Cross-Layer Intrusion Detection System for Wireless Sensor Networks

Manal Al-harthi

A thesis submitted for the requirements of the degree of Master of Science

Supervised By

Dr.Manal Abdullah

Faculty of Computing and Information Technology
KING ABDULAZIZ UNIVERSITY
JEDDAH-SAUDI ARABIA
28 February 2019

Cross-Layer Intrusion Detection System for Wireless Sensor Networks

Manal Al-harthi

ABSTRACT

Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a field to collect information about surrounding environment. Their distributed nature, multi-hop data forwarding, and open wireless medium are the factors that make WSNs highly vulnerable to security attacks at various levels. WSNs are particularly vulnerable to various attacks at different layers of the protocol stack. Many Intrusion Detection System (IDS) have been proposed to secure WSNs, but all these systems operate on a single layer of OSI model. This research developed a new IDS based on cross layer interaction between Network, and Mac layers of OSI model. This new Cross-Layer IDS (XLID) is checked against other traditional (non-cross-layered) IDS that are based on single layer protocol. For this purpose, a simulator was built specifically for simulating the proposed approach. XLID showed its superiority in terms of number of detected intruders, power consumption, and throughput, over other non-cross-layered IDS. Based on the results XLID enhanced the intrusion detection rate by 42% on average, 75% higher throughput to base station, and a 23% reduction of power consumption compared to non-cross-layered IDS. Moreover, the total energy saved during simulation time ranges from 25% up to 45% compared to non-cross-layered IDS. Findings pointed out that, the detection rate at Network layer

ranges from 5% up to 18% compared to non-cross-layered IDS, while it is from 2% up to 15% in the MAC layer. However, all attacks were being detected at MAC layer, while only Blackhole attack violate the rule and showed 5% higher in non-cross-layered IDS.

نظام اكتشاف التطفل عبر الطبقات لشبكات الاستشعار اللاسلكية

منال الحارثي

المستخلص

{ إن شبكة المجسات اللاسلكية تتكون من مجموعه من المجسات والموزعه بطريقه معينه وضمن حقل معين بحيث تتحسس هذه المجسات القراءآت المختلفة من الطبيعة المحيطة بها. إن الطبيعة الموزعة لهذه المجسات وطريقة نقلها للبيانات بالاضافة الى الوسط الذي تتواجد فيه يجعلها عرضة للاختراقات والهجمات الخارجية وعلى مستويات مختلفه.

ان انظمة اكتشاف الاختراقات تلعب دورا كبيرا في اكتشاف ووقاية شبكة المجسات اللاسلكية من الهجمات الامنية، حيث تتعرض هذه الشبكة لعدة هجمات وعلى طبقات مختلفة من برتوكول الاتصال المعتمد لهذه المجسات. إن معظم أنظمة اكتشاف الاختراقات والهجمات توفر بيئة آمنه لهذه المجسات ولكن على مستوى طبقة واحده من برتوكول الاتصال المفتوح (OSI)وقد لا تهتم كثيرا الى التفاعلات التي تحدث بين طبقات الاتصال المختلفه.

يهدف هذا البحث الى تطوير نظام اكتشاف الاختراقات والذي يعتمد على التقاطع بين طبقة الشبكات وطبقة الماك التابعتين لبرتوكول الاتصال المفتوح (OSI). هذا النظام التقاطعي والذي

يدعى (XLID) تم فحصه والتحقق منه من خلال مقارنته بأنظمة اكتشاف الاختراقات التقليدية والمعتمده على الطبقه المفرده. ولهذا الغرض تم بناء محاكي خاص لهذا النوع من طرق اكتشاف الاختراقات. ان نظام (XLID) اثبت تفوقه في مجال عدد الاكتشافات ، استهلاك الطاقه ، والانتاجيه للرسائل الخارجه من المجس الى القاعدة المستقبله، مقارنة بأنظمة اكتشاف الاختراقات التقليدية والمعتمده على الطبقه المفرده.

بالاعتماد على نتائج المحاكاة زاد معدل اكتشاف الاختراقات بنسبة ٤٢%، زيادة ما نسبته ٧٥% من انتاجية الرسائل الى قاعدة الاستقبال، وتخفيض في استهلاك الطاقة بلغ ٢٣% مقارنة بأنظمة اكتشاف الاختراقات التقليدية والمعتمده على الطبقه المفرده. بالاضافة الى انه مقدار المحفوظ من الطاقه خلال فترة المحاكاة بلغ من ٢٥% الى ٤٥% مقارنة بأنظمة اكتشاف الاختراقات التقليدية والمعتمده على الطبقه المفرده. اشارت النتائج الى ان معدل اكتشاف الاختراقات في طبقة الشبكات قد تم زيادته بمعدل من ٥% الى ١٨%، كما ان معدل الزيادة في الاكتشافات في طبقة الماك بلغ من ٢% ولغاية ١٥%. اضف الى ذلك ان جميع انواع الاختراقات في طبقة الماك تم اكتشافها، بينما جميع الاختراقات تم اكتشافها في طبقة الشبكات باستثناء Blackhole او الثقب الاسود حيث كان معدل اكتشاف هذا النوع من الاختراقات اضعف بمعدل ٥% مقارنة بأنظمة اكتشاف الاختراقات التقليدية والمعتمده على الطبقه المفرده.

أخيرا ، قمنا بقياس دقة النظام المقترح والمعتمد على تقاطع الطبقات وكذلك دقة النظام المتعارف عليه لاكتشاف الاختراقات وذلك بالاعتماد على عدد الهجمات التي تم التعرف عليها او التي لم يتم التعرف عليها ، بمعنى اخر معدل الاصابة والخطأ. لقد وجدنا أن النظام المقترح حقق دقه مقدارها ٩٠% مقارنة مع ٧٤% للنظام التقليدي المعتمد على طبقة واحده}

نظام اكتشاف التطفل عبر الطبقات لشبكات الاستشعار اللاسلكية

منال الحارثي

بحث مقدم لنيل درجة الماجستير في علوم الحاسب
(علوم حاسب)

باشراف الدكتورة
د.منال عبد الله

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
جماد الثاني ١٤٤٠هـ – فبراير 2019 م