عنوان الرسالة: المصادقة المستمرة بين الأجهزة باستخدام تعلم الآلة لإنترنت الأشياء
للطالبة: أسماء مسعد سعيد السفري
بإشراف: د. سهير ظافر الشهري

انترنت الأشياء هو تقنية حديثة تقدم تطورا في العديد من المجالات. هذا التطور السريع يزيد من عدد الأجهزة المستخدمة وكمية البيانات السرية المتبادلة عبر الشبكة مما يسبب زيادة عدد الهجمات الأمنية. المصادقة كإحدى تقنيات الأمان الأساسية، هي عملية التحقق من صحة الهوية المقدمة. المصادقة الأولية عند بداية كل اتصال تعد غير كافية حيث يمكن اختراق الجلسة وإحداث عدد من الهجمات وكشف الخصوصية. من هنا تظهر الحاجة لتطبيق المصادقة المستمرة خلال مدة الاتصال. المصادقة المستمرة للأجهزة مطلب أساسي حيث يتم تبادل بيانات حساسة وذات قيمة عالية. نظرا للتنوع في الأجهزة والاختلاف فيما بينها ومحدودية موارد الطاقة والمعالجة، لا تزال المصادقة المستمرة للأجهزة بحاجة للمزيد من البحث والدراسة.
في هذه البحث، نتدارس المصادقة المستمرة من جهاز إلى جهاز باستخدام تقنيات التعلم الآلي لاكتشاف الأجهزة غير الشرعية. وأيضا نقدم نظرة عامة شاملة على بيئة إنترنت الأشياء، والمصادقة في إنترنت الأشياء، وتحديات التي تواجه عملية المصادقة. نبحث أحدث تقنيات المصادقة بما في ذلك المصادقة المستمرة من جهاز إلى جهاز ونناقش مزاياها وقيودها. علاوة على ذلك، ندرس تواقيع الأجهزة اللاسلكية التي تستخدم كبصمة فريدة للأجهزة. بصمة الترددات اللاسلكية للأجهزة (RFF) تمثل الاختلافات الدقيقة في الإشارات المرسلة وهي تمثل تغييرات مميزة في عينات الطور (I) والطور التربيعي (Q) حيث يتم إرسال الإشارة عبر دائرة الإرسال.
في هذه الرسالة، نقترح نموذج مصادقة مستمرة من جهاز إلى جهاز لأجهزة إنترنت الأشياء الذي يستخدم التعلم العميق ويعتمد على (RFF) للكشف عن الأجهزة غير المشروعة. يتم تغذية إشارات التردد اللاسلكي المرسلة بشكل متكرر أثناء الجلسة إلى نموذج التعلم العميق للتحقق من شرعية جهاز الإرسال. توضح النتائج التجريبية أن نهجنا يمكّن من تحديد أجهزة إنترنت الأشياء غير المصرح بها من خلال المصادقة المستمرة لجهاز الإرسال عبر (RFF)، وبالتالي التخفيف من انتحال هوية الأجهزة وحفظ خصوصية الأفراد والمؤسسات. بالإضافة إلى ذلك، لا يحتاج نموذجنا (RFF) للمهاجمين أثناء تدريب النموذج. قمنا بتقييم أداء نموذجنا فيما يتعلق بالصحة والدقة والاستدعاء ودرجة- ف يصل إلى ٩٩.٦٤٪، ٩٩.٣٠٪، ٩٩.٦٥٪ على التوالي.

DEVICE-TO-DEVICE CONTINUOUS AUTHENTICATION USING MACHINE LEARNING FOR THE INTERNET OF THINGS

By: Asmaa Masad S Alsefri
Advisor: Suhair Alshehri

Device-to-device (D2D) authentication is a fundamental security requirement that cannot be neglected in Internet of Things (IoT) environment. Usually, devices are authenticated statically at the beginning of the session. Session impersonation is one of the issues that arise with static authentication. Continuous authentication, in which the entity is continuously authenticated at a given frequency throughout a session, is an efficient solution that overcomes this vulnerability.

Artificial intelligence in IoT security solutions safeguards communications and improves the identification and prediction of attacks. Coupled with edge computing, it can result in improved performance and decreased latency. However, edge-based D2D continuous authentication with machine learning is still in its early stage.

In this thesis, we provide a comprehensive review of the IoT environment, authentication in IoT, and authentication challenges.

Furthermore, we investigate wireless device signatures that are robust against rogue agents, namely Radio Frequency Fingerprinting (RFF) to identify devices. We propose a D2D continuous authentication model for IoT devices that uses deep learning and RFF to detect illegitimate devices. The transmitted radio frequency signals are fed frequently during the session to the deep learning model to check the transmitter device's legitimacy.

Experimental results demonstrate that our model performance, in terms of accuracy, precision, recall, and F-score, achieve 99.65%, 1.0, 99.30%, and 99.64% respectively. The process of detecting a frame group takes into account environmental conditions, real-time sensing, and validation. This reduces latency so that the process of verifying each frame group takes less than 0.019s.