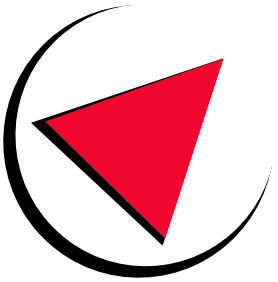

L I F C

LABORATOIRE D'INFORMATIQUE DE L'UNIVERSITE DE FRANCHE-COMTE

EA 4269

Problématiques de sécurité dans un système de géolocalisation implicite

Matteo Cypriani — Philippe Canalda — François Spies

Rapport de Recherche no RR 2011–04

THÈME 4 – Octobre 2009

Problématiques de sécurité dans un système de géolocalisation implicite

Matteo Cypriani, Philippe Canalda, François Spies

Thème 4
OMNI

Octobre 2009

Résumé : Dans le cadre de nos recherches sur la géolocalisation en intérieur par Wi-Fi, nous avons réalisé un système expérimental permettant de tester et comparer différentes techniques de positionnement. Cet article introduit l'une des perspectives majeures d'amélioration, à court terme, de notre système : la géolocalisation implicite, c'est-à-dire ne nécessitant pas que le mobile requière explicitement sa position auprès de l'infrastructure. Cette dernière, à partir des informations qu'elle reçoit sur le réseau, est capable de détecter la présence des mobiles et de calculer leur position. Nous appliquons ici ce principe au cas d'un système de détection d'intrusions de mobiles non autorisés, et soulevons les problématiques posées en terme de sécurité, un tel système devant être résistant aux tentatives de tromperies de mobiles attaquants. Nous dressons ensuite une liste de techniques pouvant être utilisées par ces attaquants afin de nuire au système.

Mots-clés : IEEE 802.11, Réseaux sans fil, Géolocalisation en intérieur, Géopositionnement implicite, Détection d'intrusions, Auto-calibration dynamique

Laboratoire d'Informatique de l'Université de Franche-Comté,
Antenne de Montbéliard — UFR STGI,
Pôle universitaire du Pays de Montbéliard,
25200 Montbéliard Cedex (France)
Téléphone : +33 (0)3 81 99 47 43 — Télécopie +33 (0)3 81 99 47 91

Security issues in an implicit positioning system

Abstract: In the scope of our research about Wi-Fi indoor positioning, we realised an experimental system allowing us to test and compare various positioning techniques. This paper introduces one of the major short-term improvements of our system : implicit positioning, that does not need any request explicitly transmitted by the mobile to the infrastructure. Computing the information received on the radio network, the infrastructure is able to detect and localise mobiles. We use this principle in the case of an unauthorised mobiles' intrusion detection system and expose the main security issues. Then, we list some techniques that could be used by attackers to slip past the system's guard or make it ineffective.

Key-words: IEEE 802.11, Wireless LAN, Indoor localisation, Implicit position measurement, Unauthorised device detection, Dynamic self-calibration

Laboratoire d'Informatique de l'Université de Franche-Comté,
Antenne de Montbéliard — UFR STGI,
Pôle universitaire du Pays de Montbéliard,
25200 Montbéliard Cedex (France)
Téléphone : +33 (0)3 81 99 47 43 — Télécopie +33 (0)3 81 99 47 91

1 Introduction

Dans le cadre de nos recherches sur la géolocalisation en intérieur, nous avons développé un système expérimental baptisé OWLPS (*Open Wireless Positioning System*). Il met en œuvre plusieurs algorithmes et techniques de calcul de la position, fondés sur une cartographie des puissances des signaux Wi-Fi (IEEE 802.11), des modèles de propagation du signal, éventuellement prenant en compte la topologie du bâtiment et la politique de déplacement de l'utilisateur. Il se base pour cela sur une infrastructure composée essentiellement de points d'accès répartis au sein de la zone de déploiement. Le calcul de la position est effectué par un serveur utilisant les données récoltées par ces points d'accès. L'architecture du système et les différents algorithmes sont détaillés dans [1].

Dans cet article, nous nous placerons donc dans le cadre d'un géopositionnement par Wi-Fi, en intérieur, reposant sur une infrastructure effectuant les mesures et les calculs. Cette configuration offre une souplesse et des possibilités accrues en matière de fonctionnalités : on peut ainsi l'utiliser dans le cadre de services dépendants du contexte offerts aux mobiles, d'une simple géolocalisation, mais aussi d'un système de détection d'intrusions, comme nous le verrons dans la section 2.

2 Du positionnement explicite à la détection d'intrusions

La plupart des systèmes de géopositionnement prennent pour postulat le fait que les mobiles demandent à l'infrastructure de les localiser, afin de bénéficier d'un service ou simplement de connaître leur position. Si cette démarche simplifie le fonctionnement du système, il existe une autre approche intéressante, dans laquelle le mobile ne demande pas explicitement à être positionné : on parle alors de positionnement implicite, car le système utilise les informations émises sur le canal radio pour détecter et localiser les mobiles. Cette approche a l'avantage de ne pas nécessiter l'installation, sur chaque mobile, d'un code client permettant de contacter l'infrastructure, mais elle permet aussi de développer un système de détection d'intrusions. Dans ce cadre, non seulement le mobile ne demande pas à être positionné, mais il se peut même qu'il fasse tout pour masquer sa présence, en empêchant le fonctionnement correct de l'infrastructure de positionnement, ou simplement en mettant cette dernière en échec.

Afin de développer un système de détection d'intrusions Wi-Fi avec géopositionnement des appareils tiers, il faut donc non seulement être capable de localiser un mobile sans qu'il s'identifie préalablement et réclame lui-même sa position, mais également de résister à tout type d'attaque. L'entreprise Interlink Networks a proposé en 2002 [2] un système de géolocalisation des appareils Wi-Fi non autorisés. Ce système est cependant très peu précis (d'après nos expérimentations [1, 3]) et il n'est pas fait mention de techniques permettant de résister à des tentatives de brouillage. Interlink Networks semble s'intéresser essentiellement aux comportements problématiques d'utilisateurs innocents en entreprise : déployer un point d'accès sauvage dans son bureau, utiliser sa propre carte Wi-Fi, créer un réseau ad-hoc, etc. Le cas des attaques sur le réseau Wi-Fi est évoqué, mais pas celui d'attaques à l'encontre du système de positionnement lui-même.

Il est donc nécessaire d'imaginer les attaques dont pourrait être victime un système de géolocalisation et de modifier ou d'adapter son comportement et son fonctionnement, de manière à ce qu'il puisse y résister, déjouer les tentatives de brouillage, et si possible parvenir à localiser les attaquants malgré tout. En effet, s'il est parfois possible de se rendre compte que des mobiles tentent de tromper le système, et donc de ne pas fournir à l'utilisateur une position fausse, il est plus délicat de fournir une position correcte en situation dégradée. La section 3 dresse une liste non exhaustive des attaques possibles.

3 Classification des attaques

Variation de la puissance d'émission Un mobile modifiant sa puissance d'émission alors qu'il est déjà connu du système va introduire une altération de l'estimation des distances entre les points d'accès et lui-même, et donc une erreur dans le calcul de sa position. Cette erreur sera temporaire si le système parvient à se rendre compte de

la modification, auquel cas il modifiera les paramètres associé au mobile concerné. En revanche, si ce dernier a pour but de perturber le système, il modifiera fréquemment sa puissance d'émission, ce qui perturbera fortement le calcul de sa position si le système n'est pas assez réactif.

Modification de l'adresse MAC De la même manière, un mobile modifiant sa propre adresse MAC disparaîtra à la vue du système, au profit d'un autre. En comparant les positions des deux mobiles (le disparu et le nouveau), il est relativement facile de s'apercevoir de la supercherie. Mais si le mobile s'est beaucoup déplacé entre sa disparition et sa réapparition, ou si de nombreux attaquants modifient simultanément leurs adresses, la tâche est nettement complexifiée.

Vol d'adresse MAC Une variante de la simple modification de son adresse MAC est le vol d'adresse. Un mobile peut déclarer une adresse MAC appartenant à un autre mobile, préalablement connu du système. Non seulement le mobile attaquant pourra avoir accès à d'éventuels services fournis au mobile connu, mais ce dernier ne pourra plus être positionné par le système.

Brouillard de guerre Une autre variante consiste à ce que plusieurs mobiles attaquants déclarent la même adresse MAC et envoient des paquets identiques. Le système aura alors l'impression qu'il s'agit d'un seul et même mobile, et calculera une position erronée.

Déni de service Le système peut également être victime d'attaques plus classiques, telles que le déni de service, éventuellement distribué. Des mobiles attaquants peuvent en effet inonder le réseau radio de paquets quelconques, et ainsi surcharger l'infrastructure, en plus de ralentir le réseau Wi-Fi de manière globale.

La prochaine version d'OWLPS tente de répondre à la problématique de l'intégrité du service de positionnement en résistant à ces différents types d'attaques.

References

[1] Matteo Cypriani, Frédéric Lassabe, Philippe Canalda et François Spies : Open wireless positionning system: a Wi-Fi-based indoor positionning system. *In VTC-fall 2009, 70th IEEE Vehicular Technologie Conference*, Anchorage, Alaska, septembre 2009. IEEE Vehicular Technology Society. 5 pages.

[2] Interlink Networks, Inc. : A practical approach to identifying and tracking unauthorized 802.11 cards and access points. Rapport technique, 2002.

[3] Frédéric Lassabe : *Géolocalisation et prédiction dans les réseaux Wi-Fi en intérieur.* Thèse de doctorat, École doctorale SPIM, 2009.

Laboratoire d'Informatique de l'université de Franche-Comté
UFR Sciences et Techniques, 16, route de Gray - 25030 Besançon Cedex (France)

LIFC - Antenne de Belfort : IUT Belfort-Montbéliard, rue Engel Gros, BP 527 - 90016 Belfort Cedex (France)
LIFC - Antenne de Montbéliard : UFR STGI, Pôle universitaire du Pays de Montbéliard - 25200 Montbéliard Cedex (France)

http://lifc.univ-fcomte.fr