# Decentralised location proof system

Conor Taylor

B.A.(Mod.) Computer Science
Final Year Project, April 2016
Supervisor: Stephen Barrett

## Abstract

# 1 Introduction

## 1.1 Project and Motivation

Location verification is the process of verifying whether or not a mobile node (computer) is physically present at the location it claims to be. Existing location verification systems attept to provide this service using centralised, trusted "authoritive" nodes to provide proof of a mobile node's location. These approaches require investment in infrastructure, and are subject to data breaches and denial of service attacks. This project aims to present a *decentralised* solution to this problem, in which there is no "authoritive source" trusted and relied upon to provide and store location information.

This project will focus on obtaining location proofs by using other untrusted mobile nodes as *alibi's*. Proofs will be created over an ad-hoc peer-to-peer network, encrypted, and published on a public append-only bulletin board, known as a *blockchain*. The decentralised nature of the system means that there is no single point of failure, and no one entity controlling the security of every node's location proofs.

# 2 Background

## 2.1 Proving your location

As an increasing amount of personal information is accessible on the internet and therefore on mobile devices, the security that existed by requiring physical interaction between humans to transfer sensitive data is lost.

## 2.2 Ad-hoc networks

## 2.3 Blockchain

## 2.4 Centralised location proof systems

Location proof systems are expected to be accurate and tamper-proof. For this reason, existing solutions have chosen to use a central authority to issue proofs, or to regulate proof issuance [1, 2, 3].

A hardware technique [1] operates by supplementing existing WiFi access points with *femtocells*. A femtocell is a small cellular antenna that connects to a mobile carrier via the Internet. Location verification over the internet is made possible by determining which femtocell a mobile node is connected to as it transfers data via Wi-Fi. This solution requires investment in additional hardware to supplement existing WiFi access points, and requires access to mobile providers' user database to identify users locations.

The use of a centralised system, like that described by Brassil et al. [1], creates security, privacy and vulnerability issues. An attacker who succeeds in compromising the security of the central server can violate the privacy of the users of the system, and potentially track their location. The central system architecture is also vulnerable, in the sense that a resource availability attack such as a DDoS attack could render the central architecture unavailable, making location verification unavailable.

Luo et al. propose a system that uses Wi-Fi access points (*AP's*) to allow users to create location proofs [2]. In their system, each access point has a *group signature* and can sign location proofs for requesting users. Users can request a location proof from any access point, and receive a proof encrypted by the AP with the group signature, as shown in figure 1. This can then be submitted to a Verifier.

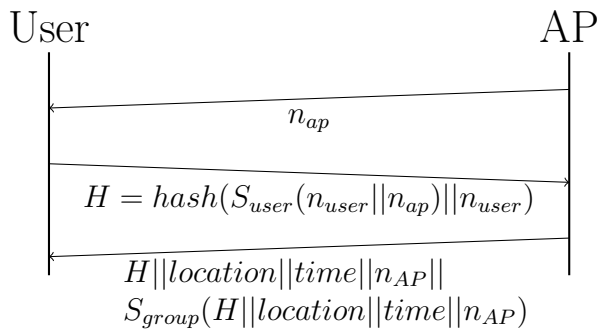


Figure 1: Adopted from Luo et al. [2]

This kind of system creates *proactive* location proofs. A proactive location proof is one which is created before it is needed. The user creates application-independent location proofs, and can use them at a later time with any application(s) he chooses.

# References


[1] J. Brassil, P.K. Manadhata, "Verifying the Location of a Mobile Device User", Proc. of MobiSec 2012, June 2012.

[2] Luo, W., Hengartner, U., "Proving your Location without giving up your Privacy", Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, HotMobile 2010, Annapolis, Maryland, February 22 - 23, pp. 712. ACM, New York (2010)

[3] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, "'Who, When, and Where?' Location Proof Assertion for Mobile Devices", Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, ser. DBSec. IFIP, July 2014.

[4] Khan, R., Zawoad, S., Haque, M., Hasan, R. "OTIT: Towards secure provenance modeling for location proofs", Proc. of ASIACCS. ACM (2014)

[5] Douceur, J.R., "The sybil attack", Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251260, Springer, Heidelberg (2002)

[6] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems", SysSec Technical Report, ETH Zurich, April, 2008