

Internet Area Working Group
Internet Draft
Intended status: Standards Track
Expires: July 16, 2020

Rob Brew
Rydal Inc.
January 2020

**GPS Over WiFi.
draft-brew-intarea-underground-01**

Abstract

When users are at known underground locations, such as tube stations they often do not have a GPS signal, as the radio waves from the satellites required cannot penetrate the earth, this draft suggests providing GPS locations over WiFi using remote IP detection for a server to respond with the correct name of clients location and the clients GPS location.IP address.

Extending this to those without WiFi access the standard goes one stage further, by offering a hidden WiFi network with a standard name, such as .location. The principle being that mobile devices can look for this network in cases where GPS data cannot be collected. It is hoped that this will allow those using mapping services to know where they are when travelling on underground trains etc.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 13, 2018.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

1. Introduction

1.1 Motivation

Those travelling underground networks, such as the London underground or the German autobahn do know where they are when underground. At best apps such as citymapper will estimate where people are based on the time the carriage takes to get to their location. It would be convenient for them to know where they are. This protocol resolves this problem, not just to those who have a wireless location but also to those who do not.

1.2 The code for this servlet, implemented in Java running on tomcat8 is available at <https://www.github.com/rydal/underground>.

1.3 Security considerations: In order to prevent spoofing of the location https can be used.

1.4 IANA Considerations:

This document has no actions for IANA.

2. Mechanisms.

2.1

The Server, with the aforementioned outline code, knows the IP address of the WiFi hot spot. It holds a list of GPS locations, related to the IP address of the provided underground network. Using this list it responds to the client (the Wireless network of the underground network), with the relevant GPS co-ordinates of the physical site being referenced by the incoming IP address. The server responds with a name of the location, it's GPS latitude and GPS longitude in a JSON array.

2.2:

Making this more accessible, including to user's not currently connected to a WiFi network, we can implement a hidden wireless network with a standardized name, such as ".location".

The operating system's of mobile phones can then search for such a wireless network when GPS is unavailable. The hidden

wireless network can then act in the same manner as described in [section 2.1](#).

2.3:

As referenced in [section 1.3](#). Standard https encryption can prevent location spoofing.

3.

Interested parties:

The transport organisations for the relevant underground locations would need to be involved in this to provide said wireless networks. The mobile manufacturers would need to add a function to their GPS location code.

Author's Address

Rob Brew

flat 5, Rydal mount, 20 hayne road, beckenham, kent, br3 4hy
UK

Phone: +44 7782200684

EMail: sputnik2012@gmail.com