An User and Location Management System for Wireless Networks

Andrei Oliveira da Silva[1], Daniel Waldman[1], Paulo Henrique de Souza Schneider[1], Fabricio D'Avila Cabral[1], Ana Cristina Benso da Silva[2], and João Batista de Oliveira[2]

[1] CPSE - Research Center on Embedded Software †
Av. Ipiranga, 6681 - Building 30 - Block 4 - Room 242,
90619-900 Porto Alegre, Brazil

Abstract. This work presents a wireless user low-grain position management system (up to 5 meters) for Wi-Fi networks. The location system is based on access point identification, where the user's device is associated, through the events generated by the access point. In this context, the access point is a station managed with SNMP. Hence, the system receives information from other SNMP agents that interact with the wireless user authentication system to provide information about users, at what time the client uses to get in the network, among others. These information will be to refine the management system for users and resources.

1 INTRODUCTION

Wireless networks have been used in different enterprises and projects to provide Internet access and ubiquitous computing environments [8]. Examples of such projects are Carnegie Mellon University's AURA project [8], Massachusetts Institute of Tecnology's Oxygen [7], Hewlett-Packard's Cooltown [3] and IBM's ContextSphere [1].

The management of pervasive computing environments is an important task because of its dynamic nature. In this context, users handle mobile devices and services must be offered in a plug-and-play fashion. In these environments the monitoring and management of users and resources are vital for the network use and its security. The monitoring of user behavior offers many possibilities at system control and service personalization levels, which are provided by the environment. An example of such scenario is the knowledge of the user's movement through the network, where it is possible to predict his future location based on this information. This kind of data can be used in many scenarios, from security to CRM (Costumer Relationship Management) applications.

This work presents a user management system for Wi-Fi networks operating in infrastructure mode. The system uses an authentication system and SNMP (Simple Network Management Protocol), respectively validating users in the network and gathering

† Supported by the Hewlett-Packard Brazil/ PUCRS (Pontifícia Universidade Católica do Rio Grande do Sul).

‡ The authors are with CPSE (Centro de Pesquisa em Software Embarcado).

§ The authors are with Faculdade de Informática, PUCRS.

Oliveira da Silva A., Waldman D., Henrique de Souza Schneider P., D'Avila Cabral F., Cristina Benso da Silva A. and Batista de Oliveira J. (2004).
An User and Location Management System for Wireless Networks.
In *Proceedings of the 1st International Workshop on Ubiquitous Computing*, pages 160-169
DOI: 10.5220/0002666301600169

information about them, where its goal is to discover the user location using the identification of the access point which user's device is associated. Through this system, it is possible to discover the estimated position of a user, based in the access point coverage area, which can be a range of 5 or 10 meter depending on the device model.

This paper is organized using the following structure: Section 2 shows the related works; Section 3 shows the authentication system [11] that were used and extended to support SNMP operations; Section 4 describes the location management system, the developed MIB and SNMP agents; Section 5 shows a study case and the Section 6 presents the conclusions and future works.

2 RELATED WORKS

According to [8] location management and context awareness are challenges for the mobility area. Amongst the related projects there is Cricket, part of MIT's Oxygen project [7]. This project uses devices, called beacons, that combine radio frequency and ultra-sound signals to determine the location of devices and applications. Cricket is focused on the user's physical location and provides a reasonable precision inside environments. Beacons can estimate the user's position based on its signal strength, identifying user's position and movement.

Another related project is Cooltown [3], based in an web services architecture and service location protocols, such as UPnP (Universal Plug'n'Play), which allows the user to remotely access a service through an URL. This project also uses beacons, but they are not used to determine the device's location. These devices are used to divulge a service URL. It is also a possibility the use of GPS (Global Positioning System) as a mean to provide the precise user location in open areas. Kindberg [3] also presents a rather different perspective from Cricket. Cooltown project describes the use of web services to provide applications in wide environments, such as a city. This work's described system is being initially developed for restricted environments, such as a museum or a smart room.

The work presented in this paper focus on extracting user's logical position, identifying which access point the user is connected and extracting information about his movement in the system. A log is maintained when the user enters and exit from the network, how much time he spent online, among other information. Through this information, it is possible to determine the user's physical location, based on the access point's position. The described system is being initially developed for restricted environments, such as a museum or a smart room.

2.1 Motivation

Location sensitivity is an important feature in an ubiquitous environment. A set of services can be created and deployed within this context, such as real time marketing and load balance systems. This feature can be explored by two different approaches: physically, which is aided through special hardware devices, and logically, which uses access point where the device is connected to estimate his position.

Physical positioning is more precise, compared to the logical approach, since it can predict the user location with few meters, or even centimeters, of error rate. A disadvantage of this method is that it is necessary to build specific hardware and protocols to manage the positioning, such as on GPS systems.

Logical position management deals with a broader range of user location, usually predicting its position in a range of 10 meters from the access point. A few methods can be applied for the access point triangulation, where the signal strength between the device and the nearby access points are measured and mapped in a database.

Another approach using access points is the use of SNMP information provided by these devices. The location prediction might not be as precise as the previous methods, since it is based in a database mapped information and positioning relative to the access point. On the other hand, it is not necessary to build specific hardware and it also allows to use public standards, such as SNMP messages. Thus, the logical position management can be more feasible, considering development and scalability. It is cheaper to develop software, since devices do not need to have a new hardware attached, making this system more extensible.

3 AUTHENTICATION SYSTEM

Whole system was built over an authentication system [11], and some components had to be adapted and others created to support the user and location management. This system protects services from unauthenticated users, in a similar fashion to NoCat [5]. All events are transmitted through SNMP messages and a few agents and managers were built to manage users in the network and to gather information about their behavior. The authentication system's components are presented in Figure 1:

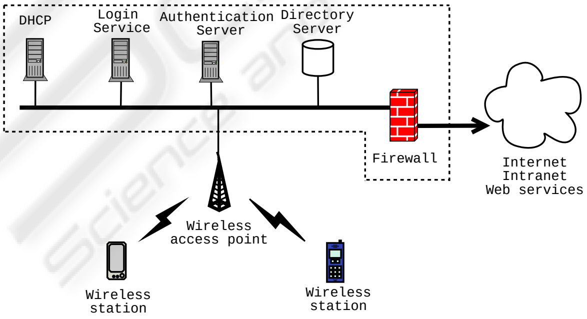

Fig. 1. Authentication system

Web services [3] were used to implement the user access control mechanism. It is important to notice that the network project must predict the access to the wireless network through a firewall in order to prevent the improper network use.

3.1 Components

In order to achieve such authentication system, a range of servers and services are needed. The components shown on Figure 1 are described below:

DHCP provides dynamic IP address allocations to wireless devices that are entering the network;

Login Service provides the authentication web page interface, where the users are redirected to be authenticated;

Authentication Server takes place of most of the management tasks. It is responsible for receiving authentication requests from the Login Service, querying the Directory Server for user profile and password, configuring the firewall to allow and deny the user access to the network and services;

Directory Server used to store user information, more specifically username, password and profile, which contains the service names that the user can access;

Firewall control which services the user can make use and which ones are not available for a given user.

3.2 Events

This authentication system presents a few events that are related to the network safety and, afterwards, the information gathering process. This subsection will briefly explore the events related to the authentication process, when the user enters the network.

1. **Entering the network:** the user enters in the range of the wireless network access point range and an IP address is set to the device, through the DHCP server;
2. **Login Server redirection:** after having a valid IP address, the user is automatically redirected for a server to be authenticated and make use of the services;
3. **Authenticate:** in the authentication server, the user logs through a web service (events 1,2,3 and 6 of Figure 2), which will sets the firewall user's rules (event 5) of his profile (event 4).

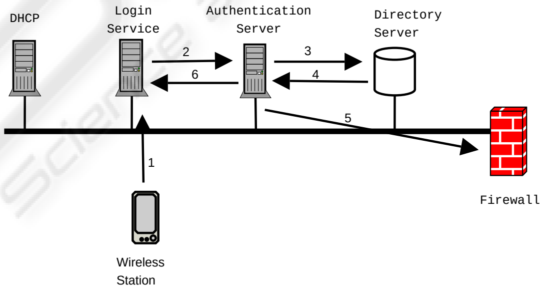

Fig. 2. User authentication

The device disassociation and user deauthentication will be better explained in an upcoming section, dealing with this system integration with the management features.

4 USER MANAGEMENT AND LOCATION SENSITIVITY

The previously described system proposed a mechanism to allow only authorized users to access the network and make use of its services. However, it's possible to aggregate other functionalities and information to this architecture within the authentication process.

Therefore, the management system presented in this work is based on user access control and user location sensitivity. Its main goals are to:

- Identify user permissions;
- Apply restriction policies;
- Service allocation policies (e.g. services which are physically closer to the user);
- Provide environment personalization;
- Allow resource allocation management.

The management of the user access control is based on the previously presented authentication system. In order to accomplish its goals, SNMP agents [6] and proprietary mechanisms were employed for the information gathering process in entities and processes related to the authentication procedure.

The location sensitivity management is accomplished through the periodic monitoring of the user movement in a Wi-Fi network, configured in infrastructure mode. Access points who have embedded SNMP agents and send association/desassociation SNMP traps can be used to monitor device's behavior. Therefore, if a device is associated with an access point it is certain that he is in the access point's range, which is usually 10 meters. This information can be used to identify the user's estimated position, related to the physical location of the access point.

Besides the management systems described above, the system generated events are stored in a MIB, where they can be easily accessed and updated through SNMP requests (get or set). This section will explore the implementation of a user management system based on the access point coverage range, as well as present the base of gathered information and the steps taken to integrate this management with the previous authentication system.

4.1 User's MIB

The authentication system provides a collection of user information, such as username, device's IP and MAC address, access point which the user is associated, for example. Combining these features with traps sent by the access point's embedded SNMP agents, it is possible to capture the time when the user enters and leaves the network and series of information that can help in determining the user profile, such as places where he usually goes, how long does he stay in a given place and so on. These information are described in a MIB whose attributes are updated whenever a system event occurs. Table 1 presents how this base was modelled.

In order to implement a MIB for user management a Net-SNMP agent [4] was used, which make it possible to create and support a new repository path. This modified agent handles MIB requests, updating and recovering information provided by the authentication system.

Index	Information	Use	Provided by
1	Device's MAC address	Identify the device being used in the network	Association traps to the access point
2	Device's IP address	Identify the IP address associated with the device, and can be used to detect network intrusions	DHCP
3	Username	The user making use of the network	Authentication server
4	Access point's IP address	Determine in which access point the device is associated, making possible to estimate the device location	Association traps to the access point
5	Deauthentication mode	Determine how a user was deauthenticated.	DHCP or disassociation traps for the access point
6	Device's entry time	Indicate when the device entered the network	Association traps to the access point
7	Device's exit time	Indicate when a device left the network	DHCP or disassociation traps for the access point

Table 1. User's Management MIB

4.2 Authentication system integration

The extension of a Net-SNMP agent can be done through scripts referenced by the configuration files. Therefore, in order to integrate the authentication system with the user management, a SNMP agent was devised to receive system information.

The access point was configured to send association/desassociation traps to the authentication server, which will update these information to the SNMP agent. This behavior is executed every time a new event occurs.

Some original authentication system components had to be modified for the integration of the location sensitivity management, and a few had to be created. The following items enumerate the required modification:

- Modify the authentication server in order for it to act as an agent (receiving information from other agents/managers, such as traps from access points) and to update the MIB, as shown in Table 1;
- Event handling by the authentication server, such as dealing with association/disassociation traps;
- Creation of a SNMP agent, with an implemented MIB 1, which stores events in a database 2.

In the following sections, the events generated by the system integration will be studied, exploring its purposes and motivations.

Device association When a device is associated in the access point, the access point's embedded SNMP agent will send a trap message, indicating this association to the authentication server, as can be seen in Figure 3. This event is sent to the agent, which combines this information in a database containing the previously stored events.

The events and messages generated by this association are the following, in chronological order:

1. When entering the access point range a trap message is sent to the authentication server, containing the device's MAC and IP addresses and access point's IP address which is associated with this device;
2. It is verified if a user is transiting between networks or if he is reassociating in the same network, depending on disassociation events. In both cases, the transition time between networks is calculated. If this time is higher then the defined timeout, the user must reauthenticate itself as it is the first time it gets in the network;
3. If it's a new user, DHCP must return a valid IP address, binding it to the device's MAC address, and must authenticate itself in the network;

Device disassociation When the access point's SNMP agent detects a device which left his access range, as seen in Figure 3, it generates a SNMP trap indicating the disassociation of this device. The trap message will carry information such as MAC and IP address of the device. When the SNMP agent receives this message, it will update the database with this event. When the device returns to the network the timeout between events is calculated, thus blocking the firewall for the device or not. This block is based on the device's MAC address, in order to avoid unwanted accesses by other devices who might try to use the same IP address.

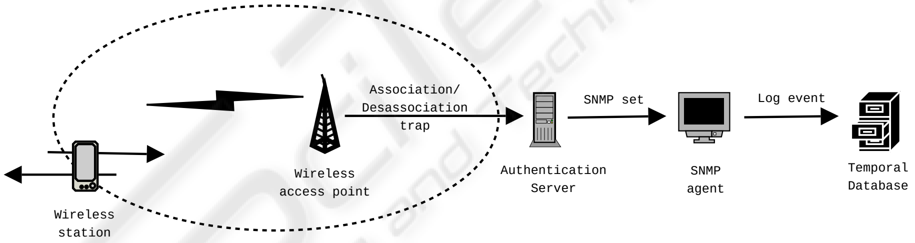

Fig. 3. Device (des)association

Device turned off The action of turning off a device does not represent an disassociation for the access point's SNMP agent. In order to avoid a scenario where another user makes use of the same device, thus inheriting the access privileges of the previous user, the firewall rules must be configured based on the device's MAC address. Therefore, when a device, which was turned off, retries to associate in the network, all its rules will be blocked by the firewall. The same case happens when tries to enter the network with a fake IP address, since the firewall rules are configured based on the MAC address, forcing the authentication process.

Data storage A desirable feature in managements system is the user and network statistics processing. To make it easier in identifying the user behavior, an event registry was built based on the agent's integration with a database. The updated information is recovered in the user management MIB through database queries sent by the SNMP agent. This process is done using scripts that handle communication with the MIB, and store the information on a temporal database [10].

Device's MAC address	Device's IP address	Username	Access Point IP address	Deauthentication mode	Entry time	Exit time
MAC1	IPDEV1	Claudia	IPAP1	DHCP	15:30	15:35
MAC1	IPDEV2	Eugenio	IPAP1	TRAP	15:35	15:37
MAC1	IPDEV2	Eugenio	IPAP2	TRAP	15:37	NULL

Table 2. Temporal database example

The database registers the event occurrences, such as an user authentication and the start and end time for this event. Table 2 exemplifies this scenario. In the first entry, Claudia is deauthenticated through the DHCP lease. Afterward, Eugenio, using the same device, associates itself in an access point $IPAP1$ and, minutes later, changes it to access point $IPAP2$.

This process is executed for all information contained in the MIB, where new updates are recovered every time a request is made.

5 CASE STUDY

A simple model that exemplify the use of the presented system is a university campus or an office building, where the scenario focuses on an user who wants to print a document in the nearest color printer. When this user access the network, his device will be associated with an access point and will be authenticated through the authentication server.

The access points and printers have their physical position and descriptions mapped in a database. Matching the user's position with the printer's description and location it is possible to send a printer job to the nearest printer through a web service [9].

Moreover, the events generated by the system can determine which places are being frequently visited by a given user, thus allowing resource allocation based on his movement patterns. It is possible to imagine the implementation of this system in a mall or super market, where the clients can receive announcements through their PDA based on the their most visited places or favorite products.

When the user access the network, his device is associated with one access point that sends a trap to the authentication server indicating the MAC address of the user's device. This event updates the user management MIB with the MAC address of the user's device and the access point's IP address. Thus, the user goes to the authentication step, where the authentication server updates the MIB with the device's user name and IP address.

A disassociation trap indicates that the user has left the access point's range. It indicates that the user is moving, thus when the device reassociates with another access point a new trap is sent to the authentication server, which updates the MIB. All these events are stored in a temporal database and they can be analyzed in the search for movement patterns in order to place services for the user.

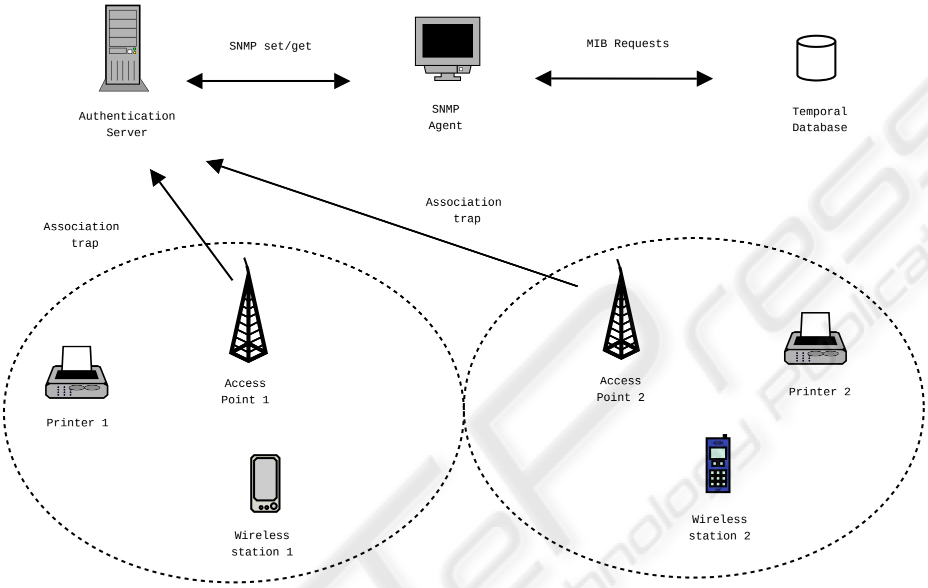

Fig. 4. Case study

Figure 4 presents the events in an environment with two access points. The system would redirect the printer job of *Station 1* to the nearest printer, based in the location information mapped in the database. If the station enters the range of the *Access Point 2*, a trap will be generated to the authentication server indicating that *Station 1* has left *Access Point 1* and its printer jobs must be sent to *Printer 2*, since it is closer to *(*Access Point 2).

Trough the analysis of the temporal database events, it is possible to determine the behavior of each user on every week's day, thus offering discounts in printer jobs and placing more services inside the most used network printers.

6 FINAL CONSIDERATIONS

The system presented in this work allows the management of the user's access control, the network access and its resources and services, as well as being able to identify the approximate position of users and devices in a wireless environment. The integration of these proposals will allow, in the future, the creation of an integrated user management environment, based on locations, in order to personalize and manage the use of services in a ubiquitous environments.

The collected information can be used to create models that allow the prediction of environment needs, as well as to model user profiles. But it depends on the specification of the access point, if it supports association/desassociation traps, what can be an disadvantage of the proposed system.

This work must still be validated in a real environment, with more users accessing the network and its services. Based on these results, it will be possible to better validate the system. However, it's necessary, foremost, to aggregate security into the authentication system, through the use of SNMPv3.

The future work is focused in integrating this system with sensor devices (such as beacons) in order to obtain a precise information about the user and device location, thus allowing to upgrade the management process.

References

1. Bisdikian, C., Christensen, J., Ebling, M. R., Hunt, G., Jerome, W., Lei, H., Maes, S., Sow, D.: Enabling location-based applications. First international workshop on Mobile commerce, Rome, Italy (2001)
2. Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J.: Ieee 802.1x remote authentication dial in user service (radius). RFC 3580. (2003)
3. Kindberg, T., Barton, J., Morgan, J., Becker, G., Caswell, D., Debaty, P., Gopal, G., Frid, M., Krishnan, V., Morris, H., Schettino, J., Serra, B., Spasojevic, M.: People, places, things: Web presence for the real world. Mobile Networks and Applications, 7. (2002)
4. NET-SNMP: The NET-SNMP home project. http://www.netsnmp.com (2003)
5. NoCatNet: NoCat. http://www.nocat.net (2003)
6. Perkins, D., McGinnis, E: Understanding SNMP MIBs. 1st edition. Prentice-Hall, Upper Saddle River, New Jersey (1997)
7. Priyantha, N. B., Chakraborty, A., Balakrishnan, H.: The cricket location-support system. Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), Boston, United States. (2000)
8. Satyanarayanan, M. (ed.): Pervasive computing: Vision and challenges.. IEEE Personal Communications, August. (2001)
9. Silva, A. O., Meneguzzi, F. R., Schneider, P. H. S., Barcelos, R. B., Rodrigues, V. O., Waldman, D., Silva, A. C. B.): Providing printing web services. Fifth IEEE InternationalWorkshop on Networked Appliances, Liverpool, England. (2002)
10. Simonetto, E. O., Ruiz, D. D. A: Temptool: A tool for temporal data modelling in: Advances in databases and information systems. 5th East-European Conference ADBIS'2001 Professional Communications, Vilnius, Lituania (2001)
11. Waldman, D., Silva, A. O., and Silva, A. C. B.: An extensible authentication architecture for wireless networks. VIII Simpósio de Informática, Uruguaiana, Brazil (1995)