Computer Communications 48 (2014) 30–43

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Privacy-aware message exchanges for HumaNets

Adam J. Aviv [a,*], Matt Blaze [b], Micah Sherr [c], Jonathan M. Smith [b]

[a] United States Naval Academy, Annapolis, MD, United States
[b] University of Pennsylvania, Philadelphia, PA, United States
[c] Georgetown University, Washington, DC, United States

ARTICLE INFO

Article history:
Available online 16 April 2014

Keywords:
Opportunistic networking
Privacy
Geographic routing
Location privacy
Anonymous communication

ABSTRACT

This paper describes a novel privacy-aware geographic routing protocol for *Human Movement Networks* (HumaNets). HumaNets are fully decentralized opportunistic store-and-forward, delay-tolerant networks composed of smartphone devices. Such networks allow participants to exchange messages *phone-to-phone* and have applications where traditional infrastructure is unavailable (*e.g.*, during a disaster) and in totalitarian states where cellular network monitoring and censorship are employed. Our protocol leverages self-determined *location profiles* of smartphone operators' movements as a predictor of future locations, enabling efficient geographic routing over metropolitan-wide areas. Since these profiles contain sensitive information about participants' *prior movements*, our routing protocol is designed to minimize the exposure of sensitive information during a message exchange. We demonstrate via simulation over both synthetic and real-world trace data that our protocol is highly scalable, leaks little information, and balances privacy and efficiency: messages are approximately 20% more likely to be delivered than similar random walk protocols, and the median latency is comparable to epidemic protocols while requiring an order of magnitude fewer messages.

Published by Elsevier B.V.

1. Introduction

The ubiquity of smartphones enable new communication models beyond those provided by cellular carriers. While standard cellular communication uses a centralized infrastructure that is maintained by the service provider, smartphones have communication interfaces such as ad-hoc WiFi and Bluetooth that allow direct communication between devices. Since smartphone owners often carry their devices, leave them on, and encounter other individuals (and their smartphones) in their daily routines, *smartphones enable fully decentralized store-and-forward networks that completely avoid the cellular infrastructure.*

1.1. Human movement networks

(HumaNets) [1,2] fit this model and are designed to allow participants to exchange messages phone-to-phone without using any centralized infrastructure. HumaNets' "out-of-band" message passing is applicable when cellular networks are unavailable or if the networks are untrusted (*i.e.*, operated by a totalitarian state that censors [3], shuts down [4], or otherwise leverages its communication systems to restrict its citizenry [5]).

Rather than rely on network addresses, HumaNets route messages using *geocast* – an addressing scheme that directs messages towards a particular geographic region. Such a messaging system could be used, for example, to notify a group of people in a targeted area of an upcoming event, or to warn them of some impending crisis. To cope with mobility, HumaNet routing protocols route messages based on message carriers' predicted *future* locations. This is accomplished by leveraging self-determined *location profiles* that approximate the smartphone owners' routine movements. The patterns of human mobility – for example, the daily commute to and from work – serve as predictors of future locations. HumaNets take advantage of this observation by greedily forwarding messages to smartphones whose owners' location profiles indicate that they are good candidates for delivery.

Privacy issues must be central when designing a HumaNet routing protocol since location profiles contain sensitive information about participants' *prior movements*. The disclosure of such information is particularly dangerous when HumaNets are used for covert communication in totalitarian regimes. Existing decentralized routing approaches that do not consider privacy [6,7], rely on trusted third parties [8], or assume *a priori* trust relationships [9] are also unsuitable for HumaNets.

* Corresponding author. Address: 572M Holloway Road, Stop 9F, Annapolis, MD 21402-5002, United States. Tel.: +1 410 293 6655; fax: +1 410 293 6800.
E-mail addresses: aviv@usna.edu (A.J. Aviv), blaze@cis.upenn.edu (M. Blaze), msherr@cs.georgetown.edu (M. Sherr), jms@cis.upenn.edu (J.M. Smith).

http://dx.doi.org/10.1016/j.comcom.2014.03.013
0140-3664/Published by Elsevier B.V.

This paper proposes a novel routing protocol for HumaNets that protects participants' location profiles from an adversary who wishes to learn previous movements and/or determine "important" locations of network users (*e.g.*, home, work, or the location of underground activist meetings). Our technique, which we call *Probabilistic Profile-Based Routing* (PPBR), balances performance and privacy by efficiently routing messages in a manner that minimizes the exposure of users' location profiles. We demonstrate through trace-driven simulations using both real-world and synthetic human movement data that our PPBR protocol is highly scalable, efficiently routes messages, and preserves the privacy of profile information. In summary, the contributions of this paper are:

- The introduction and design of a fully decentralized, privacy-preserving, geographic-based HumaNet message routing protocol for smartphones;
- An analysis of the privacy and security properties offered by our routing protocol;
- A trace-driven simulation study (using both real-world and synthetic data) that evaluates our method's scalability and efficiency.

2. Network assumptions and goals

To achieve reasonable performance, HumaNets leverage humans' tendency to follow *routines*: The locations that people frequented in the past are predictors of their future locations [1]. However, a device's location history may be extremely sensitive, and moreover, combining multiple nodes' location histories may allow an adversary to discover social networks and enumerate participants' movements. Hence, the high-level goal of our PPBR protocol and the central challenge of this paper is to enable *efficient geographic-based messaging that limits the exposure of information at message exchanges*. In particular, an adversary who witnesses a message exchange should learn little *important* information about the participants' location histories.

Importantly, however, our HumaNet routing protocol does not conceal the identities of the network's participants. An adversary who intercepts a PPBR message can reasonably conclude that the sender is participating in a HumaNet. Participating in a HumaNet inherently carries risk if used as an anti-censorship technology: This is unfortunately true of any system that may be deemed "subversive". However, when other means of communication are impossible (either due to global monitoring or blocked connectivity), HumaNets provide a *means* to exchange information in a manner that is efficient, scalable, difficult to surveil, and privacy-aware.[1]

2.1. Requirements

HumaNets routing protocols are designed for location-aware mobile devices. We assume that network participants can learn their locations (*e.g.*, via GPS[2]) without relying on the cellular service provider's network, and that devices contain sufficient storage to record their movement histories. We note that current generation smartphones meet HumaNets' modest storage and processing requirements.

If GPS is used to determine location, the GPS receiver needs to be activated intermittently and only during regularly scheduled times during which HumaNets messages are exchanged. As recent work notes that GPS reception increases power consumption on smartphones only by approximately 15% [10], we expect the power consumption due to HumaNets to be manageable. Additionally, if any other application on the smartphone requests location information, HumaNets software may use the "last known position" OS feature to determine location with negligible cost. We evaluate the energy costs of our routing scheme in more detail in Section 5.11.

We additionally assume that participants have knowledge of the routing area. Since HumaNets enable geocast routing, a message that is targeted at specific receivers requires the sender to have some knowledge about the receivers' likely future locations (*e.g.*, their home or work); this requirement is similar to that imposed by traditional networking where users need knowledge of a service's hostname or IP address. We also assume that participants know some coarse-grain information about general movement statistics over the routing area. In particular, nodes should be capable of estimating the "popularity" of city areas – *e.g.*, that the upper west side of Manhattan is more densely traveled than Far Rockaway, Queens. This information can be obtained from census data, other public source of information, or personal experience. Such information can be shipped with the HumaNets software and is assumed to be known to an adversary.

2.2. Threat model

We envision both passive and active adversaries. A passive adversary may have any number of confederates and is able to observe message exchanges at a fixed number of locations throughout the HumaNet routing area. An active adversary may additionally participate in HumaNets by generating fake messages, accepting messages, and/or dropping or misrouting messages.

We do not provide protection against a *mobile targeting adversary*. An adversary that can physically follow a node can trivially learn about its whereabouts and discover its routine movements. Such a "stalker" adversary is also very costly to deploy. In this paper, we focus on less targeted attackers and assume an adversary who monitors, intercepts, or participates in local exchanges that occur in its presence. The adversary is aware of the participants and their locations at the time of an exchange, and thus we do not claim that our system provides traditional location-privacy [11] for ad hoc networks, although such extensions may be relevant here.

The adversary's goals are as follows:

- Disruption: Inject failures into the network such that messages can no longer be reliably delivered.
- De-anonymization: Determine the originating sender of intercepted messages.
- Profiling: Infer movement patterns of a targeted individual or learn his/her "important" locations (*e.g.*, home, work, underground meeting place).

2.3. Performance and security goals

The goal of our routing protocol is to provide the following properties in the presence of active and passive adversaries:

- Reliability: Messages should reach their intended destinations with high probability.
- Efficiency: Messages should reach their intended destinations with reasonable latency and overhead.
- Scalability: HumaNets should be able to scale to a large number of participants with many concurrent messages.
- Point-to-Point: Messages should be exchanged only point-to-point and avoid any centralized routing structures.
- Privacy-Preservation: The protocol should not leak the sender's identity, nor should it reveal information about participants' previous locations. We do not distinguish between locations

[1] It may be possible for users to use steganographic channels to conceal their participation in a HumaNet, although we do not explore such techniques in this paper.

[2] GPS is a unidirectional protocol and requires only the reception of signals from U.S.-operated satellites.