باحثون يطورون وسيلةً جديدةً لحماية شبكات الجيش

حقوق الصورة: CC0 Public Domain.

طور باحثو الجيش الأميركي خوارزميةً جديدةً لحماية الشبكات من خلال السماح بالكشف عن السلوكيات العدائية التي قد تفوّتها الأساليب التحليلية الحالية؛ الفكرة الرئيسية هي بناء شبكةِ درجةٍ أعلى للبحث عن أي تغيير دقيق في تدفق البيانات قد يشير إلى نشاطٍ مشبوه.

تتبنى معظم الطرق التحليلية الحالية شبكات الدرجة الأولى، حيث تمثل الروابطُ الحركةَ بين عقدتين، يمكننا ضرب مثال بالمطارات المتصلة برحلاتٍ مباشرةٍ حيث تنطلق الطائرة بين نقطتين اثنتين فقط، ما يُفقدنا هنا ميزة السفر متعدد الوجهات الذي نجده في شبكات الدرجة الأعلى التي تستطيع استيعاب أكثر من عقدتين لتمثيل النقاط الأكثر تدفقًا في البيانات.

يركز البحث على جمع الإشارات الاجتماعية لالتقاط الظواهر المريبة في بيانات الشبكة، أي توسيع النظرة التي تتبناها شبكات الدرجة الأولى وعدم الوقوف على أنماط ماركوف التي سيأتي ذكرها.

وهكذا، اتجه الباحثون إلى إضافة تبعيات أخرى، أي عوامل تؤثر في المسار الذي يُرجى التنبؤ به، إلى الشبكة لكي تعكس ظواهر ومقاييس واقعية للبيانات الضخمة وأدوات تحليل الشبكات الموجودة، واستخدموا هذا النموذج لأداء تحليلات الشبكة لتحديد العقد المؤثرة، وكشف الشذوذ، والتنبؤ بالتطور المشترك للشبكات متعددة الأنواع.

يقول الدكتور لانس كابلان **Lance Kaplan**، الباحث في مختبر أبحاث الجيش التابع لقيادة الجيش الأميركي لتطوير القدرات القتالية: "لقد صممنا خوارزميةً قابلةً للتطوير لتمثيل شبكة الدرجة الأعلى، هي **BuildHON+**. ونحن نثبت كفاءة **BuildHON+** بناءً على عملنا السابق من خلال تحليل لآدائها على بيانات حركة السفن العالمية، والتي من المعروف أنّ لها تبعيات تتجاوز الترتيب الخامس، أي أننا على سبيل المثال نتنبأ بالميناء التالي استنادًا إلى أكثر من الموانئ الخمسة الماضية التي مرت بها السفينة".

هذا العمل هو نتيجة للتعاون في مختبر تحالف التكنولوجيا التعاوني لعلوم الشبكة بين كابلان، وماندنا سايبي **Mandana Saebi**، وجيان شو **Jian Xu**، ونيتيش تشاولا **Nitesh Chawla** من جامعة نوتردام، وبرونو ريبيرو **Bruno Ribeiro** من جامعة بوردو. لقد تمكنوا من عرض أداء **BuildHON+** في إطار مهمة الكشف عن الشذوذ في مجموعات بياناتٍ خاصة بمسارات سيارات التاكسي، مجموعة بيانات من العالم الحقيقي، ومجموعة أخرى صنعية. تضمنت البيانات الصنعية أماكن البداية لسيارات التاكسي ووجهاتها، بالنسبة لمجموعة البيانات الحقيقية فقد تمكنوا من رصد يومٍ واحدٍ فقط غير طبيعي فيها، أما المجموعة الصنعية فقد أتاحت لهم مقارنةً أكثر منهجيةً بين **BuildHON+** وأسلوب شبكة الدرجة الأولى.

يقول كابلان: "لقد بيّنّا من خلال التطبيق على نطاق افتراضي واسع يصل إلى مليار مسار للتاكسي عجزَ أساليب الكشف عن الشذوذ الحالية المعتمدة على شبكة الدرجة الأولى في التقاط السلوكيات الشاذة في عملية التنقل التي تتجاوز الدرجة الأولى، وبيّنّا أيضًا كيف أن بإمكان **BuildHON+** حل المشكلة".

يخبرنا كابلان أيضًا أن معظم التحليلات الحالية لتدفق البيانات عبر الشبكة تعتمد على نظرية ماركوف، وهي أن احتمالية انتقال السفينة أو التاكسي إلى الميناء أو الموقع التالي يعتمد فقط على موقعها الحالي، في حين أن قدرتنا على إضافة عواملَ أخرى مؤثرة (تبعيات) تمكّننا من التنبؤ بمساراتٍ أكثر دقةً وبراعةً.

ويقول إن استخدام شبكة الترتيب الأعلى يؤدي إلى تمثيلٍ أكثر دقةً للاتجاهات والأنماط الأساسية في سلوك النظام المعقد، وهي الطريقة الصحيحة لإنشاء شبكةٍ لا تفوتها أي تبعياتٍ أو إشاراتٍ هامة، وتبرز أهمية هذا خصوصًا حينما تحوي البيانات كميةً كبيرةً من المعلومات عديمة الأهمية، وتبعياتٍ ذاتَ طابعٍ تسلسليٍّ داخل مساراتٍ غير مباشرة.

يمكننا شرح هذا بأسلوبٍ آخر، وهو النظر إلى حركة السفن، إذ يقول: "فلنتأمل سفينةً تسافر من ميناءٍ إلى آخر: يمثّل كلُّ ميناء عقدةً في الشبكة، بالنسبة إلى شبكة الدرجة الأولى فهي تنظر فقط إلى السفينة وهي في الميناء (أ) حيث يُنبئ مجرد وجودها في هذا الميناء بضرورة إبحارها إلى الميناء (ب) أيًا كان المكان الذي قدمِت منه سابقًا، فهي تنظر إلى الرابط بين العقدتين اللتين تمثلان هذين المينائين، أما بالنسبة إلى شبكة الدرجة الأعلى فإنها تأخذ في الاعتبار المسارات التي سلكتها السفينة قبل رُسوّها في الميناء (أ)، أي تنظر إلى الروابط بين العُقد السابقة لعقدة الميناء (ب) التي أوصلت إليه، وبدراسة هذه البيانات، تعرف الشبكة أن السفينة لن تتجه بالضرورة إلى الميناء (ب)، وإنما قد تتبع مسارًا مختلفًا إلى غيره، وهذا كله بناءً على النظر إلى حالها السابقة وعدم الانحصار في حالتها الحاضرة. إذًا تستخدم الخوارزمية تدفق البيانات في بناء شبكة درجةٍ أعلى من هذا القبيل، من خلال استخدام اختباراتٍ إحصائيةٍ متخصصةٍ لتنفيذ المسارات المحتمل سلوكها، المتمثلة في الروابط، وتحديد أيها ضروري وأيها عديم الأهمية".

عند بناء شبكات الدرجة الأعلى من تدفق البيانات على فتراتٍ زمنيةٍ متقاربة، يمكننا التقاط التغيرات الدقيقة في تدفق البيانات التي قد تفوّتها شبكات الدرجة الأولى، فلنتخيل مثلا (ه) ميناءً صغيرًا تخرج منه فجأةً شحنةٌ كبيرةٌ نسبيًا متجهةٌ إلى الميناء (د) ثم (ج) ثم (ب) ثم (أ)، ولكن وبسبب صغر الميناء (ه) ولأن معظم الشحنات تخرج من (ه) نحو (د) على أي حال، فإن التغير في تدفق البيانات لن يغير شيئًا في بنية شبكة الدرجة الأولى، أما شبكة الدرجة الأعلى ففي مقدورها التقاط تغيراتٍ كهذه، وكان سبب التغير الدقيق هنا شحنةَ متفجراتٍ سيستخدمها الخصم في منطقة نزاع يخدمها الميناء (أ)، ويُبين هذا كيف للتغيرات الدقيقة في تدفق البيانات لشبكات الإمداد والتنظيم أن توفر معلومات استخباراتية عن أنشطةٍ شنيعةٍ محتملة.

يقول كابلان: "توجد تطبيقاتٌ متعددةٌ لهذا البحث مثل مجال تبادل المعلومات، والنشاط التفاعلي للناس على مواقع الإنترنت، والنقل، والأنواع الغازِيَة (فصائل من الكائنات الحية تستوطن في بيئاتٍ غير مواطنها ما يسبب ضررًا للكائنات الأصلية في ذاك الوطن)، وتتبع المخدرات والبشر، وبالنسبة للجنود فيمكن تطبيقه على سلاسل التوريد واستخدامها من قبل كلٍّ من الجنود والمدنيين".

"ويمكن لتحليلات شبكة الدرجة الأولى أن تجد إشاراتٍ ضعيفةً ذات سلوكٍ عدائيٍّ في شبكات التنظيم والتخطيط قد تُفوّتها شبكة الدرجة الأولى، وقد يتضمن هذا استعدادات كياناتٍ غير حكوميةٍ لشن هجومٍ مؤازرٍ للخصم".

لا يزال هناك العديد من الأسئلة العلمية التي سيسعى الفريق والمجتمع العلمي إلى إجابتها أثناء المضي قدمًا في هذا البحث.

يقول كابلان: "يفتح مفهوم شبكات الدرجة الأعلى أمامنا مساحاتٍ مختلفةً ومثيرةً من الاستكشاف في علوم الشبكات للتنبؤ بشكلٍ أفضل بالتطور المشترك لها، ورصد الإشارات الضعيفة للسلوكيات العدائية. فمثلًا هناك اتجاهٌ محتملٌ للبحث وهو تعميم مفهوم العقد على باقي عناصر الشبكة، مثل الرسومات التي تمثل الشبكة. وهذا يمكننا من أن نفهم بشكل أفضل كيف يمكن أن تتطور المعايير الاجتماعية بين عامة السكان، وهناك مجالٌ آخر، وهو تجربة شبكات الدرجة الأعلى في الشبكات متعددة الطبقات التي قد تمثل مجموعاتٍ اجتماعيةً مختلفةً أو طرقًا مختلفةً لنقل المعلومات لزيادة الدقة في إيجاد الإشارات الضعيفة الشاذة، والسؤال المطروح هو كيفية تقوية عملية التحليل لئلا تُكتشف، حيث قد يحدث تلاعب ببنية الشبكة".

يُنبئ الباحثون بتحسُّن هذه الشبكة بالمزيد من الاختبارات والاستكشافات، وهذا من أجل الجنود في المستقبل لجعلهم أكثر أمانًا واستعدادًا للمهام التي تنتظرهم.

- التاريخ: 2020-09-01
- التصنيف: تكنولوجيا

#الامن الالكتروني

المصادر

- techxplore.com

المساهمون

- ترجمة
  - سماء محمد
- مُراجعة
  - هبة العيوطي
- تحرير
  - رأفت فياض
- تصميم
  - Azmi J. Salem
- نشر
  - احمد صلاح