Ad Hoc Networks 25 (2015) 383–392

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Neighbour discovery in opportunistic networks

M. Orlinski [a,*], N. Filer [b]

[a] Fraunhofer IAIS, Schloss Birlinghoven, 53757 Sankt Augustin, Germany
[b] School of Computer Science, University of Manchester, Manchester M13 9PL, UK

ARTICLE INFO

Article history:
Received 21 February 2014
Received in revised form 17 July 2014
Accepted 28 July 2014
Available online 14 August 2014

Keywords:
Opportunistic networks
Neighbour discovery
Human mobility

ABSTRACT

Continuous or frequent scanning for opportunistic encounters would quickly drain the battery on existing personal mobile wireless devices. Furthermore, there is a great deal of uncertainty about when encounters between devices carried by humans will take place.

This paper will discuss some of the drawbacks of using current short range neighbour discovery technology in opportunistic networks. Finally, we proposes a new neighbour discovery algorithm called PISTONSv2 which enables mobile devices to dynamically alter the rate at which they search for others, thus creating a fully decentralised and autonomous network whilst saving energy.

1. Introduction

The goal of opportunistic networks such as PeopleNet [1], is to facilitate peer-to-peer communication using the mobility of participants and the occasional connections between them. Opportunistic networks created using personal mobile wireless devices are also sometimes referred to as Pocket Switched Networks (PSNs) because they are created using devices that are often carried in participants' pockets [2].

Rapid and unpredictable topological changes which occur as a consequence of dynamic human mobility patterns and short communication range [3] mean that opportunistic networks may not be suitable for all real-time communication. However, infrastructureless communication between personal mobile devices with fully distributed coordination is expected to facilitate a number of new applications. For example:

1. Continued, albeit limited, communication during unplanned outages of cellular communication networks [4].
2. Basic communication for developing and remote regions where it would otherwise be too expensive or difficult to do otherwise [5].
3. Provide some relief for overloaded cellular networks [6].
4. Sharing of resources between devices [7].

This paper addresses the problem of detecting encounters between mobile devices (called neighbour discovery) in opportunistic networks. Neighbour discovery is critically important because not only is data delivery latency within the network constrained by transmission range, bit rate, and the movement patterns of devices, but also by the rate at which devices scan for others [8].

However, current personal mobile devices cannot be in a constant state of neighbour discovery as this would lower the battery life to the point where they need to be fully recharged at least twice a day [9]. In addition, caching of known neighbours implies an element of exploitable stability within the network which is not the case in opportunistic networks. It is therefore critically important that neighbour discovery procedures in opportunistic networks be as sensitive to change as possible as well as energy efficient.

* Corresponding author.
E-mail address: dr.m.orlinski@ieee.org (M. Orlinski).

http://dx.doi.org/10.1016/j.adhoc.2014.07.024
1570-8705/© 2014 Published by Elsevier B.V.

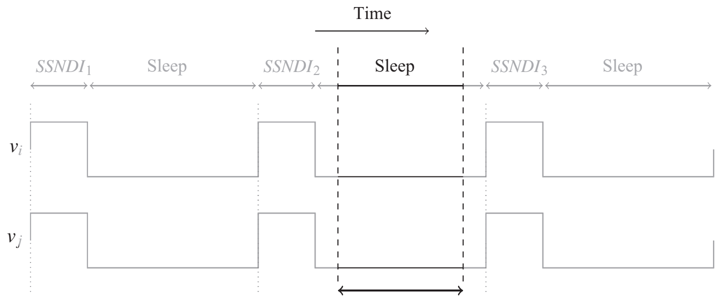

Fig. 1. An inter-probe time which is too long may lead to some short encounters being missed. In this example the devices v_i and v_j briefly come into transmission range of each other during the period p_{int}. There is no Synchronised Symmetric Neighbour Discovery Interval (SSNDI) during p_{int}, thus v_i and v_j do not discover each other.

2. Related work

The different types of signals that are sent between wireless devices during neighbour discovery can be categorised as either Neighbour Discovery Requests (NDREQs) and Neighbour Discovery Replies (NDREPs) [10], or independent neighbour discovery beacons [11,12].

The neighbour discovery procedure of Bluetooth (which is present in most smartphones sold today) uses NDREQs and NDREPs. Bluetooth's neighbour discovery procedure is also *asymmetric* in that Bluetooth devices in transmission range need to be in different but compatible states at the same time in order to detect each other [13].

Asymmetrical states are problematic for opportunistic networks because the assumption that two devices in transmission range are configured as one being the sender and the other the receiver at a particular time is not realistic [14]. Furthermore, Bluetooth devices also need to be in transmission range for long periods of time in order to discover each other and exchange data. Bluetooth 4.0: Basic Rate devices in the Inquiry state can sometimes wait up to 10.24 s (or more in error-prone environments) for a NDREP because of the time needed to perform the 1024 frequency hops outlined in the Bluetooth specification [13]. This means that discovery between stationary devices is often much more reliable than neighbour discovery between mobile devices [15].

In *symmetric* neighbour discovery there is a single state in which devices are required to support transmission, reception, and the processing of NDREQs and NDREPs or beacons. For example, the IEEE 802.15.4 standard outlines the procedure for symmetric state neighbour discovery between Full-Function Devices (FFDs) in ZigBee [16] using periodically broadcast beacons. Symmetric state neighbour discovery is more commonly used in wireless networks where it is difficult to ensure that devices are in complementary neighbour discovery states when in transmission range of one another. For example, when detecting the encounters between Zebras in Kenya [11] or in mountain rescue scenarios [17].

2.1. Autonomous neighbour discovery

So that mobile devices can detect each other in an unsupervised manner and still save energy, new methods are required that keep radios powered off for most of the time but which can still guarantee new encounters between devices will be discovered.

2.1.1. Synchronised symmetric neighbour discovery intervals

One way that personal mobile wireless devices can save energy yet still discover one another autonomously is to initiate symmetric neighbour discovery intervals *simultaneously* on every device. For example, GPS-aided time calibration and a regular operation schedule are used in Impala [11] and CenWits [17] to synchronise symmetric neighbour discovery intervals.

Synchronised symmetric neighbour discovery intervals must overlap whilst mobile devices are in transmission range so they can discover one another. If devices are in transmission range but their synchronised symmetric neighbour discovery intervals do not overlap, then encounters may be missed entirely as Fig. 1 shows, or encounters may be part detected as Fig. 2 shows. During the design of the CenWits system it was calculated that two hill walkers have 102 s to discover the presence of each other if they have a maximum transmission range of 70 m and are moving past each other on the same path. As a result, CenWits devices were configured to start a new symmetric neighbour discovery interval every 90 s.

2.1.2. Asynchronous symmetric neighbour discovery intervals

Section 6.1.2 will show that symmetric neighbour discovery intervals need not be synchronised on every device in order for the opportunistic network to function. This has the benefit of creating an opportunistic network without the need to synchronise time between devices, and allows for different participants to have different encounter patterns.

Two approaches that allow devices to choose the length of time between symmetric neighbour discovery intervals are STAR [18] and DWARF [10]. For brevity, we will now refer to the time between symmetric neighbour discovery intervals as chosen by a device as their *inter-probe time*.

STAR was produced after observing that optimal inter-probe times will vary over time [19]. However, whilst STAR