RC22500 (W0206-126) June 24, 2002 Declassified 07/31/2003
Computer Science

IBM Research Report

Device Disambiguation for a Retail Shopping Scenario

**Mandayam T. Raghunath, Stefan Berger, Stefan Hild,
Christian Hoertnagl, Herbert S. McFaddin,
Chandrasekhar Narayanaswami, Jung-Mu Tang, Miriam Zohar**

IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Device Disambiguation for a Retail Shopping Scenario

M. T. Raghunath, Stefan Berger, Stefan Hild, Christian Hoertnagl, Scott McFaddin, Chandra Narayanaswami, Jung-Mu Tang, Mimi Zohar
IBM Research

Abstract

Consider a scenario where a customer purchases several items at a retail store and wishes to pay for these purchases using a wireless mobile device at an unstaffed store kiosk. The kiosk has both wired and wireless connectivity. One of the problems that needs to be solved in the context is the pairing of the mobile device with the correct kiosk. We refer to this as the disambiguation problem. This report discusses several issues associated with the disambiguation problem and presents solutions to this problem.

1 Introduction

Mobile devices are rapidly improving in terms of their computing and storage capabilities. For instance, many of today's hand-held devices are powered by processors that run at a few 100 MHz and have few tens of megabytes of memory [1]. In terms of raw capabilities these hand-helds are more powerful than desktop computers which were considered top of the line less than a decade ago. Technological improvements have also led to increased capabilities in other mobile devices such as laptop computers, cell phones and even wrist watches [2].

A range of different communication technologies are also being leveraged to enable such mobile devices to connect to the networking infrastructure. At the lowest level the communication technology can be a wired connection such as a serial or ethernet cable. Wireless technologies such as 802.11 [3] are also becoming common place.

In the light of these advances in computation and communication capabilities of mobile devices, it is becoming possible to use mobile devices in everyday interactions and transactions. A number of different technical problems need to be solved to realize this vision. We consider one specific problem in this technical report: the *device disambiguation problem*.

2 The Disambiguation Problem

Consider a scenario where a customer purchases several items at a retail store and wishes to pay for these purchases using a mobile device at an unstaffed store kiosk. The *device disambiguation* problem as applicable to this scenario is as follows: There can be multiplicity of mobile devices (carried by shoppers) {D_1, D_2, .. D_n} in close proximity to multiple kiosks {K_1,K_2, .. K_m}. Let the shopper carrying device D_i wish to make a purchase at Kiosk K_j. The problem of device disambiguation is how to make the correct association between D_i and K_j. After the correct association has been made, the kiosk and the shopper's device can communicate with each other to complete the shopping transaction.

In the particular example of a shopper transacting at a kiosk the disambiguation must be achieved based on physical proximity and orientation. In other words, the shoppers device needs to find the particular kiosk that is in front of, and facing the shopper.

In other examples other criteria may apply. Thus, one generalization of the disambiguation problem is that of finding a partner device from amongst all possible partner devices such that some selection criteria C is met. In examples where more than one device meets the selection criteria, we may want to maximize some selection metric. For instance we may want to find the *closest* printer on the same floor, that can print a document in 600 dpi color.

A further generalization of the disambiguation problem is that of making an association between some small subset of devices (from amongst a larger collection of devices) while maximizing a scenario-dependent selection criteria. This subset of devices can subsequently communicate with each other to perform a task of interest to one or more users.

It is important for the mechanism that achieves disambiguation to be simple and intuitive. Any explicit actions on the part of the shopper should be minimal, and suited to the limited user interface capabilities of mobile devices.

As we will see below, solutions to this problem are not trivial, even for the specific case of the scenario outlined above, especially when we need to deal with a diverse set of mobile devices which are characterized by a range of different form factors and different user interface and communication capabilities.

3 Simplistic solutions based on specific communication mechanisms

One easy way of solving the disambiguation problem is to require the mobile devices and the kiosks to implement a communication mechanism that can determine the pairing. In other words, the kiosk and the mobile device implement a communication mechanism that limits the number of mobile devices that can be paired with a particular kiosk to exactly one in all practical situations.

There are many examples of such mechanisms. Wired connections are a good example. Another example is to use a short-range RFID [4] reader on the kiosk. The mobile device could have an identifier that is recorded on it using an RFID tag. In order for the kiosk to read the tag, the mobile device will have to be placed within this small range of sensitivity. If the range is small enough, we can rule out the possibility that more than one mobile device can be in the range of the kiosk's RFID reader.

A third example is IrDA [5], which is a narrow beam line-of-sight communication mechanism. The user of the mobile device will have to aim the IR beam from the mobile device to the kiosk's IR receiver. By making the cone of communication narrow the IR mechanism can ensure that there is no ambiguity as far as which mobile device is communicating with which kiosk.

Many other examples such as physical cable connections, magnetic stripe readers, laser pointers, bar code reader based mechanisms, etc., all fall into this category.

The problem with solutions that rely on particular communication mechanisms is that we cannot mandate particular mechanisms for all mobile devices that people would be willing to carry. Mobile devices will come in different form factors, and each device will implement communication mechanisms that are appropriate to its form factor, battery capacity and other characteristics. Further, a mechanism that solves the disambiguation problem in the manner described above, may not be appropriate for general inter-device communication. For instance, RFID tags are powered by energy from the reader and they send their identifier back to the reader. Simple RFID tags are unable to download and process data from the kiosk. Even if the mechanism is capable of establishing a two-way communication link (such as IrDA, for instance), it may be cumbersome for the shopper to hold the mobile device in the position and orientation for the entire duration of the transaction.

Hence, one may envision the use of such a mechanism only for the disambiguation step, and then revert to another communication mechanism (such as WiFi, for example) to conduct the data communication itself.

4 More generalized solutions

For the reasons described above, we believe that requiring both the kiosk and the device to implement a common disambiguating communication is overly restrictive. While we may be able to leverage communication mechanisms when they are available, we still need to find a way to solve the disambiguation problem when the underlying communication mechanisms do not help.

We will use our shopping scenario as a background in the following discussion, although some of our observations and solutions may be applicable to the more general disambiguation problem as well.

For the rest of Section 4 we assume that all the mobile devices in the store are able to communicate with all of the kiosks in the store. Further, from the view point of the communication mechanism all kiosks appear similar (equidistant from a communication perspective) to each mobile device. Likewise, all mobile devices appear similar to each kiosk. For instance, this assumption is valid when the mobile devices and the kiosks are connected to each other over a 802.11 LAN, or when some other wide-area wireless communication (like GSM) is used.

4.1 Solution based on user input on kiosk

Due to the energy requirements associated with communication from mobile devices, we believe that it is reasonable to assume that the mobile device will not be constantly connected to the network or other communication infrastructure. In the context of the scenario, we assume that the user of the mobile device will initiate a connection to the store's network at some point before arriving at the kiosk. A typical usage scenario might be to connect to the network upon entering the store and remain connected until the transaction is complete. Alternatively, the connection may be established just before the shopper is ready to check out.

When the connection is established to the store, the store, and all of the kiosks in the store become aware that a particular mobile device is in the store, or at least can learn of the availability of the newly arrived device by interrogating the store's LAN infrastructure. When the shopper subsequently walks up to the kiosk the two devices need to "disambiguate" and establish a data link. This involves that either the kiosk identifies the device that has now approached the kiosk from among the ones that are on the store's network, or that the device takes the initiative and identifies the kiosk. In both cases, what this effectively implies is that the two devices learn the current network address of their intended communications counterpart. If the shopper knows the network address of his device, the problem can be solved trivially by having the shopper enter the network address on a keyboard or other input device attached to the kiosk (limited input capabilities may make it difficult to enter the network address of the kiosk on the mobile device). However, network addresses are unlikely to be shopper-friendly. Further it is likely that the network address of the mobile device is automatically assigned by the communications infrastructure using mechanisms such as DHCP [7] or IPv6 auto-configuration [8]. Therefore, the device address may change as the device roams between communication networks (which, for example, may happen as the shopper moves between stores). Even if we were to use a fixed address such as a 802.11 MAC address [3], it is unlikely that the shopper will be able to remember this address. Humans can remember names far better than a string of hex digits.

Therefore, any solution that requires the shopper to enter something on the kiosk, must rely on names or other text strings that people can remember easily. Further, shoppers are more likely to remember names if we permit the shoppers to choose these names on their own. As part of the initial connection to the network, the mobile device should therefore send its name to the store. The store maintains a table of a associations between the device's network address and the device’s name. When the device leaves the store and network address is eventually released, the store can delete the entry from the table.

Subsequently when the shopper enters this name on the kiosk, the kiosk can look up the name that was entered in the table to find the network address of the shopper’s mobile device and connect to it. To make it simpler for the shoppers, the names may be displayed in a list on the kiosk and the shopper can select the name from a list instead of typing it in.

When shoppers pick their own names, it is possible that two different shoppers select the same name for their mobile devices. Since these names are not (and cannot be) administratively managed to ensure that they are unique, we need to find a way to deal with duplication in the names.

The name duplication problem can be reduced significantly by asking the shopper to pick two names: a primary and secondary name for their device. If there is a duplication of the primary name, the secondary name can be used to resolve the ambiguity. If the names are chosen independently it is highly unlikely that there will be a conflict in both the primary and secondary name.

4.2 Solution based on user input on the mobile device

We can flip the above model around so that the shopper enters the name of the kiosk on the mobile device. The kiosk names can be displayed prominently on the kiosks for all shoppers to see. After the shopper enters the name of the kiosk on the mobile device, the mobile device can look up the network address corresponding to the name entered and establish a connection to the appropriate kiosk. Guaranteeing uniqueness of kiosk names should be relatively easy since they are all under the same administrative domain, managed by the store.

This solution requires the mobile device to support the ability to enter text. Depending on the form factor of the device, text entry may be cumbersome, and selection from a list may be easier than actual text entry. To support list selection, the store will have to send a list of all kiosk names to the mobile. However if the store is large and has a large number of kiosks, even list selection may be difficult. If location information is available, the store may shorten the list of kiosks based on proximity; For example, only kiosks on the same floor as the mobile device may be presented.

In the discussion so far, we have assumed that each shopper is carrying only one mobile device. However, it is conceivable that a shopper is actually carrying multiple mobile devices, all of which are capable of performing the transaction. When the shopper enters the kiosk’s name on a mobile device, the shopper automatically selects one of the devices he or she is carrying for the transaction.

4.3 Solutions based on precise location

If the store has a precise geometric model of the locations of the store kiosks and there is infrastructure that can help precisely determine the location of mobile devices, the location information can be used to determine which mobile device is in front of which kiosk.

Unfortunately, indoor location tracking is still a hard problem [9]. GPS receivers do not usually work inside buildings and can rarely provide location information that is precise enough to resolve ambiguities, such as pinpointing the particular kiosk in question when a shopper is standing in front of a row of such kiosks.

The location of the device may also be pinpointed by tracking it’s RF communication signal. For example, one may record the presence of the mobile device in a particular 802.11 cell or within a particular BlueTooth^{TM} [6] piconet. It is further possible to measure signal strength and use it to deduce the relative distance from the access point to enhance the accuracy of the position information. Unfortunately this may still not be accurate enough to distinguish between kiosks spaced apart by only a couple of feet. Even so, such location information may be useful in reducing the search space of the possible device pairings.

Eventually, standard schemes for precise location determination may evolve. When such schemes are implemented on a large subset of mobile devices, location information may be used to solve the disambiguation problem.

4.4 Privacy issues

In the solution described in Section 4.1 the mobile device provides its names to the store without any user intervention. Any store that the shopper enters, carrying the mobile device, will have access to the name. Therefore it is important that these names have no secrecy value. The shopper should be willing to give these names to anyone who asks or cares. The shopper may also want to change these names periodically. The only important feature of these names are that the shopper can easily remember them. Examples of such device names may be:

- Shopper's first name.
- Name of shoppers pet goldfish.
- License plate number of first automobile owned by the shopper.
- Favorite ice cream flavor.

Obviously unique identifiers such as the shopper’s social security number or credit card numbers should not be used as names for the mobile device.

4.5 Security

The disambiguation solutions described above are susceptible to attacks where a wrong association can be made between devices due to erroneous input by a shopper, or due to an attacker mounting a successful attack on the disambiguation process. In this section we describe some of the possible attacks and motivate the need for security mechanisms to protect against such attacks.

In the solution of Section 4.1, the shopper might make a mistake in entering the name on the kiosk. If the wrong name actually belonged to some other mobile device currently in the store, the kiosk could initiate a connection to the other device. Alternatively, a malicious individual (attacker) can discover the name of a particular shopper’s device[1] and enter that name on a different kiosk, causing that kiosk to initiate a connection to the victim’s device. Therefore, it is possible that though device disambiguation has occurred, it might not be what the shopper intended.

Similar attacks can be mounted on the solution described in Section 4.2. Attacks on this solution may be easier since kiosk names have to be displayed prominently for all shoppers to see. Therefore an attacker could easily initiate a connection from his or her mobile device to the kiosk that another shopper intends to transact with.

For these reasons, it is important to incorporate additional handshakes and security mechanisms to ensure that a successful attack on the disambiguation process does not result in the shopper giving up any private or confidential information to the attacker. For instance, the shopper may be required to enter a password, or a credit card number at the kiosk to complete the transaction. Security mechanisms are needed to prevent an attacker’s device from getting access to such information.

One way to make the disambiguation process safer is as follows. As part of the connection establishment, the mobile device could generate a random (one-time) string and present this string on its display. When the kiosk tries to establish a secure communication channel with the shopper’s mobile device, the mobile can request the kiosk to present this secret string. The kiosk prompts the shopper, who reads the string off the mobile device and enters it on the kiosk. The kiosk then sends the string to the mobile device, which verifies it and permits the connection. For usability reasons it is desirable to keep the string simple, say a random 6 digit number. This security mechanism relies on a couple of factors: it is hard for an attacker to read the secret string off the mobile device, it is hard for an attacker to guess the secret string, and even if the attacker were to observe the secret string as it is used, it has no value in the context of a future transaction because each transaction uses a randomly generated string.

We could consider flipping the above security mechanism around so that the secret string is generated by the kiosk and entered on the mobile device if we are using the mechanism described in Section 4.2. However, in this case it is conceivable that the attacker could read the string displayed on the kiosk, since the display is likely to be larger and potentially readable from a farther distance.

Additional security mechanisms may be needed to protect the entire transaction scenario from attacks. A discussion of these attacks and the defense mechanisms are beyond the scope of this paper.

5 Conclusions

In this report, we presented the problem of disambiguation in the context of a retail shopping scenario. The disambiguation problem in this scenario is the problem of determining the correct paring between a shopper’s wireless mobile device with the kiosk at which the shopper wants to complete the shopping transaction.

We discussed several ways of solving the disambiguation problem, with some solutions relying on the mobile device and the kiosk to implement a common underlying communication mechanism, and other solutions that work even when such a communication mechanism is not supported. We also discussed some attacks against the disambiguation process and suggested ways of defending against such attacks.

Our future work will address ways of generalizing the solutions presented in this report to a broader set of

[1] The attacker’s task of guessing a name is easier if all names are displayed in a list on the kiosk. If a valid name has to be typed on the kiosk, the attacker’s task is more difficult, but still feasible.

scenarios. We will also address a broader range of attacks and defense mechanisms against such attacks.

6 References

1 Hand-held platforms. http://www.handhelds.org/platforms.html

2 Narayanaswami C, et al. *IBM's Linux Watch: the challenge of miniaturization*, IEEE Computer, V 35, No 1, January 2002, pp 33-41.

3 IEEE working group for Wireless LANs. http://grouper.ieee.org/groups/802/11/

4 Radio Frequency Identification. http://www.rfid.org/

5 Infrared Data Association. http://www.irda.org/

6 The Official Bluetooth Wireless Info Site. http://www.bluetooth.com/

7 Dynamic Host Configuration Protocol. RFC 2131

8 IPv6 Stateless Address Autoconfiguration. RFC 2462

9 Nissanka B. Priyantha, Anit Chakraborty, and Hari Balakrishnan. *The Cricket location-support system*. In Proceedings of the Sixth Annual ACM International Conference on Mobile Computing and Networking, Boston, MA, August 2000, pp 32-43.