تحديات جديدة للمدينة الذكية



ما الخوارزمية التي حوَّلت هذه الأضواء إلى اللون الأحمر؟ حقوق الصورة: monticello/Shutterstock.com

لعلّ لحظة انتظارنا لرؤية السيارات تتواصل وتتفاعل فيما بينها وبين إشارات المرور وحواجز الأرصفة بدأت تقترب بسرعة. وتحقيقًا لوعود تقليل الزحام المروري وخفض عدد الحوادث بدأت الولايات المتحدة بتطوير هذه الأنظمة في جميع أنحاء البلاد.

على سبيل المثال، اختُبِرَت إشارة مرور ذكية مطوَّرة من قبل وزارة النقل الأميركية على الطرق العامة في ولايتي أريزونا وكاليفورنيا، وبشكل مكثف في مدينتي نيويورك وتامبا في فلوريدا. وتسمح هذه الإشارات للسيارة بمشاركة موقعها وسرعتها، وبالتالي يمكن استخدامها لتحسين توقيت حركة المرور بشكل فعال في التقاطعات مما يقلل وقت انتظار السيارة أمام إشارات المرور.

وفي هذا الصدد، عكف الباحثون في مجموعة الأبحاث روبوستنيت **RobustNet Research Group** بمختبر المرور في جامعة ميشيغان الأميركية على ابتكار أنظمة آمنة محمية من الاختراقات، لكنهم وجدوا أنه من السهل خداعها نسبيًا. إذ يمكن لسيارة واحدة أن ترسل بيانات مزيفة وتسبب الزحام؛ وجرّاء هذا يمكن لمجموعة من السيارات أن تُسبب اختناقًا مروريًا عند قيامها بذلك. إلى جانب ذلك، وجد الباحثون أن الضعف ليس في التكنولوجيا المطبّقة في الاتصالات الأساسية، بل في الخوارزميات المستخدمة لإدارة تدفق الحركة المرورية.

أخطاء الخوارزمية

بشكل عام، تهدف الخوارزميات إلى أخذْ مجموعة متنوعة من المُدخلات، كعدد السيارات في مواقع مختلفة حول أحد التقاطعات، لاستخراج بيانات تلبي هدفًا معينًا، مثل تقليل وقت انتظار السيارات عند إشارة المرور؛ لذا تفترض خوارزميات التحكم في المرور في نظام إشارات المرور الذكية المسمى **I-SIG** أن المدخلات آمنة وصحيحة، لكن الافتراض غير آمن.

ولكنه من الممكن إجراء التعديلات اللازمة في عتاد السيارة وبرمجياتها إما ماديًا عن طريق مُشخِّص الأعطال في السيارة أو بواسطة اتصالات لاسلكية مع السيارة بهدف جعلها تنقل بيانات كاذبة، ويمكن للشخص الذي يريد اختراق إشارة المرور الذكية تعديل نظام سيارته بتلك الطرق والانتقال إلى تقاطع ما وركن سيارته في مكان قريب.

وبمجرد الوقوف بالقرب من التقاطع يستغل المخترق نقطتي ضعف في الخوارزمية التي تتحكم بضوء الإشارة الأخضر لتمديد الوقت في الطريق المتواجد فيه وبالتالي يطيل مدة ضوء الإشارة الأحمر في الطرق الأخرى.

هذا الضعف الذي وجدوه والمسمى بـ "ميزة السيارة الأخيرة" هو سبيل لإطالة زمن الضوء الأخضر، إذ تراقب الخوارزمية عدد السيارات المقتربة من التقاطع، وتقدر طول خط السيارات وتحدد المدة التي يفترض أن تستغرقها جميع المركبْات في خط مروري للوصول إلى التقاطع. يساعد هذا النظام على تخديم أكبر عدد من السيارات في كل مرة. إلا أنه من الممكن إساءة استخدامه بحيث يقوم المخترق بتوجيه سيارته للقيام بإبلاغ كاذب عن الانضمام إلى خط السيارات في وقت متأخر جدًا، ثم ستحتفظ الإشارة باللون الأخضر لوقت أكثر من اللازم وسيترتب على ذلك إيقاف الطرق الأخرى أيضًا.

الاختناق المروري عند نظام مراقبة الإشارة المرورية

أما نقطة الضعف الأخرى فأطلقوا عليها "هجوم السيارة المتخفية". بُنِيَتْ خوارزمية إشارة المرور الذكية آخذين بعين الاعتبار وجود سيارات غير متصلة بها، فيُستخدم بدلًا من ذلك نماذج قيادة ومعلومات السيارات الأحدث والمتصلة لتعيين الوقت المطلوب لمرور السيارات الأقدم وغير المتصلة، لذلك إذا أبلغت سيارة متصلة أنها توقفت على مسافة طويلة من التقاطع، ستفترض الخوارزمية أن هناك طابورًا طويلًا من المركبات القديمة المنتظرة أمامها. ومن ثمَّ يقوم النظام بإطالة مدة الضوء الأخضر للمسار بسبب الطابور الطويل الذي يُعتقد أنه موجود ولكنه في الحقيقة ليس موجودًا.

تحدث هذه الاختراقات بجعل الجهاز يكذب حول موقعه وسرعته. وهذا يختلف كثيرًا عن طرق الاختراقات الإلكترونية المعروفة، مثل إدخال الرسائل في اتصالات غير مشفرة أو تسجيل دخول مُستخدم بطريقة غير مصرحة بواسطة حساب مُميز، لذلك لا يمكن للحماية المعروفة ضد تلك الاختراقات أن تفعل أي شيء بخصوص الجهاز الكاذب.

نتائج اختراقات الخوارزمية

يمكن لاستخدام تلك الثغرات أن يتيح للمخترقين إطالة مدة الضوء الأخضر للطرق قليلة الازدحام وإطالة مدة الضوء الأحمر لتلك الأكثر ازدحاماً. لكنك قد تتساءل ما الذي يدفع الناس للعبث بإشارة المرور؟ يمكن أن يكون هذا النوع من العبث بإشارات المرور للمتعة فقط!

فعلى سبيل المثال، يمكن للشخص الذي يريد السفر بشكل أسرع تعديل توقيت الضوء الأخضر الخاص به، على حساب تأخير السائقين الآخرين. كما قد يسعى المجرمون أيضًا إلى ذلك لإبعاد الشبهة عن أنفسهم في مسرح الجريمة أو لإعاقة ملاحقة سيارات الشرطة. ضف إلى هذا وجود بعض مخاطر سياسية ومالية حيث يمكن لمجموعة من الناس إيقاف عدة تقاطعات رئيسية والمطالبة بالمال لاستعادتها.

إن هذا النوع من الهجمات يستهدف الخوارزمية الذكية نفسها، ونتيجة لذلك فإن إصلاحها يتطلب جهودًا من وزارة النقل وأمن الفضاء الإلكتروني (السيبراني). وأهم ما تعلمناه في هذه التجربة أن أجهزة الاستشعار الأساسية التي تقوم عليها الأنظمة التفاعلية، كالمركبات في نظام **I-SIG**، ليست جديرة بالثقة، بل يجب قبل البدء في العمليات الحسابية أن تحاول الخوارزميات التحقق من صحة البيانات التي تستخدمها. ولعلّنا نسوق مثال على هذا، يمكن لنظام التحكم في حركة المرور استخدام أجهزة استشعار أخرى، مثل أجهزة الاستشعار الموجودة على الطرق الممتدة بالفعل في جميع أنحاء البلاد، للتحقق من عدد السيارات الموجودة.

تعتبر هذه بداية الطريق لإيجاد أنواع جديدة من المشاكل الأمنية في نظم النقل الذكية مستقبلًا، والتي يحاول الباحثون اكتشاف جميع نقاط الضعف فيها وإيجاد أساليب لحماية السائقين والطرق.

- التاريخ: 2018-10-07
- التصنيف: تكنولوجيا

#الخوارزميات الحاسوبية #اشارات مرور #السيارات ذاتية القيادة #تبادل البيانات بين السيارات

المصادر

- Techxplore

المساهمون

- ترجمة
  - يمان علاء الدين
- مُراجعة
  - حنان مشقوق
- تحرير
  - محمد عبوده
  - رأفت فياض
- تصميم
  - رنيم ديب
- نشر
  - كرم الحلبي