Location Discovery using Ad Hoc Networks

Anand S. Gajparia and Po Wah Yau

Technical Report
RHUL–MA–2006–6
14 September 2006

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Abstract

This paper presents a generic service which allows a device to discover the location of other devices in an ad hoc network. The service has advantages in a variety of scenarios, since it does not rely on location infrastructures such as GPS satellites or GSM cellular base stations. An outline of the technology that will be needed to realise the service is given, along with a look at the fundamental security issues which surround the use of this location discovery service.

1 Introduction

The emergence of wireless technology has provided a catalyst for industry and academia to develop numerous new applications and services. How the underlying wireless technology works dictates what services can be provided. An example of this is the emergence of ad hoc networks as a communications medium. For our purposes, ad hoc networks are a permanent or temporary collection of nodes that can communicate with each other. The distinguishing properties of such networks are that there is no pre-existing infrastructure, there is no central entity to provide network administration services, and end-to-end communication may require information to be routed via several nodes[1].

Ad hoc networks are potentially very useful in certain scenarios, such as emergency response networks, where a dynamic set of entities, such as police, fire services, paramedics and other agencies, need to intercommunicate in an environment where no communications infrastructure exists, either because there was none to start with or because it has been destroyed by a disaster. In this paper we present a service that can be provided in an ad hoc network environment that enables the location of an object to be determined by appropriately authorised users. This is achieved using ad hoc network routing principles, so that there is no need for an expensive communications infrastructure.

The first scenario involves the use of the service to locate a vehicle. One case where such a service would be useful is where a driver walks into a car park but forgets where his car is parked. The user's mobile phone can form an ad hoc network with all the cars in the car park, including the user's car and other ad hoc capable devices. On request, the user's phone can broadcast

[1]This is why ad hoc networks are sometimes referred to as multi-hop networks, where a hop is a direct link between two nodes. If wireless communications are being used then two nodes are within one hop of each other if they lie in each other's transmission range.

the car's identifier[2]. The network can then respond to the request, providing the user with details on where the car is parked. Another case where such a service would be useful is when the user's car is stolen. Depending on the scale and pervasiveness of ad hoc network nodes, the location service could be used to track the vehicle, a potentially valuable tool for the police service. This application could thus provide a low cost alternative to expensive tracking devices which use the GPS satellite system [8, 11].

A second scenario involves locating items of stock in a warehouse. We suppose that the stock items contain devices capable of forming an ad hoc network. When a warehouse worker wishes to locate an item in the warehouse, the stock items create an ad hoc network which is used to indicate the location of the desired item to the warehouse worker. Such a scenario would also vastly reduce the time and cost of stock-taking. Instead of itemising the goods found in the warehouse by going through the laborious process of checking each individual item, the process may be automated by checking the nodes of the ad hoc network.

A third application is military, appropriately given that research in the use of ad hoc networks was originally driven by military scenarios. The ability to accurately locate military devices and personnel has obvious advantages in battlefield scenarios.

Yet another set of applications is provided by the 'active office' environment [9, 25]. Here, users or even an automated telephone system can locate where colleagues are located within an 'active' building, e.g. to route telephone calls. Alternatively, a user's PC work environment might be automatically transferred to a display adjacent to their location.

Possible ways in which the service can be provided are outlined in this paper, along with a review of what underlying location discovery technologies might be appropriate to support the service. The location discovery service has some potentially very important security and privacy requirements which are also discussed, along with initial thoughts on how these requirements can be met.

2 Terminology

The following terms are used in this document, but may be used differently elsewhere. A *node* is a device which has a network interface that is participating in the ad hoc network's routing service. It may or may not be mobile, and may also be part of another network. It is important to realise that a node can actually be a large network, or it could just be a single mobile

[2]Or some other information identifying the car whose location is being sought.

device such as a mobile phone. A *locating device* is a node which wishes to discover the location of other nodes, known as *targeted devices*.

A node is a *neighbour node* of another node if it is only one hop away and within direct transmission range. If the destination node is not a neighbour node of the originator node, the data packet will have to traverse a multi-hop route consisting of *intermediate nodes*. In a specific scenario, the *sending node* is the last node to have forwarded the data packet.

There are two types of location discovery. The first is *absolute location* where a node learns the exact geographical location of a targeted device, to a certain degree of accuracy. The second is *relative location* where a locating device will discover the location of the target device relative to its own location, e.g. in terms of which direction the targeted device is located.

3 Ad hoc networks

The motivation for using ad hoc networks for this location discovery application is that ad hoc networks have the potential to be deployed anywhere, leading to true pervasive computing. They are thus not subject to environmental limitations which may prevent other technologies from working. Also, the multi-hop nature of ad hoc networks means that each device does not need sophisticated and potentially power hungry wireless communications facilities to be able to exchange information with the whole network. We assume the existence of an ad hoc network independent of any infrastructure, although there may, of course, be limited infrastructure available.

This service makes use of ad hoc routing protocols to disseminate information. We will describe an application protocol that runs over an ad hoc network. This creates various requirements on the underlying network architecture. These are discussed further in section 5.

There are two main types of ad hoc network routing protocol, namely proactive and reactive protocols. Within these categories, individual schemes use a variety of techniques to find and maintain routes. Most routing protocols are table-driven, where information is processed and stored in routing tables, but other methods have been proposed.

Reactive protocol operation is typically divided into a route discovery cycle and route maintenance. A node initiates route discovery when it needs to send a data packet to a destination whose route is unknown. This typically involves broadcasting some form of route request message, where an intermediate node or the destination node itself can provide the originator node with a reply containing the route to the destination. Route maintenance is required, as there are no periodic route update messages. Instead, when a link

break is detected between two nodes, one or both of these nodes are responsible for propagating error information about the broken link to all affected parties. Examples of reactive routing schemes are the Ad hoc On-Demand Distance Vector (AODV) protocol [15]; Dynamic Source Routing (DSR) [12], which uses 'source routes'; and Location Aided Routing (LAR) [23], which uses geographical coordinates to increase the efficiency of routing.

Pro-active protocols use periodic topology updates to disseminate route information throughout the whole network, but try to minimise the information being sent in order to save bandwidth. Various techniques are used to achieve this, as exemplified by the Optimised Link State Routing (OLSR) [5] and Topology Broadcast Reverse Path Forwarding (TBRPF) [3] protocols.

4 The location discovery service

We now give an overview of the service and introduce some terminology. An outline is then given of possible technologies that may be used to provide the service.

We suppose that the user has a collection of wireless-enabled devices, perhaps as part of a Personal Distributed Environment (PDE) [7]. When the user wishes to locate a device beyond the radio range of its own device, they can do so using one of the devices in an ad hoc network.

The locating device may or may not be currently operating in the ad hoc network being used to provide the location service. If not, the user must first perform whatever operation is required to make the device join this ad hoc network, including providing any necessary authentication credentials. Once this has been achieved, the user will need to specify the identity of the device to be located.

The location discovery service is provided using a special pair of messages sent through the ad hoc network. The locating device broadcasts the identifier of the targeted device throughout the ad hoc network using a *TrackingRequest* message[3]. When the targeted device receives the *TrackingRequest*, it unicasts a *DirectionReply* to the locating device. This *DirectionReply* is forwarded back to the locating device via intermediate nodes. When the locating device receives the *DirectionReply* it uses location information contained within the message to determine the direction and distance of the targeted device. The contents and format of the location information will depend on the underlying technology being used, and this is discussed further in section 6.

[3]This is equivalent to a Route Request message in a reactive ad hoc routing protocol.

As the nodes may be mobile, the service could be periodically re-run, so that the targeted device periodically sends a *DirectionReply*. To save power, the targeted device could even be instructed to sleep, checking less incoming messages. It could be instructed to wake when it expects to be located by the locating device.

Possible advantages offered by this application include that it allows smaller devices with restricted battery power to participate, and not every device needs location aware hardware such as a GPS receiver. The service is designed to cope without an infrastructure, but is capable of taking advantage of an infrastructure should it be available. Section 9 gives a brief description of how similar services are offered by other technologies.

The success of the service will depend on the density of ad hoc network deployment in the area in which the user is located. If there are no nodes to form an ad hoc route from the user to the target device, then clearly the system will not work.

5 Requirements and Architecture

This section outlines the requirements on devices that are to be involved in the provision of this service, and introduced two possible scenarios — an infrastructure based scenario, and a pure ad hoc network based scenario.

5.1 Requirements

Every device which is to be located using the scheme described here must be capable of broadcasting its identifier. Any device that the user wants to use as a locating device will need to store the identifiers of all the devices that the user may wish to locate. All devices should be able to operate within the ad hoc network using the existing routing protocols.

The locating device will need to have a measure of location-awareness, i.e. to have some information about its current location. This is necessary in order for the locating device to be able to provide a user-accessible interpretation of the location information it receives regarding the targeted device. The location-awareness may be absolute and precise, e.g. as provided by a GPS receiver, or it may only be relative to some other device.

The locating device will also need a user interface capable of conveying location information to the user. This might be achieved using a compass style direction indicator, or a more sophisticated graphical display. Current mobile phones and PDAs will clearly be adequate in this respect.

The requirements on the devices to be located will depend on the environment of use, and we now describe some possible usage scenarios.

5.2 Infrastructure based tracking

The first scenario makes use of an existing location infrastructure, and we use the setting of a car park. We suppose that the target device is the user's car. The car park is divided into zones, and each zone has a beacon device. These beacons simply transmit their identities either periodically, or upon request (which may be authenticated). Each car has a means of receiving and processing information from the beacons, and is also capable of acting as a member of an ad hoc network.

When a user needs to find his car, he uses his mobile phone to form an ad hoc network with all the ad hoc enabled devices, in this case including at least some of the cars in the car park. The mobile phone broadcasts a *TrackingRequest* which contains the mobile phone identifier, the identifier of the car and, optionally, the zone in which the user is located. This *TrackingRequest* is propagated throughout the ad hoc network until the request reaches the car. The car unicasts a *DirectionReply* back to the mobile phone, containing the identifier of the beacon closest to the target car (which might be determined on the basis of signal strength). When the mobile phone receives this, it could show the user a map of the car park and where the car is located. This map could be downloaded onto the mobile phone when the user enters the car park as part of a location based service. If this is not possible, then the zone identifier could be displayed and a map could be provided at frequent points on the walls of the car park.

5.3 Ad hoc tracking

In the second scenario, again concerned with locating a car, we suppose that either one or both of the mobile phone and car is not within range of a location infrastructure device. Here we need an alternative means of relaying the location information to the user. As the targeted device cannot be sure whether the locating device is linked to an infrastructure location node, it has to provide location information which is not dependent on the infrastructure. If the targeted device has a GPS device installed, it could send its location coordinates as location information. However, if the locating device has no map then this may be useless information. Even with a map, the user may still be confused as to the direction in which to move. Information which would be more useful to the user is a direction and, possibly, a distance.

This could be relayed to the user in the form of a graphical compass arrow and an estimated distance.

The location information could thus be relayed in one of the following ways:

1. *Physical route method:* This is similar to how a source route in the DSR protocol is constructed. Here, each intermediate node appends the direction from which it received the *DirectionReply* message to the Physical route field of the packet. This provides the locating device with a sequence of directions to follow in order to reach the targeted device.

2. *Periodic beaconing method:* Every intermediate node which receives the *DirectionReply* message periodically broadcasts the identifier of the targeted device, and the direction from which the *DirectionReply* was received. Thus, as the locating device moves within transmission range of an intermediate node, it can pick up the beacon. This is particularly useful when the targeted device is mobile and periodically sends a *DirectionReply* message to indicate its new location. Also, the hop count may be included in the *DirectionReply* message, indicating how many hops away the targeted device is. Thus the locating device can determine that it is getting closer to the targeted device, as the hop count in the received *DirectionReply* messages decreases.

5.4 Other scenarios

As outlined in section 1, the service is applicable to many other scenarios. A warehouse stock management scenario is ideally suited for the infrastructure tracking service, as mobility will be low and a limited infrastructure is very feasible. Here, RFID tags [21] may be used for each item, and and their presence could be picked up and collated by the infrastructure nodes.

Finally, military scenarios are likely to benefit from an ad hoc tracking service in environments where infrastructure is likely to be limited or even non-existent.

6 Location technology overview

We now propose a variety of location determining techniques which could be used to help deliver the desired service. With each scheme we provide a discussion of its relative advantages and disadvantages in the context of the location service. The likelihood is that, in order to provide an accurate

service, more than one technology will need to be combined. For example, if parts of an ad hoc network contain GPS capable devices then the location information provided from these devices could be used with other location information to provide a more accurate location service.

6.1 The GPS method

If both the locating device and targeted device can discover their coordinates using GPS, then the targeted device can send its coordinates to the locating device via a *DirectionReply* message. The locating device can readily combine the received coordinates with its own coordinates to calculate the distance and direction of the targeted device.

However, if the locating device does not know the direction in which it is pointing, it will not be able to convey this direction information in a useful form to the user. Determining the orientation of the locating device will require the device to move. In such a case the device could use its new coordinates and the previous coordinates to display a direction for the user to move towards the targeted device. This feature exists with many current GPS devices [24]. However, the disadvantage of using GPS is that it is very inaccurate indoors. Hence, using GPS would not be suitable for the warehouse scenario. Also, in this situation, GPS may not be accurate enough to pinpoint individual items.

However, the car parking scenario could readily use the GPS method, as many cars are equipped with GPS capable devices. The locating device does not need to be GPS capable, as the cars themselves can calculate a relative location for the locating device to use.

Military scenarios could use the Precise Positioning Service (PPS) [24], which give an even greater accuracy than the civilian enabled Standard Positioning Service (SPS) [24].

However, there are many disadvantages to using GPS, as has been widely discussed [19]. The relatively high cost of equipment and the lack of accuracy indoors are among the main issues with using GPS [9].

6.2 The smart antenna method

If a mobile device is equipped with a directional antenna, then this could be used to help provide the location discovery service. Ramanathan [18] gives an overview of the possible uses of such antennas in ad hoc networks, along with a discussion of possible advantages and disadvantages. Directional antennas can be used to help provide the service described in this paper

through direction of arrival (DOA) techniques. DOA techniques attempt to determine the direction from which a radio transmission has been received.

If the wireless device can determine from which direction a transmission was received, then this information can be included in the *DirectionReply* messages. If a device is also fitted with an electronic compass, then the *DirectionReply* could also include a compass heading.

The use of smart (directional) antennas would allow the service to be provided in the absence of any pre-existing location measurement infrastructure. Line of sight problems can be overcome, since the path from the locating device to the targeted device can go around obstacles.

The main disadvantage of using directional antennas for wireless communication is the size and relative cost. However, as Ramanathan [18] states, antenna size is decreasing as technology becomes more advanced.

6.3 DOA for omnidirectional antennas

A possible DOA technique for devices with onmidirectional antennas is as follows. This idea uses the same techniques that the human brain uses to determine the direction from which sound originates. A device would need two aerials spaced as widely as possible. As the device receives a reply it can determine the DOA of the *DirectionalReply* by measuring the differences between the strengths, frequencies and times of the two received signals.

Harter et al. [9] apply a similar technique by measuring the time difference between two 'bats' in order to determine the orientation of an object. They state that the greater the distance between the 'bats' the better the orientation measure.

The Cricket compass scheme [17] uses the differences in distance between sensors on a device to determine orientation. However, the authors state that, with current technology, this cannot be achieved reliably, and so they outline other techniques to improve the accuracy of their system.

7 Security Requirements

This section is dedicated to exploring the security requirements of an ad hoc network based location tracking service. The security concerns lie largely with privacy and authentication. In a hostile environment, where there may exist many nodes from multiple domains, it is possible that some nodes cannot be trusted.

An unauthorised node is defined as one which is not authorised to view location information or infer location information regarding a targeted device.

One possible security requirement is that it should not be possible for an unauthorised node to link target and locating devices. Doing so compromises the privacy of both the target device and the locating device. For example, if an unauthorised node discovers that locating device A is requesting the location of target device B, then it may be able to deduce that A is related to B. In the car park scenario, the unauthorised node could deduce that a particular car is owned by a certain person.

Another security requirement may be that it should not be possible for an unauthorised node to acquire information linking target and locating devices by posing as a targeted device, posing as a locating device, passively eavesdropping on communications, or by subverting a valid target device or locating device. Due to the likely mobile nature of devices used in ad hoc networks, the probability that they may be lost or stolen is greater than with desktop computers, for example. For this reason, particular attention must be paid to preventing access to information in compromised devices.

Security requirements may also extend to preventing unauthorised nodes learning of a device's presence. Not only should it be impossible for an unauthorised node to find the precise location of nodes, it should also not be possible for them to learn the existence of such nodes.[4]

If a traditional authentication mechanism is being used, then node existence may be inferred by receiving messages which deny access to location information. Looking at the military scenario as an example, when an enemy receives a message stating that access to some location information is denied, then they may still deduce a node exists in the direction from which the signal was received, which is an undesirable property. In this case, anonymity may also be a requirement.

Authentication mechanisms should be in place to prevent unauthorised nodes from discovering location information by accessing the location discovery service. The prevention of denial of service attacks is also a potential requirement which may be of particular importance in the military scenario; in this latter case, if location information is denied to a locating device, then the targeted device may be incorrectly assumed to be an enemy device.

An unauthorised node should not be able to acquire location information by replaying intercepted messages. This means that replay prevention is required.

Finally, it is also prudent to mention user acceptance of location systems, since this is both an important issue in its own right and a driver for security in such schemes. Some techniques, such as the location track-

[4]This contrasts with some sensor networks, where it is the task of the sensor network to detect the existence of foreign nodes.

ing and prediction service proposed by Liu, Bahl and Chlamtac [14], could arouse opposition and a low uptake of the service could potentially result. Such a reaction could occur despite the fact that, as in this latter case, the service could enhance connection reliability by managing cell handoffs more effectively.

8 Possible security solutions

Securing the routing of protocol messages should be the responsibility of the underlying ad hoc routing protocol. For example, the routing protocol should provide availability, so that if a route exists between a locating device and a targeted device, then the service should be successful in sending the location discovery service messages between the two. There are already several papers on this topic (see, for example, [26]), so we do not address this issue further here.

The control of access to the location discovery service is clearly an important issue. Conventionally, this requires the use of an authentication mechanism. This might be possible in the car park scenario, so that only locating devices within the car park, and maybe only those locating devices which have subscribed, can use the location discovery service. However, where an infrastructure does not exist it will be difficult to provide an authentication mechanism; indeed, one of the advantages of the proposed service is that it can be provided by a set of ad hoc devices which meet for the first time. One possible solution would involve device manufacturers collaborating to support a key management infrastructure for all mobile devices.

If the location messages contain map coordinates or zone identifiers, as in the infrastructure based tracking service (see section 5), then these messages should be encrypted to provide confidentiality. Integrity checks could also be provided.

Our service has the advantage over conventional ad hoc network security schemes that we can assume that the locating device and the targeted device have a security association. This is likely to have been set up by the owner of both the devices. Thus both symmetric and asymmetric cryptography could be used to provide end-to-end protection.

An important threat arises from on compromised devices. There does not appear to be a feasible means for targeted devices to determine whether or not a locating device has been compromised. Users may have the option of 'locking out' locating devices which are believed to be compromised. Unfortunately determining the locating devices which are thought to be compromised still remains a problem. Thus, the security of locating devices arises

from securing the device itself via password-authentication mechanisms and physical security.

The possible physical compromise of targeted devices to reveal their secret keys poses a more interesting problem. Again, physical security measures would ideally be provided; however, targeted devices may sometimes be too small (and low cost) to allow high level physical security protection. One solution is to use short lived keys to limit the window of opportunity afforded to an attacker who retrieves compromised keys.

9 Related Work

Much research has already been performed in this area, and many schemes have been proposed that offer a similar location tracking service using different technologies. However, not much has been written about the associated security issues. We now give an overview of the advantages and disadvantages of the various existing techniques, and also, where relevant, highlight the security concerns which have been raised. Hightower and Borriello [10] provide a taxonomy of location systems and give a survey of current research.

The 'Active Badge' location system [25] provides a similar service, but in an indoor environment. This system relies on infra-red technology, where sensors detect periodic signals emitted by 'Active badges'. These signals are collated and processed by a central server. This information is either relayed via a desktop application, or used to automate the routing of telephone calls in a Public Branch Exchange (PBX) telephony network. The 'Active badge' successor, the 'BAT' system [9], uses ultrasound techniques. The main difference between our scheme and the 'Active Badge' system is that the latter depends on a infrastructure backbone and a central server, the presence of which cannot be assumed in an ad hoc network. Also, Hightower and Borriello [10] highlight the limitations of using infrared and ultrasound technology. Want et al. [25] discuss the privacy issues arising from use of the Active Badge system. In particular, they consider concerns about the misuse of location information and giving users the right not to wear Active Badges.

The 'EasyLiving' tracking system [13] uses computer vision techniques to track the location of people in an indoor intelligent environment. Stereo camera images in the room are analysed for 'blobs', which are used to form the shape of a human figure, and additional information such as colour histograms are used for idenfication purposes. So, while the application is similar to ours, 'EasyLiving' provides a more specialised system, which again relies on an indoor infrastructure and probably also does not scale well.

Hightower and Borriello [10] again provide more technical insight into the difficulties of using vision location systems.

Typically, location based schemes are designed for use in an environment where devices can locate their own position, either on a map or by learning geographical coordinates. Wireless LANs (WLAN) have become extremely popular over the past few years, with IEEE 802.11 standards emerging as the dominant technology. Tao et al. [22] is one of many examples of research aimed at achieving location discovery of WLAN devices using radio frequency techniques(see also [20, 1]).

The Tao et al. system is designed for use indoors, and requires the presence of a number of fixed wireless access points. Thus an infrastructure is required, with a central server that controls location sensing. Initially, an offline training phase takes place, in which the server builds a conditional probability distribution in order to determine the likely future location of a target. This is achieved by the use of 'snoopers', which may be fixed access points or mobile laptops. The server can then use the conditional probability distribution with Bayesian inference to determine the location of a target WLAN device. The authors explain how to use their system to locate rogue machines which are attempting to gain unauthorised access to the building network. Whereas previous systems are vulnerable to a rogue attacker varying their broadcast power to remain undetected, Tao at al. [22] claim that their algorithms are not vulnerable to such an attack. However, they do highlight several security concerns for their system, including the possibility that an attacker could set up its own 'snoopers' and locate WLAN devices. This problem arises because wireless broadcast devices cannot choose who will receive their signals. War-driving is given as an example threat. As previously, the system has implementation problems compared to the solution we propose. There is a reliance on a centralised and fixed infrastructure. In addition, most WLAN schemes need a training period and so would not be usable in a dynamic environment. Finally, Hightower and Borriello [10] point out that WLAN technology may not be available on smaller devices.

Smailagic and Kogan [20] present a 'Portable Help Desk', so that users in a university campus can locate other users and see their contact information. They also discuss how user location privacy can be provided through the use of time scheduled rules. Each rule determines the visibility[5] of the user during a certain period of time. From a survey of users which used the 'Portable Help Desk', they reveal that users are unwilling to engage in setting up offline communications channels, preferring interactive access control or just letting anyone communicate. With respect to who can see a user online in the

[5]Visible to all, Invisible to some, Visible to some or Invisible to all.

system, again users were willing for anyone to see them, but here more users preferred offline access control.

The emergence of sensor networks has also provided a catalyst for location detection. Doherty, Pister and El Ghaoui [6] present a position estimation method for ad hoc sensor networks, in which all sensors send their connection information to a central computer that calculates the positions of every sensor in the network. In the context of our location discovery service, the central computer would be the locating device. However, this system requires that the intermediate nodes must reveal their location, which may be unacceptable for privacy reasons.

Capkun, Hamdi and Hubaux [4] introduce the Self-Positioning Algorithm (SPA) where a node can determine its own relative position in the ad hoc network. This might be useful to allow the locating device and targeted device to individually discover their own relative locations. The targeted device can then sends its coordinates to the locating device. However this system suffers from the fact that cooperation is needed between a number of nodes, where the accuracy of the system increases as the number of involved nodes rises; hence privacy issues again arise. Also, all nodes have to align their 'Network Coordinate System' to a 'Local Reference Group', and the extra overhead of control messages may be too much for a wireless network. This system would also be very vulnerable to attack. Finally, there are issues with relying on Time of Arrival techniques to determine distance.

Priyantha, Chakraborty and Blakrishnan [16] introduce a decentralised scheme based on both radio frequency and ultrasound techniques, where there is no central database of control. The 'Cricket' scheme is designed to give location support to services made available to a user. They claim that their solution is scalable and enhances user privacy. The system uses a beacon infrastructure, and thus this technology may be utilised in the car park scenario. The authors also introduce the concept of a map server, by which nodes in the network can discover what services are available by downloading an active map.

In [17], Priyantha et al. extend the scheme to create an electronic compass called 'Wayfinder', and a service discovery scheme called 'viewfinder'. The 'Wayfinder' is identical in purpose to our application. However, because of its reliance on the beacon infrastructure, and the fact that a map has to be pre-installed on the devices, our ad hoc network based solution is more dynamic and easily adaptable.

Much work has been performed on location services for cellular technology such as CDMA and GSM, and Zagami et al. [27] provide a useful overview. This work has been motivated by the E911 FCC ruling that all specialised mobile radio and personal communication systems making 911

emergency calls should be automatically located to within 125 metres. Numerous commercial GSM location services are already available in Europe. These location services operate by modifying the base stations to use time of arrival (TOA) and angle of arrival (AOA) techniques. The main advantage is that no modification of existing mobile handsets is required. The main disadvantage is that data from three or more base stations are needed to determine a position, which means that the system is sometimes not available. Zagami et al. [27] also suggest other applications for a location discovery service, such as tracking missing/lost Altzeimer's patients and also tracking tagged criminals. Many of these schemes could be used in conjunction with our location discovery tracking service to provide a comprehensive set of location functions to the user. For example, a user with a GSM phone in a car park could call the phone number of a stationary locating device in the car park. This locating device could then perform the car location service on behalf of the user. Cellular location techniques could be used to track the user, and the ad hoc location technique could be used to track the car. These could then be combined to direct the user. However, a coordinated effort is required in order to make the different systems interoperate in this way.

Finally, Bauer, Becker and Rothermel [2] present a location modelling language, which could be useful for implementing applications which use our scheme.

10 Future work

The next logical step in this research would involve an investigation into the messages transferred in this scheme. This would enable a quantitative measurement to be made of the cost of deployment of such a scheme. Further, simulation of this scheme would enable an analysis of its efficiency.

Research in the underlying technologies which would enable this service to function, such as those touched upon in section 6, could create greater efficiency in location calculation. This, of course, would also improve the general efficiency of this scheme.

The security requirements above reveal several important issues regarding the privacy of location information, and some of these have been discussed in section 8. However, much more research is needed on issues such as key management for the use of public key cryptography.

11 Conclusions

We have shown how a locating service may be useful in a variety of scenarios, and we have introduced the notion of providing such a service using ad hoc network routing principles. In particular, we have shown the requirements of an infrastructure for such a service and evaluated ways in which this may be implemented using a variety of different technologies. Security requirements for the deployment of such a service with a focus on authentication and privacy with corresponding solutions have been discussed. An overview of solutions proposed by other authors has also been provided. Finally, we examined future directions for this research.

References

[1] P. Bahl and V. N. Padmanabhan. Radar: An in-building RF-based user location and tracking system. In *Proceedings of the IEEE Infocom, March 26-30, 2000, Tel Aviv, Israel*, pages 775–784. IEEE Press, 2000.

[2] M. Bauer, C. Becker, and K. Rothermel. Location models from the perspective of context-aware applications and mobile ad hoc networks. *Personal and Ubiquitous Computing*, 6:322–328, 2002.

[3] B. Bellur and R. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In *Proceedings IEEE INFOCOM '99, The Conference on Computer Communications, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, The Future Is Now, 21-25 March, 1999, New York, NY, USA*, volume 1, pages 178–186. IEEE Press, 1999.

[4] S. Capkun, M. Hamdi, and J. Hubaux. GPS-free positioning in mobile ad-hoc networks. *Cluster Computing Journal*, 5(2):157–167, 2002.

[5] T. Clausen, G. Hansen, L. Christensen, and G. Behrmann. The optimized link state routing protocol, evaluation through experiments and simulation. In *Proceedings 4th International Symposium on Wireless Personal Multimedia Communications, September 9-12, 2001, Aalborg, Denmark*, pages 841–846. IEEE Press, 2001.

[6] L. Doherty, K. S. J. Pister, and L. El Ghaoui. Convex position estimation in wireless sensor networks. In *Proceedings of the Infocom, April 22–26, 2001, Anchorage, Alaska, USA*, pages 165–1663. IEEE Press, 2001.

[7] J. Dunlop, R. C. Atkinson, J. Irvine, and D. Pearce. A personal distributed environment for future mobile systems. In *Proceedings of the IST Mobile and Wireless Communications Summit, June 15 – 18, 2003, Aveiro, Portugal*, pages 705–709. Instituto de Telecomunicações, 2003.

[8] P. Enge and P. Misra. Special issue on global positioning system. *Proceedings of the IEEE*, 87(1):3–15, 1999.

[9] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster. The anatomy of a context-aware application. *Wireless Networks*, 8(2/3):187–197, 2002.

[10] J. Hightower and G. Borriello. Location systems for ubiquitous computing. *Computer*, 34(8):57–66, 2001.

[11] T. Imielinski and J. C. Navas. GPS-based geographic addressing, routing, and resource discovery. *Communications of the ACM*, 42(4):86–92, April 1999.

[12] D. Johnson, D. Maltz, and J. Broch. DSR — The dynamic source routing protocol for multihop wireless ad hoc networks. In C. Perkins, editor, *Ad Hoc Networking*, chapter 5, pages 139–172. Addison-Wesley, 2001.

[13] J. Krumm, S. Harris, B. Meyes, B. Brummitt, M. Hale, and S. Shafer. Multi-camera multi-person tracking for easyliving. In *Proceedings of the Third IEEE International Workshop on Visual Surveillance, July 1, 2000, Dublin, Ireland*, pages 3–10. IEEE Press, 2000.

[14] T. Liu, P. Bahl, and I. Chlamtac. Mobility modeling, location tracking and trajectory prediction in wireless atm networks. *IEEE Journal on Selected Areas in Communications*, 16(6):922–936, Aug 1998.

[15] C. Perkins and E. Royer. The ad hoc on-demand distance-vector protocol. In C. Perkins, editor, *Ad Hoc Networking*, chapter 6, pages 173–219. Addison-Wesley, 2001.

[16] N. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location support system. In R. Pickholtz, S. Das, R. Caceres, and J. J. Garcia-Luna-Aceves, editors, *Proceedings of the 6th annual international conference on Mobile computing and networking, August 6 – 11, 2000, Boston, USA*, pages 32–43. ACM Press, August 2000.

[17] N. Priyantha, A. Miu, H. Balakrishnan, and S. Teller. The cricket compass for context-aware mobile applications. In C. Rose, editor, *Proceedings of the 7th annual international conference on Mobile computing and networking, July 16 – 21, 2001, Rome, Italy*, pages 1–14. ACM Press, July 2001.

[18] R. Ramanathan. On the performance of ad hoc networks with beamforming antennas. In N. Vaidya, M. Corson, and S. Das, editors, *Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking and computing, October 4-5, 2001, Long Beach, California, USA*, pages 95–105. ACM Press, 2001.

[19] J. Reed, K. Krizman, B. Woerner, and T. Rappaport. An overview of the challenges and progree in meeting the e-911 requirement for location service. *IEEE Communications Magazine*, 36(4):30–37, April 1998.

[20] A. Smailagic and D. Kogan. Location sensing and privacy in a context-aware computing environment. *IEEE Wireless Communications*, 9(5):10–17, October 2002.

[21] Vince Stanford. Pervasive computing goes the last hundred feet with RFID systems. *IEEE Pervasive Computing*, 2(2):9–14, 2003.

[22] P. Tao, A.Rudys, A. Ladd, and D. S. Wallach. Wireless LAN location-sensing for security applications. In D. Maughan and A. Perrig, editors, *Proceedings of the ACM Workshop on Wireless Security, September 19, 2003, San Diego, California, USA*, pages 11–20. ACM Press, 2003.

[23] Y. Tseng, S. Wu, W. Laio, and C. Chao. Location awareness in ad hoc wireless mobile networks. *IEEE Computer*, 34(6):46–52, June 2001.

[24] U.S. Department of Defense. *Global Positioning System Standard Positioning Service Signal Specification*. U.S. Department of Defense, 2nd edition, June 1995.

[25] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The active badge location system. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.

[26] P. Yau and C. J. Mitchell. 2HARP: A secure routing protocol to detect failed and selfish nodes in mobile ad hoc networks. In *Proceedings of the 5th World Wireless Congress, May 25–28, San Francisco, USA*, pages 1–6. Delson Group Inc., May 2004.

[27] J. Zagami, S. A. Parl, J. Bussgang, and K. Devereaux Melillo. Providing universal locations services using a wireless E911 location network. *IEEE Communications Magazine*, 36(4):66–71, April 1998.