الجمهورية العربية السورية
جامعة البعث
كلية الهندسة المعلوماتية
قسم هندسة النظم والشّبكات الحاسوبية

تحسين نظام التشغيل في شبكة الحسّاسات

"Enhancement Operating System in Sensor Networks"

رسالة أعدت لنيل درجة الماجستير في هندسة النظم والشّبكات الحاسوبية

إعداد:

المهندس محمد غازي الهلامي

إشراف:

الدكتور المهندس أكرم المرعي

أستاذ مساعد في قسم هندسة النظم والشّبكات الحاسوبية – جامعة البعث

١٤٣٨ هـ – ٢٠١٦ م

الملخص

تعد شبكات الحسّاسات اللّاسلّكيّة واحدة من أهم الموضوعات البحثية الحالية وذلك لاتساع مجالات تطبيقاتها.حيث تتألف الشبكة من مجموعة من عقد الاستشعار اللّاسلّكيّة الّتي هي عبارة عن أجهزة صغيرة الحجم محدودة الطاقة والذاكرة والقدرة الحسابية،وبوجه عام نظراً لطبيعة الشبكة الّتي تنشر في الأماكن الغير مراقبة في الطبيعة فإنها تكون عرضة لمجموعة من الاعتداءات الأمنيّة،وهذه الاعتداءات من الصعب الحماية منها وتتطلب آليات أمنية فعالة،وإحدى هذه الحلول الأمنيّة هو نظام كشف الاختراق والذي يشكل خط الدفاع الثاني بالشّبكة.ويعتمّد على مبدأ أن عقد الاستشعار الّتي تكون قريبة مكانياً من بعضها البعض يكون لديها سلوك مماثل من حيث كمية إرسال البيانات واستقبالها،ويختلف هذا السلوك بشكل كبير عن العقد المجاورة في حال كان هناك عقد مهاجمة داخل الشبكة.

في هذه الأطروحة قمنا بتحليل أعراض ثلاثة من الهجمات الّتي تصيب شبكات الحسّاسات اللّاسلّكيّة وهي هجوم الإرسال الانتقائي(Selective Forwarding) وهجمات التشويش الإذاعي(Jamming) وهجوم فيضان حزم الترحيب(hello flooding)،وقمنا بمحاكاة نظام الكشف أولي يعتمد على مبدأ التعاون بين العقد من أجل الكشف عن هذه الهجمات،ويعمل هذا النظام على منصة نظام التشغيل الخاص بشبكة الحسّاسات اللّاسلّكيّة (TinyOS)،حيث إنّ النظام الذي تمّ محاكاته يحوي خيارين الأول (Standalone) من أجل عملية الكشف المحلي مع الجيران المباشرين للعقدة أما الخيار الثاني(Collaboration) من أجل التعاون مع العقد المجاورة والتي تبعد عن هذه العقدة بمقدار قفزة أو قفزتين.

وباستخدام المحاكي (TOSSIM) قمنا بمحاكاة نظام كشف الاختراق على العقد من نوع (Micaz) ودراسة أهم المقاييس الّتي تستخدم في تقييم أداة هذا النظام.وأظهرت النتائج أن تقنية كشف الاختراق المتعاونة (Collaboration) تمّتلك دقة عالية في الكشف عن هجمات (الإرسال الانتقائي،هجمات التشويش،هجوم تدفق حزم الترحيب) بالمقارنة مع نظام الكشف المستقل (Standalone).

الكلمات المفتاحية: شبكات الحسّاسات اللّاسلّكيّة،الاعتداءات الأمنيّة،نظم كشف الاختراق،محاكي الشبكة TOSSIM

Abstract

Wireless Sensor Network (WSN) is an emerging important research area.Nowadays the wireless sensor networks a wide spread applications.The Wireless Sensor Nodes is a tiny device with limited energy,memory,transmission range,and computational power.Because WSNs in general and in nature are unattended and physically reachable from the outside world,they could be vulnerable to some attacks.These forms of attacks are hard to protect against and require intelligent prevention methods.Intrusion Detection in Wireless Sensor Networks is valuable security measure.The Intrusion Detection Systems(IDS) in wireless sensor networks explores the principle that sensor nodes situated spatially close to each other tend to have similar behavior.A node is considered malicious if its behavior significantly differs from its neighbors.

In this thesis we analyze symptoms of three kinds of attacks that affect the wireless sensor networks (Selective Forwarding Attacks,Jamming Attacks and Hello Flooding Attack).We simulation an intrusion detection system which employs the neighbor-based detection technique.The system was designed to works with TinyOS operating system.

The intrusion detection system comes in two modifications – one with local knowledge of immediate neighbors only and one involving information exchanged among 1-hop or 2-hop neighbors.Collaboration is employed in order to refine information about the activity of neighboring nodes.We evaluated accuracy of the technique in detection of selective forwarding,jamming and hello flood attacks.

The results show that the neighbor-based intrusion detection technique is highly accurate,especially in the case when collaboration among neighboring nodes is used.Using the TOSSIM simulator,we evaluated the detection accuracy of the intrusion detection system for a given application scenario.

Keywords:**Wireless Sensor Networks,Security Threats,Intrusion DetectionSystem,TOSSIM Network Simulator**