استخدام شبكات SDN لاكتشاف البرمجيات الخبيثة والحد من انتشارها في الشبكات واسعة النطاق

غدير عبيد الشريف

إشراف:

أ.د. أحمد محمد مصطفى برناوي

المستخلص

في شبكة واسعة النطاق ، تنتشر البرمجيات الخبيثة في الشبكة بسرعة مؤثرة بشكل كبير وسلبي على توفر الخدمات، مما يجعل انتشار هذه البرمجيات الخبيثة واحدة من أكثر المشكلات إلحاحًا التي يجب حلها فيما يتعلق بالنواحي الأمنية للشبكات. في السنوات الأخيرة ، تعتبر الشبكات المعرفة بالبرمجيات (SDN)تقنية واعدة لتسهيل إدارة الشبكة بالإضافة إلى تحسين أمان الشبكة. البنية المميزة لشبكات SDNتساهم في عملية تنفيذ القواعد الامنية للشبكة بشكل أسرع وأقل تكلفة مقارنة بالشبكات التقليدية. بالإضافة إلى ذلك، هذه البنية المميزة لشبكات SDNتوفر رؤية مركزية لمستوى التحكم بحالة الشبكة وأنواع البيانات المارة من خلالها، وكذلك توفر إمكانية برمجة تطبيقات أمنية لأنواع مختلفة من الهجمات. تواجه أنظمة الدفاع الحالية المستندة إلى SDNالعديد من التحديات مثل دقة الكشف المنخفضة واستهلاك موارد المتحكم وكذلك مشكلة نقطة الفشل الواحدة. في هذا البحث ، نقوم بتطوير إطار عمل موزَّع يعتمد شبكات SDN متعددة وحدات التحكم. بحيث يكون هذا النظام قادر على اكتشاف الهجمات في الشبكات ذات حركة المرور الضخمة بشكل فعال وبدون التأثير على سرعة مرور البيانات فيها. يجمع النظام بين دمج تقنيات التعلم الذاتي والتقنيات الاحصائية للحصول على اعلى دقة كشف ممكنة وكذلك سرعة اكتشاف تهديدات عالية. تُظهر التجارب أن نظامنا يمكنه أن يكتشف الهجوم بفاعلية مع انخفاض شديد في كل من الإنذار الخاطئ وتأخير الكشف.

Software-Defined Network (SDN) Approach to Detect and React to Malware Propagation in Large-Scale Network

Ghadeer Obaid Alsharif

Supervised By: Prof. Ahmed Barnawi

ABSTRACT

In a large-scale network, the network intrusion deploys quickly and has a significant impact on the availability of services, making the spread of intrusions one of the more pressing problems to be solved in network security. Recent years, software-defined networking (SDN) considered a promising technology to facilitate network management as well as enhance network security. Due to the SDN architecture, it provides a global and centralized view of network states to the con- troller. As well as the programmability support the application of different security defence for variant types of attacks. The existing SDN-based defence systems face many challenges such as low detection accuracy due to the high false alarms, controller overhead and single point of failure. In this research, we develop a distributed framework based on SDN multi-controller able to detect attacks on high volume traffic networks. The system combines machine learning detection method and statistical detection methods to provide accurate detection accuracy with minimum controller response time as possible. The experiments show that our system can effectively detect the attack with an extremely low of both false alarm and detection delay.