العنوان: الحد من هجمات الروبوتات باستخدام تعليم الآله في الشبكات المعرفة بالبرمجيات

اسم الطالبة: خلود شينان سعيد الشهري

المشرف الرئيسي: د. خالد الصبحي

المشرف المساعد: أ.د احمد الزهراني

المستخلص:

على مدى العقد الماضي، نما الأنترنت وغير العالم بشكل كبير، مما تسبب في نمو كبير في الهجمات الإلكترونية. يمثل الأمن السيبراني أحد اخطر التهديدات للمجتمع ويكلف ملايين الدولارات كل عام. تعد شبكات البوت نت مسؤوله عن معظم هجمات الانترنت على الشبكات التقليدية وأصبحت اليوم مصدر القلق الرئيسي واحد أكبر التهديدات علي الشبكات المعرفة بالبرمجيات. الشبكات المعرفة بالبرمجيات هي تقنيه شبكات جديدة تجعل برمجه الشبكات أسهل من خلال فصل مستوي البيانات عن مستوي التحكم. وهذا يجعل مستوي التحكم مستقلا ومركزيا للتحكم بالشبكة. تم اقتراح عده طرق لاكتشاف وتخفيف هجمات الروبوتات في الشبكات المعرفة بالبرمجيات، ولكن التحديات لاتزال قائمه. تعتمد طرق اكتشاف الروبوتات على ميزات تدفق حركه المرور التي تعتمد على حساب الميزات الإحصائية لكل تدفق حركه مرور وهذه الطرق تتفادي تقنيات الاكتشاف بأساليب مختلفة. الهدف من هذه الأطروحة هو اقتراح نظام امن يكتشف بكفاه هجمات الروبوتات ويخففها تلقائيا في الشبكات المعرفة بالبرمجيات. يطبق النظام الامن مرحلتين: المرحلة الاولي هي نموذج تصنيف اكتشاف الروبوتات المستند الي الرسم البياني المسمى (البوت سورد). والمرحلة الثانية هي التحقق من صحة نموذج (البوت سورد) المدرب في بيئة الشبكات المعرفة بالبرمجيات مع الحفاظ على الاداء العالي، وتحسين النطاق الترددي، وانخفاض تكاليف المعالجة، بالإضافة الي الحظر التلقائي لجميع المضيفين المصابين لتقليل عدد المضيفين المصابين ومقدار تلف الشبكه. اظهر نموذج (البوت سورد) مقاييس ادا ممتازة (في الدقة، الاسترجاع، الضبط، الكفاءه الكلية) أكثر من ٩٩٪ وخطأ منخفض بنسبه ٠.٠٠٢٪ حيث تم تقييمها على مجموعه بيانات معياريه. بعد ذلك تم التحقق من صحة النموذج في بيئة الشبكات المعرفة بالبرمجيات، اظهر نموذجنا نفس الأداء الممتاز في جميع المقاييس مع أكثر من ٩٩٪ وخطأ منخفض بنسبه ٠.٠٠٩٪ وتحسن في استخدام النطاق الترددي بحوالي ٩٠٪ واستخدام اقل لوحده المعالجة المركزية. هذا التحسين متوقع لأن نظامنا يكتشف الروبوتات ويمنعها من التواصل مع مضيفين آخرين.

الكلمات المفتاحية: البوتنت، الشبكات المعرفة بالبرمجيات، الرسم البياني ، تعلم الآلة

Title: Botnet Mitigation based on Machine Learning in Software Defined Networks

Student name: Khlood Shinan Alshehri

dvisor: Dr. Khalid Alsubhi

Co-Advisor: Prof. Ahmed Alzahrani

Abstract

Over the past decade, the internet has grown and changed the world tremendously, which has caused significant growth in cyber attacks. Cybersecurity represents one of the most serious threats to society and costs millions of dollars each year. Botnets are responsible for most internet attacks on conventional networks and have become the main concern and one of the biggest threats to software-defined networking (SDN). SDN is a new networking technology that makes networks easier to program by separating the data plane from the control plane. This makes the control plane independent and centralized for network control. Several methods have been proposed to detect and mitigate botnet attacks in SDN, but the challenges still exist. These methods of botnet detection based on NetFlow traffic features rely on computing statistical features of flow traffic and avoid detection in different ways. The aim of this thesis is to propose a secure system that efficiently detects botnet attacks and automatically mitigates them in the SDN. The secure system employs two phases: The first phase is the graph-based bot detection classification model called BotSword, and the second phase is validating the trained BotSword model in the SDN environment with maintaining high performance, bandwidth improvement, and low processing overhead, as well as automatically blocking all infected hosts to minimize the number of infected hosts and the amount of network damage. The proposed BotSword model showed excellent performance metrics (accuracy, recall, precision, and F1_score) over 99% and a low FPR of 0.002% evaluated in the CTU-13 dataset. Following validating in the SDN environment, our model showed the same excellent performance in all metrics with over 99%, a low FPR of 0.009%, improvement in bandwidth utilization of around 90%, and minor CPU utilization overhead. This enhancement is possible because our system detects bots and prevents them from communicating with other hosts.

Key Word: *Cybersecurity, Botnet, software-defined networking (SDN), Graph fea- tures, Machine Learning*