Can You See Me? The Use of a Binary Visibility Metric in Distance Bounding

Michelle Graham and David Gray

School of Computing, Dublin City University, Dublin, Republic of Ireland
mgraham@computing.dcu.ie, dgray@computing.dcu.ie

Abstract. Wireless networks are becoming more and more commonplace, with ubiquitous computing flourishing in this ever expanding environment. As this occurs, the demand for a reliable method of locating devices has also increased dramatically. Locating devices with no a prioi knowledge is a very large problem, requiring much special equipment. Instead, we focus on the issue of location verification, a smaller aspect of the location issue. Distance bounding is a well respected technique used in this area, however it relies on precise calculations to locate a device. We propose a method of locating a device which does not rely on these calculations. Instead, we employ a binary "yes/no" visibility metric, where neighbouring devices indicate whether they can "see" or communicate directly with the claiming device. We confirm the existence of a direct link through excluding the possibility of a proxied connection being employed. The intersection of the ranges of these devices can then be used to extract a location area, without relying on calculating exact distances through precise timings.

1 Introduction

The issue of location verification is relatively new to the area of research. Previously, focus was upon locating a device with no a priori knowledge. However, location verification simplifies this problem through limiting the field in which the device may possibly be located. This reduces the location verification issue to discovering whether or not a device is present within a specific area.

Location verification has a number of uses within the area of security. For example, a device may need to be granted access to some facilities within a secure network. This access should only be granted when the device is physically present within the area of the network. The system must therefore first ascertain whether the device is physically located in the area of the network, or merely using some form of proxy to gain access. We propose a method of location verification employing distance bounding which guards against proxy attacks such as this.

The technique of distance bounding was first proposed by Brands and Chaum in [1] as a method of determining the upper bound on the physical distance between two parties. This is achieved using a challenge-response scenario, where the delay between sending a bit and receiving the corresponding response bit

B. Liu et al. (Eds.): WASA 2009, LNCS 5682, pp. 378–387, 2009.

is timed and a distance extrapolated. This method of location extraction has been employed in varying approaches [2,3,4], however as the calculations are of such a precise nature, the resulting location is often inaccurate. We propose a method of verifying the location of a device in a wireless network without requiring these precise measurements. Instead, a device claiming its location (a *claimant*) distance bounds with multiple neighbouring devices (*verifiers*) in the claimed area. Each of the verifiers produce a binary yes/no verdict concerning the visibility of the claimant to them. A claimant can communicate with a verifier through either a direct or proxied connection. A direct connection is deemed to be where the claimant and the verifier are within one hop of each other in an ad hoc network. We propose that receiving a positive visibility verdict indicates that a claimant has completed the distance bounding process satisfactorily and does not appear to be utilising a proxy connection. As the only other method of communication between a claimant and its verifier is through a direct connection, it follows that a positive visibility verdict indicates that the claimant is present in the area of that verifier. This binary metric and its related issues are explained further in sect. 3.

The remainder of our paper is structured as follows: In Sect. 2, we discuss the technique of distance bounding in greater detail and examine other work in the area. In Sect. 3, we describe the use of a binary metric and how it can result in the calculation of a location. In Sect. 4, we detail the results of simulated "honest" distance bounding exchanges and those involving a proxy. In Sect. 5, we outline our plans for future work in the area of this binary metric and finally in Sect. 5, we present our conclusions regarding this work.

2 Literature Review

Distance bounding was first proposed in 1993 by Brands and Chaum [1]. The process involves a device A sending a challenge bit to device B and timing the delay between transmission and receiving the corresponding responce bit back. This delay is used to calculate an upper bound on the distance between devices A and B. In practice, a series of these exchanges is done to lessen the effects of network delays on the overall result.

Without any protection or additional security, distance bounding is vulnerable to a number of attacks, most notably the mafia and proxy attacks. The *mafia fraud* [5] is a form of *man-in-the-middle* attack where an intruder acts as both a malicious claiming device and a malicious verifying device in between an honest claiming device and an honest verifiying device. The intruder interacts with an honest claiming device as a verifier and with an honest verifying device as a claiming device, passing off the honest claimant's responses as his own. In essence this allows him to identify himself as the honest claimant to the honest verifier. The *proxy attack* is an extension of the mafia fraud, where both the claiming device and the intruder collaborate to deceive the verifying device. As in the mafia fraud, the intruder passes off messages to the verifying device from the claiming device as his own. However, unlike in the mafia fraud, the claiming device is fully aware that this is happening, and has enlisted the intruder to act