FoxyTag, l'avertisseur de radar 100 % autogéré

Michel Dériaz, *Director* ■ *FoxyTag Ltd, Dukes Court, 32 Duke Street, Londres SW1Y 6DF*
Tel. : + 41 22 379 01 04 ; e-mail : michel.deriaz@foxytag.com

Comment un avertisseur radar collaboratif peut-il fonctionner de manière fiable dans le monde entier sans qu'aucune intervention humaine ne valide les données recueillies ? C'est le secret de FoxyTag, ou plutôt de son moteur de confiance.

Présentation de *FoxyTag*

FoxyTag désigne un système d'avertisseur radar pour téléphone mobile fonctionnant dans le monde entier. Ce système est collaboratif et autogéré : ce sont les utilisateurs qui « *ajoutent* » les radars et ce sont des moteurs de confiance électroniques qui assurent la qualité des données. *FoxyTag* contient aujourd'hui plus de 37 000 radars fixes, essentiellement en Europe, Afrique du Sud, Australie, Maghreb, Émirats-Arabes-Unis, Brésil, Chine, Taïwan, États-Unis, Canada, Russie, Nouvelle-Zélande, Singapour et Israël. *FoxyTag* signale également les radars mobiles ainsi que les *tags* fantômes (emplacements ayant souvent des contrôles mobiles).

Le modèle commercial est très simple : *FoxyTag* gère le serveur ainsi que la base de données, et ce sont des partenaires indépendants qui créent les applications pour *smartphones*. Ces partenaires peuvent vendre leur application comme bon leur semble, et l'utilisation du système *FoxyTag* se fait en contrepartie d'une taxe prélevée à chaque connexion. Ce système a permis de voir apparaître des avertisseurs de radars pour les plateformes *Java*, *iPhone* et *Android*.

Différents types d'avertisseurs de radar fonctionnant sur téléphones mobiles de type *smartphone*.

Fiable mais pas à jour, ou à jour mais pas fiable ?

Les services permettant le géocodage d'informations peuvent se classer en deux catégories, chacune présentant un atout ainsi qu'un défaut majeur :

➤ Les services non-collaboratifs, où une entité particulière pose les *tags*. L'information est souvent de qualité mais coûte cher et n'est pas nécessairement à jour ;

➤ Les services collaboratifs, où ce sont les utilisateurs eux-mêmes qui posent les *tags*. L'information coûte peu cher et est souvent à jour, mais l'utilisateur n'a aucune idée de la qualité des données.

Un bon exemple illustrant le problème des données collaboratives (*crowdsourcing*) peut se trouver sur *Google Earth* : si l'on cherche le sommet du Mont-Blanc, on en trouvera plusieurs, chacun rattaché à un auteur différent. Il est donc impossible de savoir *a priori* lequel de tous ces sommets potentiels est le « *vrai* ».

Le problème avec les radars est similaire. Comment savoir si un *tag* posé par un utilisateur définit réellement l'emplacement d'un radar ? Comment faire la différence avec une erreur commise par quelqu'un ne sachant pas utiliser l'application, ou pire, par un acte malveillant de la part d'un concurrent ou d'une « *taupe* » ? La solution généralement retenue par les fournisseurs d'avertisseurs de radars consiste à vérifier les données en les croisant avec d'autres sources. Il s'agit là d'un travail manuel relativement onéreux et évidemment limité à un territoire donné. Une solution intermédiaire consiste à encourager les usagers à confirmer ou infirmer les *tags* des autres participants afin de déterminer la probabilité que le *tag* soit valide. Néanmoins, deux problèmes majeurs empêchent cette solution de fonctionner de manière optimale :

➤ Quoiqu'elle puisse corriger les erreurs d'un utilisateur, cette méthode ne protège pas le système d'une attaque. En effet, une collusion de quelques personnes qui se confirmeraient les *tags* les uns les autres sera difficile à détecter si leurs agissements sont aléatoires et bien répartis dans le temps. De plus, un informaticien ayant les connaissances techniques suffisantes pourra facilement mettre au point un algorithme générant des collusions d'utilisateurs virtuels malveillants ;

➤ Comment motiver les gens à confirmer ou infirmer les *tags* des autres ?

FoxyTag propose une solution qui permet de cumuler les avantages des deux catégories précédentes (services collaboratifs et services non-collaboratifs) sans pour autant souffrir des problèmes mentionnés ci-dessus (attaques du système et motivation de participer) : le moteur de confiance.

La clef du système : le moteur de confiance

Le moteur de confiance de *FoxyTag* crée des liens entre les personnes signalant les radars de manière similaire, puis utilise ce réseau pour retourner uniquement de l'information pertinente aux utilisateurs.

Scénario

John et Jack voient un nouveau radar. John le *tague*, mais Jack qui veut nuire au système le désapprouve.

Mike est un nouvel utilisateur qui n'a pas encore créé de liens avec les autres. Comme il y a un doute sur la validité du *tag* (John et Jack ont des opinions différentes), le *tag* est montré à Mike. Mais sans liens de confiance, Mike est également susceptible de recevoir du *spam* ou de se retrouver piégé par un radar désapprouvé par plusieurs utilisateurs frauduleux.

Quand Mike voit qu'il y a effectivement un radar, il confirme le *tag*. Son vote est alors enregistré dans l'historique du *tag* et son réseau de confiance est mis à jour.

Dorénavant l'avis de John aura plus de poids que celui de Jack aux yeux de Mike.

Mettons à jour le réseau avec Luke faisant confiance à Arthur et Arthur faisant confiance à Mike.

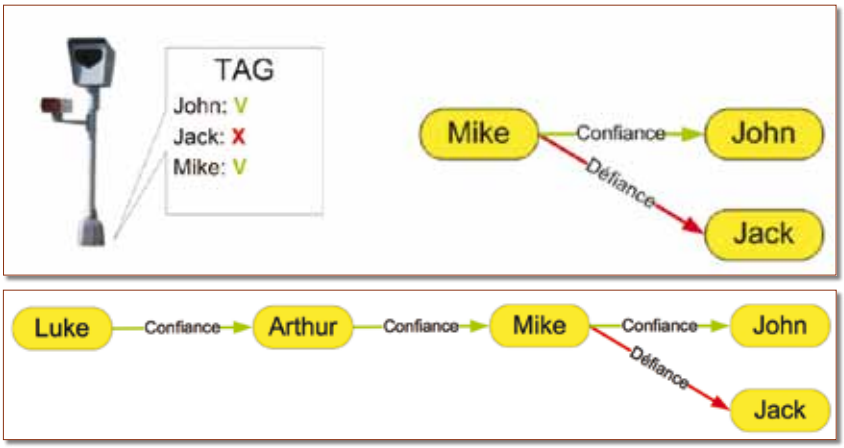
Luke ne connaît pas les personnes dans l'historique du *tag* (John, Jack et Mike), mais comme il fait confiance à Arthur, qui fait confiance à Mike qui a confirmé le *tag*, le système considère le *tag* comme pertinent et le retourne à Luke.

Tags actifs

Les *tags* sont des objets actifs participant aux aspects de confiance et de sécurité. Ils s'échangent des observations de comportements suspects, par exemple un utilisateur désapprouvant un *tag* qui a été confirmé à maintes reprises durant des mois. Dans ce cas, le *tag* en question va demander à ses voisins comment l'utilisateur est intervenu auprès d'eux, puis exclura cette personne si son comportement est jugé frauduleux.

Innovation

Le moteur de confiance rend *FoxyTag* unique : c'est le seul système collaboratif déployé mondialement qui soit complète-



ment autogéré. Les *spammers* ou autres fraudeurs sont automatiquement exclus et les utilisateurs normaux reçoivent des informations fiables et actualisées grâce aux liens de confiance qu'ils tissent entre eux. Les utilisateurs sont par conséquent motivés à participer en *taguant* ou confirmant les informations des autres ; plus ils participent, plus ils reçoivent des informations de qualité. Et connaître la position exacte d'un radar est, pour la plupart de gens, bien plus important que de connaître la positon exacte du sommet du Mont-Blanc.

Sous le capot

Le noyau du moteur de confiance consiste en une fonction récursive. Lorsque l'utilisateur demande les *tags* se trouvant autour de lui, le système va, pour chacun d'eux, le système possède assez d'informations sur le *tag* pour savoir s'il faut l'afficher ou non. En cas de surcharge du serveur, la « *profondeur* » (le nombre de niveaux des amis des amis) de recherche est automatiquement diminuée afin d'éviter que le système soit mis en péril. Néanmoins ces surcharges sont très rares car le calcul est relativement rapide ; en effet, toutes les opération se font sur le serveur.

L'application cliente n'a aucune notion du moteur de confiance. Lorsqu'elle demande les *tags* autour de sa position, elle reçoit simplement une liste de ceux qui sont pertinents par rapport à ses liens de confiance, qui eux sont conservés sur le serveur. Cette « *obscurité* » pour le client présente deux grands avantages : le premier est bien sûr la simplicité. Dans le modèle économique

Exemples de boîtes de saisie présentées à l'abonné qui désire mémoriser l'emplacement d'un radar.

analyser son historique et en déduire la pertinence. Si l'utilisateur « *connaît* » les personnes de l'historique, il peut déterminer la pertinence du *tag* simplement en comparant leurs avis (confirmation ou infirmation du *tag*). Sinon, l'utilisateur va demander à ses amis, en d'autres termes les personnes avec qui il a déjà construit des liens de confiance, leur opinion au sujet des personnes concernées. Ces amis demanderont à leur tour à leurs amis et ainsi de suite jusqu'à ce que

de *FoxyTag*, où ce sont des partenaires externes qui conçoivent les applications mobiles, cet atout est bien évidemment le bienvenu. Le deuxième est la sécurité : en effet, il est plus difficile de compromettre le système lorsqu'on a quasiment aucune information à disposition. Notons que nous ne parlons de l'algorithme lui-même, qui a été publié dans une thèse en 2008, mais bien des valeurs de confiance. On pourrait comparer *FoxyTag* avec un logiciel de chiffrage où l'algorithme est public mais où il n'y aurait strictement aucune information concernant la clef de chiffrement.

Et si je me rends dans un endroit où je ne connais personne, est-ce que mon réseau de confiance sert à quelque chose ? Oui, car lorsqu'on se rend loin de chez soi, on emprunte en principe les routes principales et, par conséquent, les chances de croiser un ami ou l'ami d'un ami sont grandes. Des tests ont d'ailleurs démontré que même un tout nouvel utilisateur, qui ne possède par conséquent aucun réseau de confiance, n'a besoin de contribuer qu'environ trois à cinq fois (poster un nouveau *tag*, confirmer un *tag* existant...) pour bâtir un réseau lui permettant d'éliminer plus de 80 % des *spam*. La réputation d'un utilisateur se construit très vite, il n'est donc pas nécessaire de définir des « *super-utilisateurs* », ou des personnes à qui on attribue d'office des liens de confiance positifs, comme c'est le cas chez certains système concurrents.

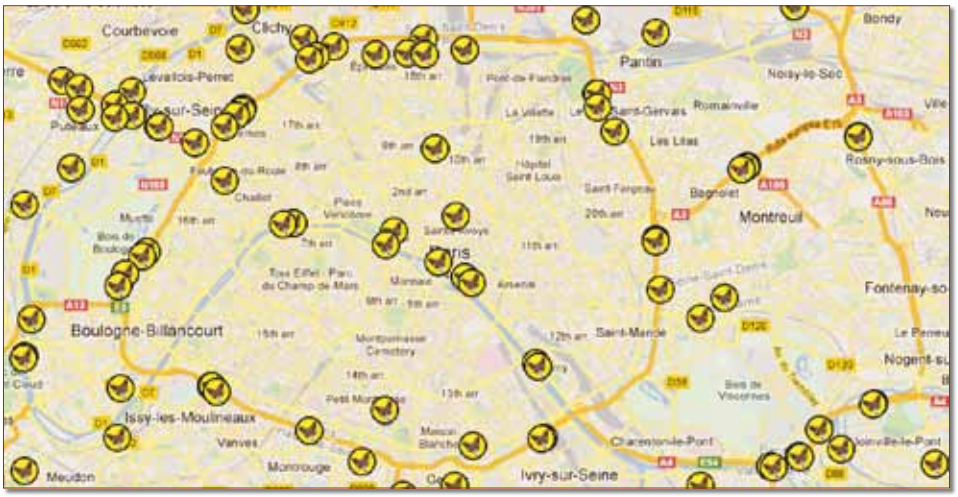
Et si y avait plus de *spammeurs* que d'utilisateurs honnêtes ?

Eh bien *FoxyTag* fonctionnerait toujours ! En effet, contrairement aux systèmes d'évaluation classiques, où, par l'intermédiaire de votes positifs et négatifs, on essaie d'attribuer une valeur de confiance globale, appelé réputation, dans *FoxyTag* chaque utilisateur possède son propre réseau de confiance, de la même manière que dans les relations humaines. Vous pouvez très bien faire confiance à une personne même si cette dernière a très mauvaise réputation. Le moteur de confiance cherche simplement à regrouper les personnes se comportant de manière similaire. Ainsi, si deux utilisateurs se mettent à *taguer* les arbres plutôt

que les radars, ils seront très vite mis à l'écart par le reste de la communauté, mais entre eux un fort lien de confiance sera établi et ils verront leurs contributions mutuelles. Dans une collusion de *spammers*, seuls ces derniers verront leurs *spams*. Néanmoins en pratique, pour éviter que *FoxyTag* soit utilisé pour autre chose que les radars, le moteur de confiance a été configuré pour mettre automatiquement en quarantaine tout individu ou groupe d'individu ne se comportant pas comme les autres.

L'incertitude de la vérité

Ou en anglais *The uncertainty of truth*. C'est derrière ce terme, qui semble plus proche d'une pensée philosophique que d'une expression technologique, que se cache un des concepts clef permettant au moteur de confiance de fonctionner. Même si tous les utilisateurs étaient honnêtes et ne commettaient aucune erreur lors du signalement d'un radar, il y aurait tout de même des situations où un utilisateur diminuerait son lien de confiance envers un autre. C'est le cas par exemple lorsqu'un radar est physiquement supprimé : un utilisateur aura créé le *tag* et d'autres l'auront peut-être confirmé, mais l'utilisateur qui passe après la suppression va désapprouver le *tag* ce qui diminuera tous les liens de confiance avec les utilisateurs précédents. Cette diminution est indispensable pour éviter que des collusions de *spammers* polluent le système avec des informations erronées. Le système doit par conséquent pouvoir *pardonner*, en d'autres termes ne pas trop pénaliser, un utilisateur qui se trouverait dans cette situation ou qui simplement commettrait une erreur. On constate en effet qu'environ 2 % des informations envoyées sont des erreurs, par exemple une personne qui demande la suppression d'un *tag* alors qu'elle souhaitait le confirmer. Pour cela la formule retenue est très simple : une contribution positive (par exemple un utilisateur qui confirme le *tag* d'un autre) fait augmenter le lien de confiance de manière linéaire, mais par contre une contribution négative (par exemple un utilisateur qui désapprouve un *tag*) diminue le lien de manière exponentielle. Et, comme on le sait, une exponentielle évolue d'abord tout doucement (le lien de confiance diminue donc peu) mais ensuite de plus en plus vite. Une personne cherchant à nuire au système ou qui se tromperait trop souvent serait donc très rapidement discréditée aux yeux des autres utilisateurs.



Fenêtre cartographique de visualisation.

Autres domaines d'application

Le moteur de confiance n'est pas limité uniquement au domaine des radars. D'une manière générale il fonctionne pour n'importe quelle donnée géographique. La société *ArxiT* a, par exemple, réalisé un guide touristique, *FoxyTour* (*http://www.foxytour.net*) qui s'adapte automatiquement à son utilisateur afin de lui proposer du contenu de plus en plus pertinent.

Le moteur de confiance contient trois couches. C'est dans la première que s'effectue le calcul de la confiance et la mise à jour des valeurs. Ce noyau est générique, il convient à n'importe quel système de confiance traitant des données géographiques. La deuxième couche contient les règles de fonctionnement qui sont propres au domaine d'utilisation : pour un avertisseur de radar, par exemple, les règles indiquent qu'il est moins grave de signaler un radar qui n'existe pas plutôt que d'essayer d'en effacer un. Enfin, la troisième couche est composée des paramètres du moteur de confiance. Elle définit combien de niveaux au maximum (amis des amis) il faut explorer lorsqu'on cherche à obtenir la pertinence d'un *tag*.

Le moteur a été validé par des publications scientifiques et son fonctionnement principal n'a pas évolué depuis 2008. Seules des optimisations concernant l'accès aux données (une demande de *tags* peut exiger plusieurs centaines de requêtes) sont régulièrement effectuées.

Développer son propre avertisseur radars en moins d'une heure

Afin d'accélérer la production de nouvelles applications, *FoxyTag* offre à ses partenaires une API contenant tout le code permettant de construire un avertisseur de radars. Libre ensuite au développeur de se contenter d'une simple personnalisation en modifiant les images ou d'entreprendre des développements supplémentaires afin d'offrir de nouvelles fonctionnalités. Ce dernier peut ainsi produire très rapidement une première application fonctionnelle, avec une interface graphique peu ou pas personnalisée, quitte à retravailler ces aspects dans un second temps. ■