Location Discovery in Enterprise-based Wireless Networks: Implementation and Applications

Simon G. M. Koo, Catherine Rosenberg, Hoi-Ho Chan, and Yat Chung Lee
School of Electrical and Computer Engineering
Purdue University
West Lafayette, IN 47907-1285, USA.
{koo,cath,hchan,lee85}@ecn.purdue.edu

Abstract – We have designed and implemented a Web service for location discovery (LODS) and a location-based printing service that uses LODS on a network with wireless LAN connectivity based on IEEE 802.11 that is typical to campuses and enterprises. The need for location management and location-based services is linked to the mobility of the users. While location discovery is already implemented in cellular telecommunication networks since the system needs to know where are the users to connect them to incoming calls, the need for such a service was not so crucial in data network where in general the mobile user is the client and initiates the connections. We propose several solutions to implement our location discovery service and compare these solutions in terms of several criteria. LODS allows mobile users to find their approximate location within the campus or the enterprise and allows location-based applications to find out the location of a user to suggest the nearest points of interest, e.g., printers, restrooms, and vending machines. We will present the case of our location-based remote printing service that was deployed in Purdue wireless network.

Keywords: Web Services, Location Discovery, Wireless LAN, E-Community.

1. Introduction

Location management has been an important topic in telecommunications for a long time since the system needs to know where are the users to connect them to incoming calls. This is called *passive connectivity*, which is a requirement in cellular systems to contact or page an idle host. However, in a client-server paradigm, like a wireless LAN, there is no real notion of paging or passive connectivity. A host usually initiates a connection as a client, and, unless the host also wants to be a server, it will not be passively connected. This limits the need for location discovery mechanism. The need for location discovery adds to the complexity of the cellular system, impacts the overall architecture, and increases signaling.

In the following sections, we will describe a new Web service for Location Discovery (LODS) that was deployed in the Engineering Computer Network (ECN) of Purdue University. This service allows mobile users, using Personal Digital Assistants (PDAs) or laptops, on a wireless LAN to find their approximate location within the campus or the enterprise and allows location-based applications to find out the location of a user to suggest the nearest points of interest, e.g., printers, restrooms, and vending machines. LODS highly enhances the mobility of the hosts within a campus or an enterprise, and,

more importantly, this service is easy to deploy and does not require additional infrastructure investment. This is especially useful in a campus or enterprise environment when a mobile user needs to find the closest printers, computing lab, restroom, cafeteria, etc. Moreover, LODS is accessible directly by common Web browsers so virtually all mobile hosts can use it without purchasing additional hardware. As a Web service, LODS can automatically be accessed by other Web-based applications through a simple API call. With proper database support, LODS can also be extended to metropolitan setting with wireless network connectivity, like the wireless coffeehouse [1].

LODS provides a service for location-based applications, which facilitates the building of an e-campus or other e-communities. An example will be our current project supported by Hewlett Packard. We have developed a Web-based remote printing service, which allows any PDA with IEEE 802.11 wireless access and a Web browser to print HTML, postscript, or PDF documents and all types of images to any network-connected printer without having to download the files [2]. In the case where the mobile user is away from his office, e.g., in a different building, as shown in Figure 1, the remote-printing service can then call LODS to find the location of the PDA to suggest the nearest printer(s) to the user.

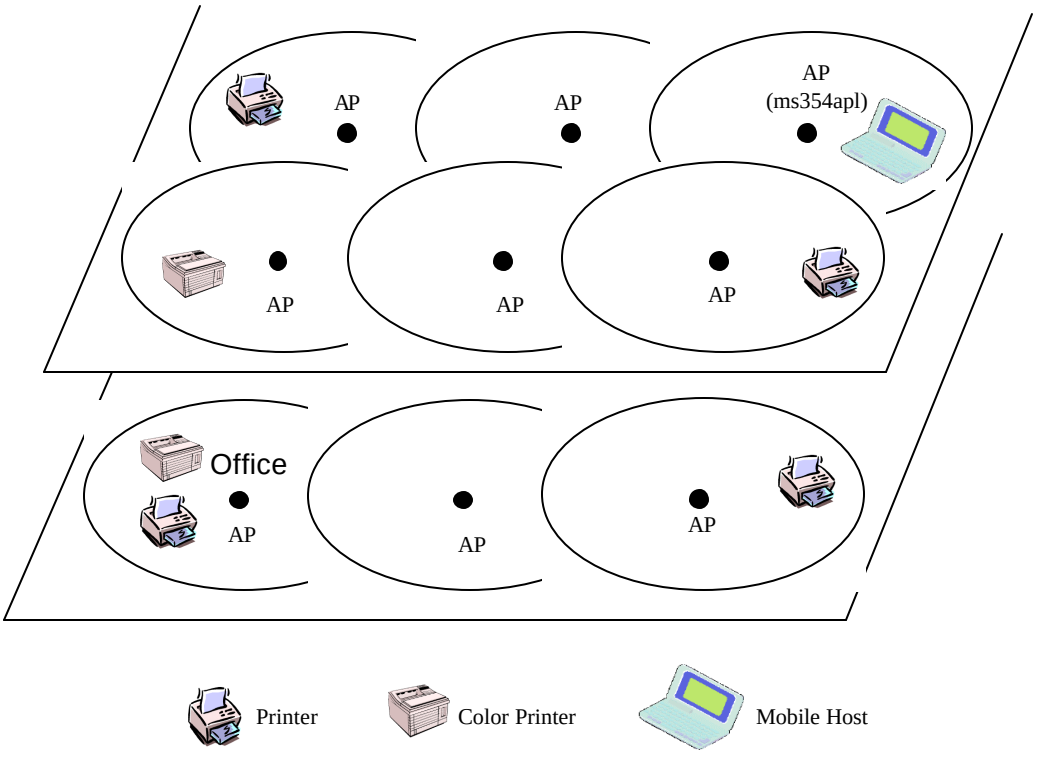

Figure 1. Remote printing scenario

We will describe LODS in details, and review some of the related works in Section 2. Assuming basic 802.11b networks setting, we proposed three schemes to track a mobile

device, and each of them will be presented and compared in Section 3. In Section 4 we will describe the applications of LODS, using remote printing service as an example. Future works and conclusion will be presented in Section 5.

2. Location Discovery (LODS)

The Location Discovery Service we designed and implemented is a Web service [3] consisting of a location discovery engine and an API for accessing the service. Upon either the direct request from the user or indirectly through the call to a location-based service, the location discovery engine will determine which access point (AP) the user's particular mobile device is currently connected to, and return the location of the AP as an estimation of the mobile's position. We believe that, to the best of our knowledge, this problem has not been addressed before. Previous work ([4], [5], [6], [7], [14], [15], [16]) has been focused on passive connectivity for which mobile devices, when idle, still have to listen to some control information, either periodically or using certain policy while in our case, users actively trigger LODS. Since it is desirable in our scenario to deploy a low cost location discovery service, our design makes use of active connectivity to locate the mobile user. We proposed three different schemes to locate a mobile user within a typical campus-wide or enterprise-wide wireless-based network that have little impact if any at all on the complexity of the system. Each of them will be discussed in details in the next section.

We need to describe what we call a typical enterprise-wide wireless-based network. A typical such network provides full wireless coverage in an enterprise comprising from few floors of a building to few medium-size buildings. It allows staff to access the Internet, their account, and their email from anywhere in the enterprise through the use of a IEEE 802.11b-enabled laptop or PDA. It consists of tens of IEEE 802.11 access points (AP) that are positioned to provide full coverage and that are interconnected through high-speed local area networks (LAN). Our solutions do not necessarily scale well to larger networks comprising hundreds of APs as will be discussed later.

Similar location service includes go2online.com [8], which is providing information about nearby restaurants, shopping place, theatre, etc. to their customers via cellular phone or Palm. The key difference is go2online.com requires their customers to input their current location to query their "Local Business Registry", while our service does not have such requirement. Our users simply logon to the service, and LODS will locate them and suggest the nearest point of interest.

3. System Description

In our network setting, all 802.11b APs are configured as transparent bridges and they are connected to some gateways via normal Ethernet. This means that it is not possible to obtain the MAC address of the AP to which a device (laptop or PDA) is connected by simply having the device sniff the headers of the incoming frames. Therefore, in order to identify to which AP a mobile user is currently connected to, we have designed three different solutions: the RADIUS approach, the SNMP approach and the device-driven approach. We have implemented the first two of them in the Engineering Computer Network (ECN) of Purdue University. Each approach has its own pros and cons that will

be presented and discussed later, so it will be up to each network administrator to decide which one is more suitable to his network.

After obtaining the ID of the AP to which the device is currently connected to, an application-dependent location-based database that contains mappings of the APs' ID to the physical location (i.e., room) of the APs (and possibly to the physical location of the closest printer or vending machine) will be queried, and the result, i.e., the room, the closest printer or vending machine will be returned to the user or application.

RADIUS Approach

Remote Authentication Dial-In User Service (RADIUS) is used to provide centralized authentication, authorization, and accounting for dial-up, virtual private network, and, more recently, wireless network access [9]. Authentication is the process of identifying and verifying the credentials of a user. Several methods can be used to authenticate a user, but the most common includes a combination of user name and password. Once a user is authenticated, authorization to various network resources and services can be granted. Authorization determines what a user can do, and accounting is the action of recording what a user is doing or has done. RADIUS is a protocol described in IETF RFC 2865. A RADIUS client (in our case a wireless access point) sends (using UDP) a RADIUS message containing the user credentials and connection parameter information to a RADIUS server. The RADIUS server authenticates and authorizes the RADIUS client request, and sends back a RADIUS message response.

Each AP can act as a RADIUS client to provide authentication to a user coming under its coverage by sending a message to the RADIUS server that responds by issuing an ACCEPT or DENY response to the AP. The RADIUS client (i.e., the AP) would then act according to the response it received. RADIUS can also be used as a mean to restrict access to APs with the use of the Extensible Authentication Protocol (EAP) [10]. EAP runs directly over the link layer and therefore does not require the use of IP addresses. The *Authenticator*, which is the end of a link that requires authentication, would request the other end, called the *Supplicant*, to provide identification. Once the supplicant provides the identification credentials, the authenticator ends the authentication phase with either a SUCCESS or a FAILURE response. The authentication mechanism that determines a SUCCESS or a FAILURE response is not specified, and is up to the network administrator's policy.

In ECN current wireless LAN setting, 802.1X [11], which is one of the authentication methods for 802.11b is used. Basically it is EAP over IEEE 802.11b. After a device has been associated with an AP, the AP would act as the EAP Authenticator and places the device in a blocked state. All non authentication-related traffic coming or going to the device is blocked by the AP. The device would act as the EAP supplicant and supply identification, here its MAC address to the authenticator. The authenticator would then contact the authentication server and check if that MAC address is registered, and issue a SUCCESS or FAILURE response depending on the response from the authentication server. If a SUCCESS response is issued, the AP will drop its filter and allow all traffic between the device and the outside world.

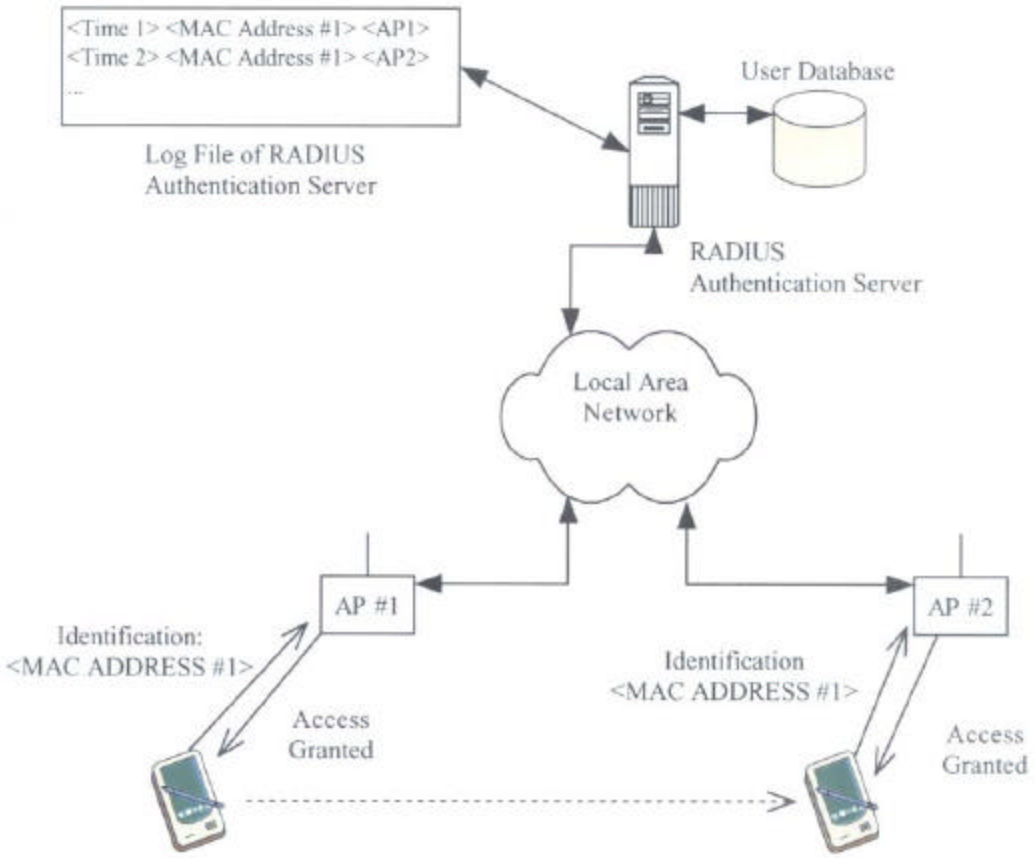

Figure 2. The RADIUS approach

Each time a device tries to associate with a new AP, an authentication process starts in which the MAC address of the device is sent to the RADIUS server by the new AP for authentication. In case the authentication process is successful, the following information is kept in a log file: the time at which the authentication request has been made, the ID of the AP that has made the request, and the MAC address of the device that was authenticated. By inspecting the log file of the authentication server, it is possible to determine to which AP a given device is currently associated with. Using this information, we can determine the approximate location of the device. Figure 2 shows the use of the RADIUS server as a mean to locate a mobile device.

For those wireless LANs that forbid non-registered users to use their services, the RADIUS approach will be a good choice, since there will be a need for authentication before using any AP in any case, and a mobile device can be located simply by monitoring the log file. This approach is also device independent. Regardless of what operating system the mobile device is using or what model it is, as long as the device has an IEEE 802.11 modem card that is registered in the network, this solution will be able to locate it. The response time of the RADIUS approach, i.e., the time it takes for the system to realize that a mobile device is in a new location, is about 3 to 5 seconds in our

implementation. The delay is mainly due to file updates over NFS (Network File System). Currently for prototype testing, we do not want to interfere with existing services, so we have the RADIUS server (currently maintained by ECN network administrators) running on one machine and LODS server (for our prototype testing) running on another machine. The LODS server detects changes in the log file on RADIUS server and updates its copy of the log file accordingly. If both the RADIUS server and the LODS server are put on the same machine, the response time should improve drastically.

The shortcomings of the RADIUS approach include the need of a RADIUS server (or other authentication service with output log), the fact that it may not scale that well with the size of the enterprise network, and the fact that all APs must be able to perform authentication (i.e., to be EAP and RADIUS enabled). It also has the shortcomings linked to a centralized approach

SNMP approach

SNMP (Simple Network Management Protocol) is the standard operations and maintenance protocol for the Internet [12]. It can be used to obtain system parameters from a device, and to configure various parameters on a device. Each parameter is called an attribute, and attributes are organized in groups called communities. Currently most APs are SNMP-able. In the ECN setting, as discussed earlier, they are configured as transparent bridge and hence they all maintain their bridge learn table. The bridge learn table of a given AP contains the mappings of the MAC addresses of the devices, which have recently used that AP, to an interface of that AP. Therefore, if an entry indicates that a particular MAC address is mapped to the wireless interface of a given AP, we can conclude that the device with this MAC address has either been recently connected or is currently connected to that AP. This table is available to the network administrator via SNMP query with authentication as long as the APs are SNMP-enabled (a network administrator can decide to disable SNMP on his APs since SNMP has some security flaws).

In this approach, the LODS server periodically queries all the APs using SNMP to obtain their bridge learn tables and creates its own log file. One of the shortcomings of this approach is that a bridge table does not refresh until a device has been inactive (possibly because it has moved) from the AP standpoint for about 15 to 20 minutes. By maintaining a log file which contains information obtained from the periodic queries, we can find the latest AP that a particular mobile device connected to through a query to that log file. The idea is shown in Figure 3. It is probably worthwhile repeating that this approach will work because we are working on location discovery based on active connectivity as opposed to passive connectivity as discussed earlier.

This approach does not require the setup of a RADIUS server and is generic, thus it is more suitable for open access AP systems like Internet café. In order for this approach to work, the APs have to be SNMP enabled which is not without security risk at the present time. The SNMP approach also is operating system and model independent. The downside of this approach is the heavy signaling generated by the periodic probing of

APs. The response time of this approach can vary. In our current prototype, the response time varies from 10 to 30 seconds for a probing period set to 10 seconds. The duration between two probes also determines how precise the locating scheme is. Obviously the right trade-off has to be found since the probing period impacts the signaling load as well as the response time (i.e., the speed at which a change of AP can be detected by the system). This approach like the previous one will not scale that well with the size of the enterprise network and has the shortcomings linked to a centralized approach.

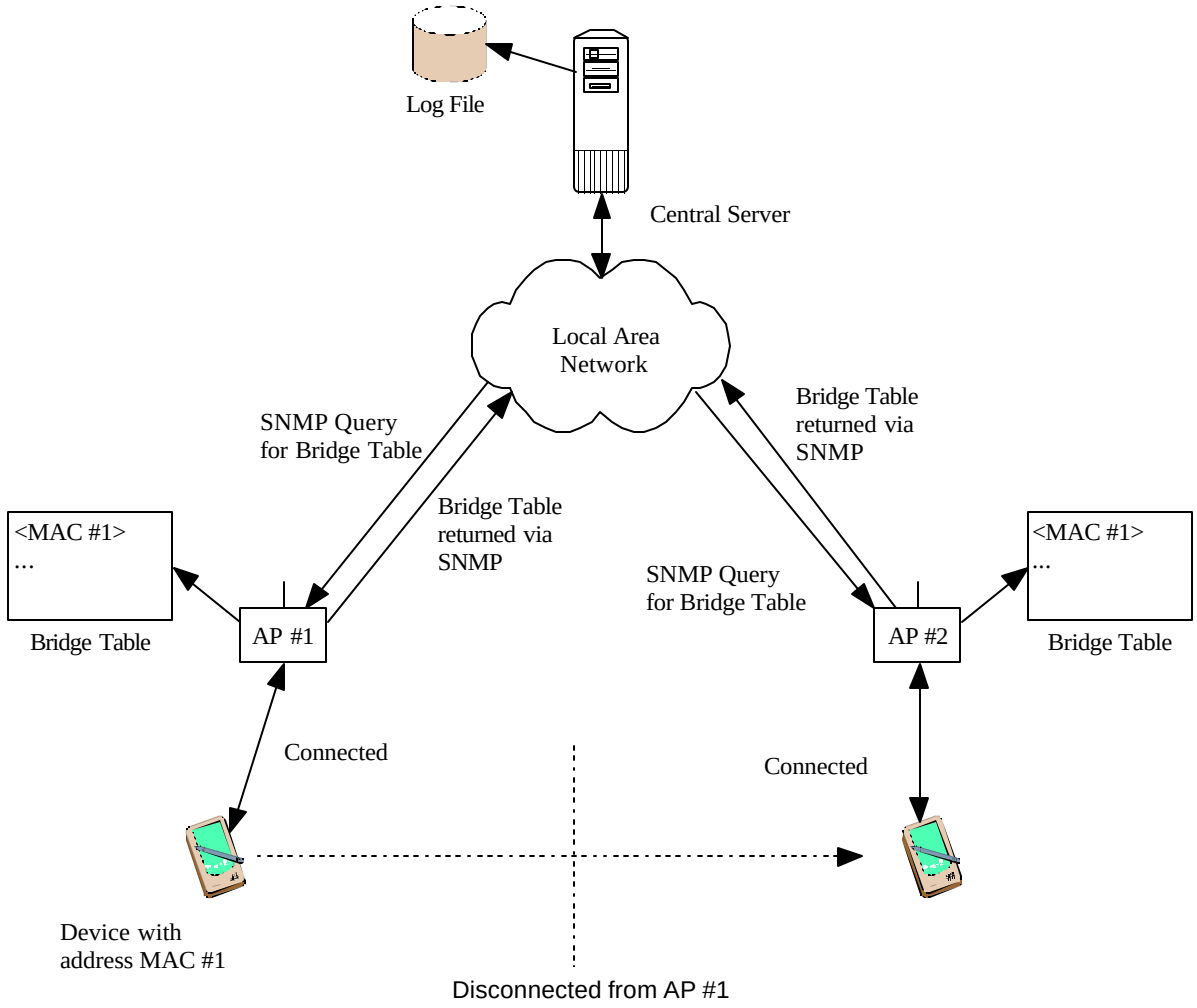

Figure 3. The SNMP approach

Device-driven approach

In 802.11b, a mobile device needs to establish relationship with an AP before using the network. In usual settings, a mobile could be under the coverage of multiple APs, and it will perform a scan to the frequency bands and select the AP with best communication quality. There are two types of scanning: active scan, where the mobile

broadcasts a *probe request* and all candidate APs (those able to receive the probe) reply with a *probe response*; or passive scan, where the mobile determines the communication quality with the potential APs from the beacon it received from each of these APs. These two scenarios are shown in Figure 4. The 802.11b modem will know at all time to which AP it is associated with, so if a LODS application located in the device could retrieve this information from the modem, it could identify the current AP to which is connected.

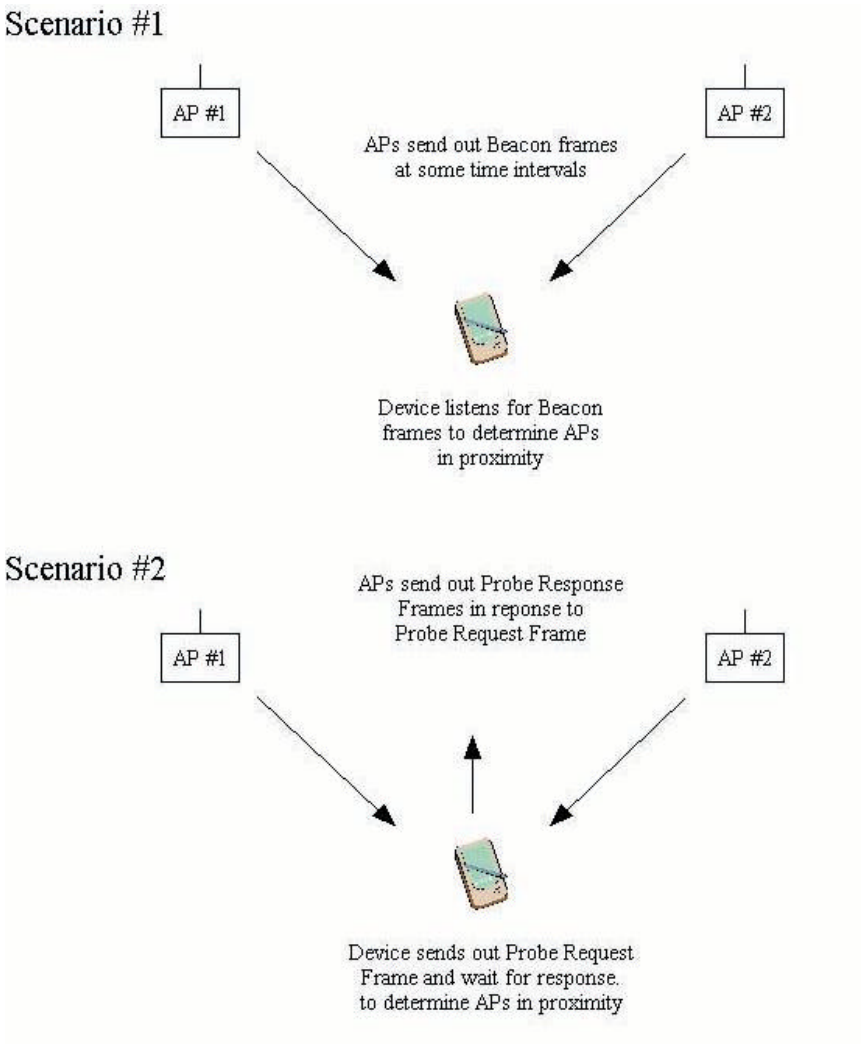

Figure 4. Device-driven approach

This approach requires least involvement from the network. Each mobile device can locate itself just by checking the information about the current AP with the modem, and send the AP's ID to the location database. This has the advantage of making the device responsible to locate itself. However, the software to communicate with the modem in order to get the AP's information will be hardware and operating system dependent.

Which approach to use?

Each of the above approach has its pros and cons, and different applicability. It is up to the network administrators to decide which is best suited for their network. A table comparing the three schemes is shown below:

	RADIUS	SNMP	Device-driven
Network Service(s) required other than the location database	RADIUS or other authentication server with log	SNMP-enabled AP, and a log file to maintain the queries	NO
Additional Signaling Required	NO	Periodic SNMP requests and updates	NO
Software Installation in Mobile Required?	NO	NO	YES
Operating System Independent?	YES	YES	NO
Hardware Model Independent?	YES	YES	NO
Ease of implementation	Easy	Intermediate	Difficult (especially for PDAs)
Response Time	3 to 5 seconds	10 to 30 seconds (depending on probing period and AP response time)	Immediately after associated with AP

Table 1. Comparison between different locating schemes

Based on our implementation and testing (we have not implemented the device-driven approach), the RADIUS approach provides excellent performance. It requires no signaling in addition to the original RADIUS service. The response time is good, and the implementation is easy. The SNMP approach, on the other hand, generated a high amount of signaling traffic, and the responsiveness is not always very satisfactory. For the device-driven approach, complexity in implementation is the main issue and vendor specific support is needed. Most PDAs or PocketPCs uses WinCE as their operating system. Since Windows is not open source and modems from different vendors may need different system calls to obtain the AP information, this makes the implementation of this scheme difficult. The retrieval of AP information can be done relatively easier in Linux.

4. Application of LODS – Remote Printing Service

Remote printing service [2] is a project supported in part by Hewlett Packard, for which we developed a web-based printing service for PDAs, so that they can print virtually any document that can be accessed through a Web browser (i.e., HTML, PS, PDF, and virtually all types of images) using any printer connected to the network without downloading the document into the PDA. The advantages of this service are that

there is no need to install any printer driver in the PDA; that files for which there is no viewer installed in the PDA can still be printed from a PDA; and more importantly, PDAs do not need to download, say, a huge postscript file, before printing it. This reduces the consumption of power and memory at the PDA and is bandwidth friendly for the wireless LAN. However, when choosing the printer to use, a user may not know where the closest printer is if he is out of his office (maybe in another building), which means that without a location-based printing service, the user may have to get his printed document unnecessarily from a distant printer, even when a closer one was available. With LODS, the remote printing service can know approximately where the user is, and suggest printers that are closer to the user. This is illustrated in Figure 5.

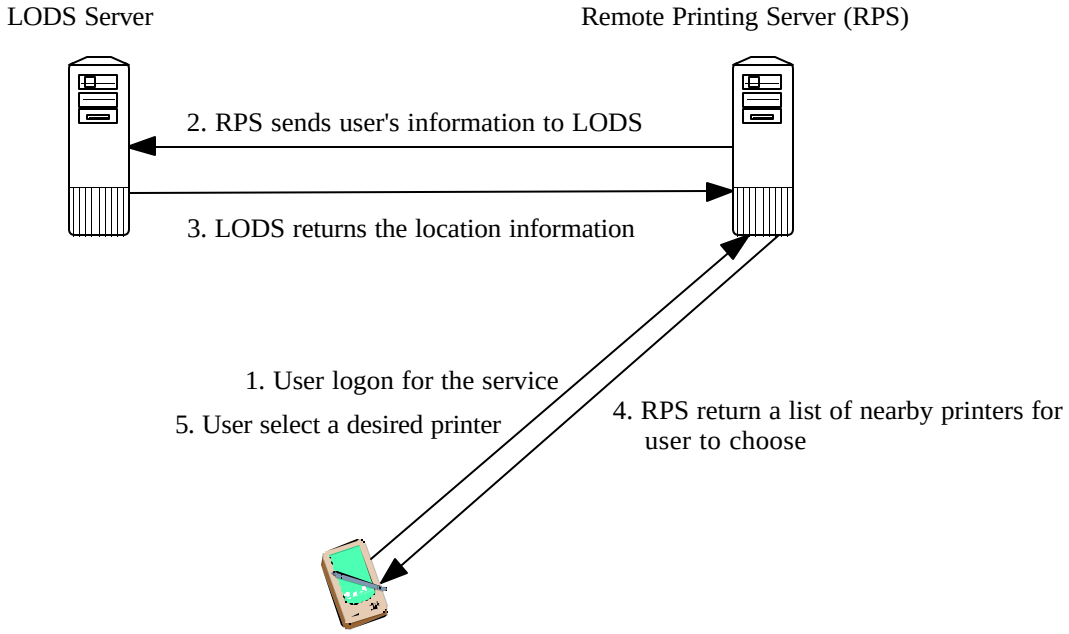

Figure 5 Flow of Remote Printing Service using LODS

The operation of our Remote Printing Service with LODS consists of four steps:

- Authentication,
- User tracking,
- Location database lookup,
- Return of information.

Since tracking a user without his knowledge could be seen as a breach of privacy, we required all users to register for LODS before they can use our remote printing service. By registering, a user agreed to be "tracked". Moreover, this registration process provides better authentication on the use of the service. A mobile device can only use LODS with its own, registered MAC address, which means it is not possible to locate somebody else. The authentication is done every time LODS is called, whether directly by users or through location-based applications. For users running Netscape or Internet

Explorer, it is possible to save the username and password in the device so that from the users' point-of-view, authentication is just done once to make the process less annoying. In ECN, a user would register his ECN login name and the MAC address of his 802.11b modem.

After the user has logon, when called by the user (directly or indirectly through an application such as the Remote Printing Service) LODS will, base on the username, know the MAC address of the device. It will then use the RADIUS or SNMP approach to determine which AP the device is currently using, and pass the result to the Location Database. If the device-driven approach is used, the software residing in the device will pass the AP ID directly to the Location Database. Once the Location Database receives the AP ID, a query will be performed and result will be returned to the entity that called the service (in this case, the remote printing service).

Our remote printing service maintains a Location Database containing the AP to printer mappings. This could be a single centralized server and database to provide services to the whole community, or the campus can be divided into regions, and each region has its own LODS server and corresponding localized database. With this clustering deployment, scalability then is not an issue. Our remote printing service will use the ID of the AP obtained from LODS to identify the closest printer(s), and return the information to the user.

5. Future Work and Conclusion

In conclusion, this paper described a new Web service for location discovery implemented in Purdue University, which locates a mobile user based on the AP it is connected to. The service can be used directly by a mobile user or through other applications via API calls. Different user locating schemes have been presented. With LODS, it is possible to provide enterprise-based wireless location services.

We have implemented a primitive LODS server prototype. One possible direction for future development will be developing a more scalable user locating approach. Ongoing work includes building generic APIs to allow other location-based applications to use the service. Another project named myPurdue, which is an e-community project aimed at providing a set of sophisticated services to the Purdue community, will make use of LODS to provide various location-based services.

Acknowledgement

The authors would like to thank Mr. Bill Simmons of Engineering Computer Network (ECN) at Purdue University for his help in deploying LODS in ECN and Hewlett-Packard for their support through the mobile laboratory grant.

References

[1] http://www.mobilestar.com/news_pressreleases_starbux.asp
[2] http://shay.ecn.purdue.edu/~wlessnet/project.html
[3] http://www.xml.com/pub/a/2002/02/06/webservices.html

[4] A. Valk, "Cellular IP: A New Approach to Internet Host Mobility", *ACM SIGCOMM Comp. Commun. Rev.*, vol. 29, no. 1, Jan. 1999, pp. 50-65.
[5] C. Perkins, "IP Mobility Support", RFC 2002, Oct, 1996.
[6] J. Z. Wang, "A fully distributed location registration strategy for universal personal communication systems", *Selected Areas in Communications, IEEE Journal* on , vol 11 Issue: 6 , Aug. 1993, pp. 850 –860.
[7] J. Sun, H.C. Lee, "Optimal mobile location tracking by multilayered model strategy", *the 3rd Int'l Conf. on Engineering of Complex Computer Systems*, pp. 86-95, 1997.
[8] http://www.go2online.com
[9] C. Rigney *et. al.*, Remote Authentication Dial In User Service, RFC 2138, Apr 1997
[10] L. Blunk *et. al.*, Extensible Authentiation Protocol, Internet Draft, Apr 2002
[11] IEEE Std 802.1X-2001: Port-Based Network Access Control
[12] J. Case et al, A Simple Network Management Protocol, RFC 1157, May 1990
[13] IEEE Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
[14] R. Shankaran, "A Distributed Location Management Scheme for Mobile Hosts", *Proceedings of ICPADS*, 2001
[15] R. Ramjee, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-area Wireless Networks," *Proceedings. IEEE Int'l. Conference Network Protocols*, 1999.
[16] A. Bar-Noy and I. Kessler, "Tracking Users in Wireless Communications Networks", In Proceedings of *IEEE Infocom Conference on Computer Communications*, 1993, pp. 1232-1239