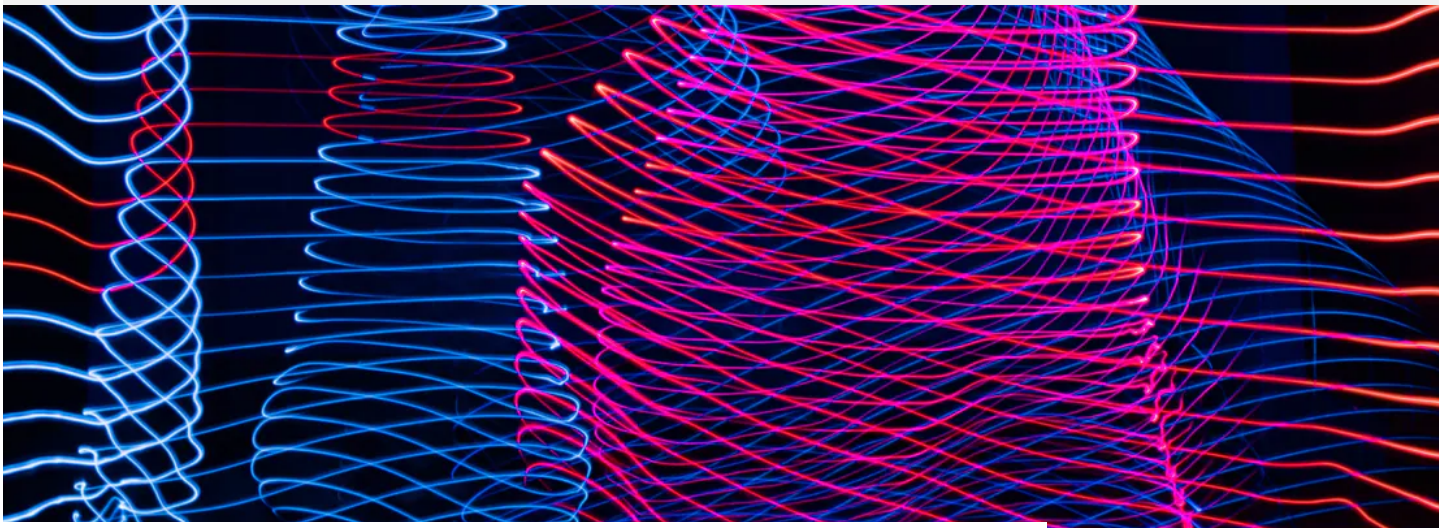
Comment marchent votre réseau wifi et vos appareils connectés – et pourquoi ils sont vulnérables aux attaques informatiques

Edward Staddon, Nathalie Mitton, Valeria Loscri

THE CONVERSATION
L'expertise universitaire, l'exigence journalistique



Comment marchent votre réseau wifi et vos appareils connectés – et pourquoi ils sont vulnérables aux attaques informatiques

27 juin 2021, 19:04 CEST

Les réseaux sans fil fonctionnent avec beaucoup d'intermédiaires. Certains sont-ils corrompus ? Zak, Unsplash, CC BY

Auteurs

Edward Staddon
Doctorant en Réseau et Cybersécurité, Inria

Nathalie Mitton
Directrice de recherche en réseau de capteurs sans fil, Inria

Valeria Loscri
Associate research scientist, Inria

L'apparition du Covid-19 a été accompagnée d'une forte hausse du nombre de cyberattaques dans le monde envers les « infrastructures critiques ». Depuis le début de la pandémie, le nombre d'attaques connues a augmenté de 300 %, avec en 2020 une hausse de 238 % envers le milieu banquier. De plus, 27 % des attaques durant 2020 ont pris pour cible le milieu hospitalier, avec la France qui en début 2021 s'est retrouvée en ligne de mire pour les cybercriminels.

Avec le déploiement d'équipements connectés, comme les pompes à insuline ou pacemakers « intelligents », les champs d'attaque et les risques associés évoluent également. Via ces appareils, un attaquant peut cibler l'état même de santé des patients et provoquer de sérieux dommages. De plus, ces attaques peuvent causer un « effet en cascade », avec des conséquences parfois inattendues sur d'autres systèmes, par exemple en allumant une prise électrique « connectée » sur laquelle est branché un radiateur, provoquant l'ouverture d'une fenêtre motorisée pour contrer l'augmentation de la chaleur.

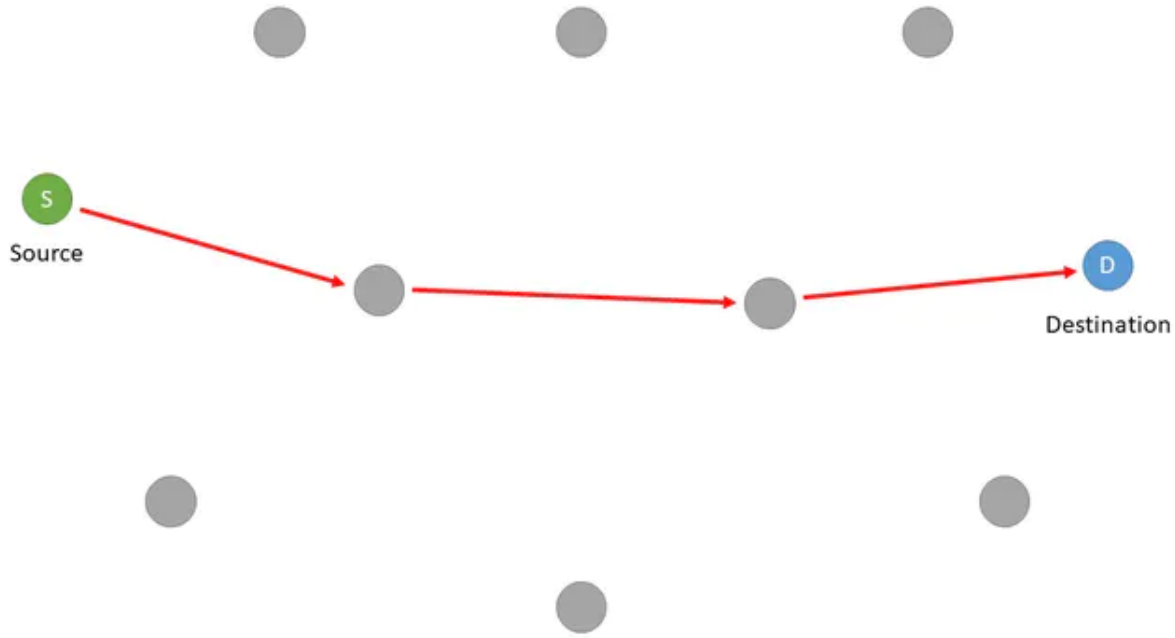
Ces équipements autonomes font partie de la famille de l'« Internet des Objets » et sont au centre de la recherche en cybersécurité. De plus, avec leurs contraintes particulières comme des capacités de calcul et d'utilisation de batteries, la sécurité des technologies sans fils utilisées intéresse également les chercheurs, en particulier pour assurer l'intégrité du réseau vis-à-vis de potentielles intrusions.

Les réseaux multi-saut

Lorsqu'on dit « réseau sans fil », on pense immédiatement à la connexion wifi classique qu'on utilise au quotidien pour se connecter à l'Internet via sa box. Bien qu'efficace, ce type de connexion possède quelques restrictions.

Pour illustrer ces propos, prenons l'exemple d'un bar où les clients ne peuvent s'adresser qu'au barman. On peut commander à boire sans problème, mais si on souhaite parler avec notre voisin, nous devons le faire via le barman qui contrôle la conversation. Maintenant, si on s'éloigne pour s'installer à une table, le barman n'est plus à proximité et ne peut donc plus entendre nos paroles : on ne peut plus ni échanger avec notre voisin ni commander à boire.

Dans la vraie vie, nous n'avons pas ces contraintes et on peut donc avoir une conversation directement avec notre voisin. Cependant, le barman est toujours trop loin et la soif commence à s'installer. La solution existe sous la forme de serveurs qui circulent entre les tables, prenant les commandes, les transmettant au barman et apportent les boissons.



Pour aller d'une source à une destination, il faut passer par des intermédiaires – trois dans cet exemple. Le choix des intermédiaires s'appelle le routage. Edward Staddon, Inria, Fourni par l'auteur

Dans le domaine du numérique, cette approche, appelée « multi-saut », est utilisée principalement dans des réseaux de grande envergure, comme les réseaux de capteurs ou les réseaux mobiles. Contrairement à notre bar, nous n'avons pas d'équipements précis qui jouent le rôle du serveur : chaque participant en possède plutôt les capacités. De ce fait, n'importe quel équipement peut transmettre et choisir un chemin, appelé « route » pour relayer un message d'un côté du réseau à l'autre – comme si nous faisions passer la commande « une limonade et des cacahuètes s'il vous plaît » de table en table.

Les attaques au sein des réseaux sans fil

Une fois les boisons reçues, on commence à discuter avec notre voisin de notre journée au travail. Cependant, assis à la table juste à côté il y a un espion qui entend tout ce qui est dit et note les informations sur une feuille, sans qu'on le sache. En partant, il allume le système sonore du bar qui joue de la musique à un volume très élevé. Malheureusement, avec ce bruit on ne peut plus échanger avec notre voisin.

Cet exemple illustre les principales difficultés au niveau des réseaux sans fil, liées à la protection des communications. Comme nos propres voix, les ondes radio utilisées par ces technologies traversent l'espace public et donc peuvent être impactées et brouillées par d'autres ondes. De plus, elles peuvent même être écoutées par d'autres équipements à proximité. L'utilisation de moyens de sécurisation, comme les mots de passe dans les réseaux wifi ou le chiffrage des échanges, limite cette écoute illicite.

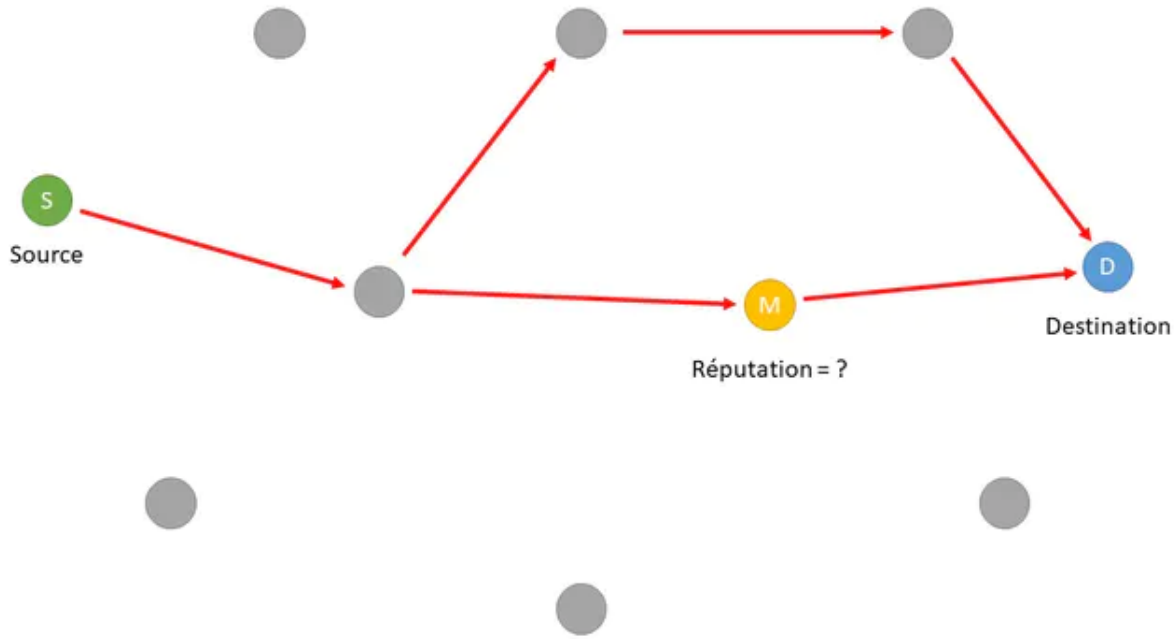
En permettant aux nœuds de relayer les informations entre eux, on ouvre le réseau à d'autres menaces, notamment celles qui ciblent le « routage » (choix de chemin à prendre lors du transfert des messages). Mettons que nous souhaitions commander une autre boisson. Le comportement du serveur influence fortement l'épanchement de notre soif. Il pourrait par exemple purement et simplement ignorer notre commande, remplacer un thé par un café ou livrer notre commande à une autre table.

Ces menaces envers le choix du chemin à emprunter dans l'émission et la réception des messages peuvent avoir de lourdes conséquences sur ces réseaux où le routage des messages joue un rôle crucial. Cependant, la réussite de telles attaques repose sur un point précis : l'intégration de l'attaquant non seulement dans le réseau, mais au sein du processus de routage.

La sécurisation du processus de routage

Plusieurs solutions existent au niveau des équipements informatiques pour la détection d'intrusion. Basées sur des technologies comme l'apprentissage machine ou l'analyse des ondes radio, elles sont assez efficaces, mais possèdent plusieurs contraintes. Les techniques d'apprentissage par exemple sont gourmandes en termes de calcul qui, dans le cadre des équipements IoT (pour « Internet-of-Things »), épuisent les batteries des objets connectés de tout type.

Une potentielle solution se trouve ici aussi au niveau du comportement humain. Dans le bar, si on voit que notre serveur agit sur notre commande sans notre accord, notre confiance en lui va baisser, impactant ainsi sa réputation. On va donc chercher un autre moyen d'acheter nos boissons en passant par un autre serveur avec une meilleure réputation.



Le choix du chemin par lequel transite l'information dans un réseau sans fil dépend de la "réputation" des intermédiaires. L'un d'eux est-il soupçonné d'être corrompu et à la solde d'un attaquant ?
Edward Staddon, Inria, Fourni par l'auteur

Au sein de notre réseau, on peut analyser le comportement des nœuds voisins et leur associer un « indice de réputation » qui indique notre niveau de confiance vis-à-vis de ce nœud. Via l'« exploration réactive »

du réseau, c'est-à-dire « à la demande » et uniquement quand on en a besoin, un chemin d'un point A à un point B est déterminé et donc connu par les différents nœuds. Ainsi, si le comportement attendu de routage d'un équipement intermédiaire dévie de ce chemin, on considère le nœud comme potentiellement malicieux et son indice de réputation est impacté, réduisant la probabilité de l'utiliser dans un futur échange.

L'indice de réputation évolue au cours du temps et permet non seulement de détecter de nouveaux équipements malicieux introduits dans le réseau par l'attaquant, mais aussi des équipements préexistants qui ont été corrompus par l'attaquant. Cet indice permet aussi réintégrer de nœuds qui ont été exclus par erreur, ou qui ont été secourus des mains des criminels.

Pour finir, avec l'utilisation de la technologie blockchain, un système de registre distribué et immuable issu de la cryptomonnaie, on peut partager ces indices de réputation de manière sécurisée, les protégeant de potentiels sabotages.

Assurer la sécurité des infrastructures critiques

La sécurité de ces réseaux est primordiale, et ce d'autant plus lorsqu'ils appartiennent à des infrastructures critiques dans des secteurs d'importance. Une attaque envers ces secteurs peut non seulement causer des dégâts financiers ou énergétiques, mais aussi humains lorsque la cible est un milieu hospitalier.

C'est dans ce contexte que le projet européen CyberSANE vise à fournir des outils avancés aux opérateurs afin de leur permettre de mieux répondre aux menaces auxquelles ils sont confrontés. CyberSANE permet aux infrastructures critiques de travailler ensemble dans la lutte contre les cybercriminels, via l'échange d'informations, afin d'alerter d'autres infrastructures critiques de potentielles menaces. De plus, via l'emploi de méthodes comme l'extraction et l'analyse de données en provenance du « deep web », CyberSANE est capable de prévenir d'une attaque en préparation, afin de fortifier les défenses avant l'arrivée de l'armada ennemie.

Internet téléphonie mobile Internet des objets informatique réseaux réseaux intelligents cybersécurité télécommunications cyber-attaques cybersurveillance cyberespionnage