشعار من حيث عمر الشبكة وتبديد الطاقة وكمية البيانات التي تصل إلى المحطة الأساسية.

تم تحديد مخطط لجمع البيانات باستخدام لغة ماتلاب ثم معالجتها لإنتاج 22 ميزة. تم اطلاق تسمية مجموعة البيانات المجمعة WSN-DS عليها. تم تدريب SVM(Support Vector Machine) على مجموعة البيانات لاكتشاف نوعين من هجمات DoS المختلفة وهي هجوم الثقب الاسود وهجوم الحوض. أظهرت النتائج أن WSN-DS حسّن قدرة IDS لتحقيق معدل دقة تصنيف أعلى. كانت دقة تصنيف الهجمات 100٪، 98٪، 98٪ للاتصالات العادية والاتصالات التي تحوي هجومي الثقب الأسود وثقب الحوض.

Developing a Classification Model For WSN-IDS

A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Master of Science
in
Computer Science
By

Sura Sabah Ibrahim ALsherifi

Supervised by

Prof. Dr. Mafaz Mohsin Khalil Alanezi

1444 A.H. **2023 A.D.**

Abstract

wireless sensor networks (WSNs) have gotten much interest, which has led to a lot of areas for those applications, from martial applications to the ecological protection. In the future, WSNs are expected to consist of many sensor nodes that will communicate over a wireless channel and perform data processing and distributed sensing tasks for many critical applications. Using these sensors will increase highway safety, wildlife survival, and reduce disaster response time. They can also be deployed as dedicated sensor networks to many applications to provide continuous and spatially intensive monitoring of ecosystems, biological and anthropogenic.

wireless sensor networks (WSN) is susceptible to various types of Security risks that can reduce performance of the whole network; Which can lead to severe issues such as denial of service (DOS) attacks, direct attacks, etc. Secure key management, authentication, and routing protocols. WSNs cannot provide security from these types of assaults. However, the intrusion detection system solves this problem. Network analyzes by compilation enough amount of data and discover the anomalous behavior for the sensitive node.

The sensitive nature of the information collected makes security in these private networks a major concern. Because of the antagonistic feature of their deployment environments, wireless environment, and the resource-limiting nature of the small sensors used in such networks, security poses more serious challenges compared to traditional networks. As attacks on any part of the hardware or software may lead to severe damage to these networks. Attackers can gain access to the nodes and extract all confidential information. They can also discard or modify the data. Attackers can also target routing information that could mislead network traffic.

Thesis analyzes challenges, key security issues, and security breaches in wireless sensor networks based on analysis of low energy adaptive

cluster hierarchy (Leach), a block-based routing protocol by changing the number of groups to monitor the impact on sensor network performance on the one hand network life with dissipation. Power and the amount of data arriving at the base station.

A scheme was defined to collect and then process data to produce 22 features. It is named WSN-DS. The support vector machine (SVM) has been trained on the dataset to discover two different types of DOS attack which are black hole attack and sink attack. results showed that WSN-DS improve the ability of IDS to achieve a higher classification accuracy rate. The accuracy of classifying attacks was 100%, and 98% and 98% for normal, black hole and sink attacks.