Proximity Based Access Control in Smart-Emergency Departments

Abstract— **An automated access control model for smart hospital emergency departments (ED) is possible through decisions based upon the proximity of users to resources. The notion of proximity of a resource is dependent upon many factors, including: the three-dimensional accuracy of the positioning system employed, geometry of the physical workspace, the electromagnetic environment and access control policies for the resource.**

In this paper, we propose a proximity based automated access control (PBAC) model for smart-ED environments. The goal is to develop a context-aware and trustworthy smart-ED that improves the existing ED work-flow by automating certain mundane activities (accessing patient record without a password) allowing caregivers to focus on the treatment of patients. The level of access provided to the users (caregivers) is dependent upon their roles within the hospital and the system context. To prevent any unauthorized access, we have suggested three levels of authentication: Unauthenticated, Authentication Level I and Authentication Level II. This authentication schema complements the access control model while facilitating appropriate level of access privileges to users. Further, the access control model is dynamic and adapts itself to unpredictable events that require urgent action.

We also present a semi-formal specification for the proposed access control model in terms of policies for different usage scenarios. We further validate our specifications by developing a prototype for the PBAC model. The prototype was built on top a Ultra Wide Band (UWB) based positioning system whose accuracy was tested in a real ED environment.

I. Introduction

Hospital emergency departments (ED) must provide effective and timely treatment to all patients, many times in an unpredictable environment. Mundane activities such as data entry and retrieval often impact ED efficiency by distracting caregivers who must interface with multiple secured hospital information systems to accomplish these tasks. Automating certain tasks, such as authentication login, will reduce these distractions and allow caregivers to concentrate on treating patients [20]. For example, in a smart-ED, caregivers needing access to a patients medical history can be automatically logged-in, without typing a user name or password, by virtue of their proximity to a computer. As a result, they can continue patient care and review clinical data without being distracted by mundane administrative procedures. However, automating access control to information resources in the smart-ED poses certain security issues. As various people need access to the information system or a particular resource, the automated access control system must be able to distinguish between different users in close proximity, determine their privileges and provide appropriate access.

In this paper, we introduce a mechanism for providing automated access to resources in a smart-ED environment via a Proximity-Based Access Control (PBAC) scheme. This scheme makes access control decisions based on the proximity of the user to a particular resource such that when the user enters an established zone around the resource, access is automatically granted. In order to be effective, privileges to access a resource must be highly granular in nature - similar to user accounts in an operating system. We address this issue by using a form of Role-Based Access Control (RBAC) [3], whereby users are assigned different roles, and based on these roles, are granted predefined access privileges to the resources. Therefore, when a user comes into the defined proximity zone of a resource, access privileges are granted based on their role within the system.

Proximity-based access has certain pitfalls in that it could potentially allow someone (even an unauthorized person) access, when an authorized user is in proximity but not currently using the resource. A malicious user could exploit this situation by accessing the resource with the other authorized user's privileges. To prevent this, the system must include authentication mechanisms to prevent users from accessing resources for which they are not actually entitled. For example, a nurse standing by computer should not be able to gain access to a doctor's log-in when the doctor is merely in proximity of the resource.

Authentication mechanisms should not be static and may need to change during unusual circumstances. Under *normal* circumstances, resource access privileges are derived from the role of the user needing access. How-

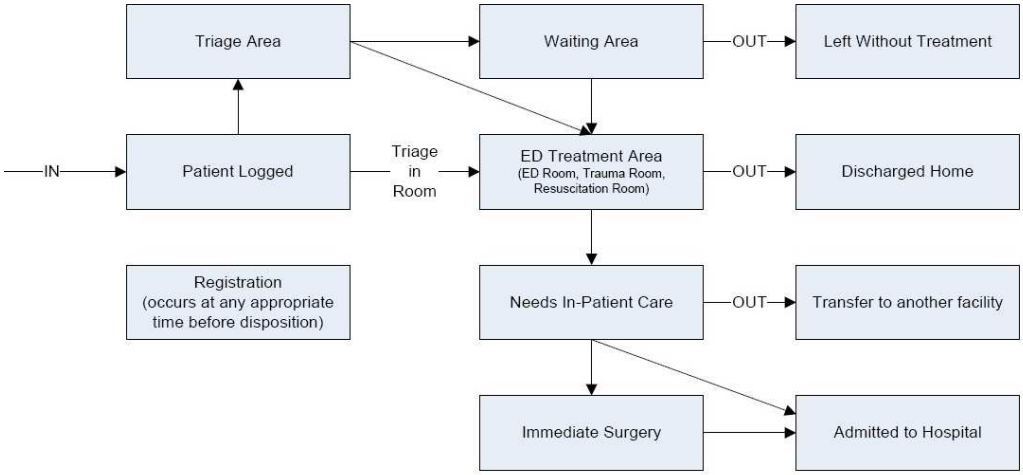

Fig. 1. ED Workflow

ever, during *abnormal* circumstances requiring urgent action, the process must allow for flexibility. Examples of abnormal circumstances might be the unavailability of caregivers assigned to a patient or an influx of a large number of patients in the ED as a result of a disaster. Routine access privileges (those used under normal circumstances) may not meet the requirements for such situations and may even impede the ability to appropriately manage them. For example if the assigned caregivers for a patient are not available during an emergency, then the routine access privileges would not allow access to any qualified caregiver in the vicinity of the patient.

Though unusual in the ED setting, this scenario shows that with the traditional authentication mechanisms it may not be possible to override security requirements during an abnormal or even disaster situation. In the rest of the paper, we refer to such situations as critical events and the state itself as criticality. The *goal* of this paper is to present a Proximity-Based Access Control (PBAC) model for smart-ED environments to provide automated access, to resources, at appropriate security levels (for medical professionals) in both critical and non-critical situations.

To implement the PBAC model we first defined the notion of *proximity* of a resource by designing a specific area, called *proximity zone*, around the resource. The shape and size of the proximity zone is designed based on the following parameters: the three-dimensional accuracy of the positioning system employed, geometry of the physical workspace in the ED, the electromagnetic environment and the access control requirements for the designated resource.

Once we have a concrete definition of proximity we can provide access to resources when a user comes in this area. However the level of access provided is not the same for all users and to prevent inadvertent or malicious access to resources, as a result of PBAC, we developed three authentication levels: Un-authenticated (access privileges only to publicly available resources), Authentication Level I (common access privileges to a group of users, i.e. nurses, physicians, etc.), Authentication Level II (access to private user information or secure clinical information). This authentication schema complements the access control model while facilitating appropriate level of access privileges to end users. We further extend the aforementioned access control model to include criticality handling capabilities. During critical situations, this model adapts itself to provide a new set of access privileges to users in order to manage the critical event.

A. Contribution

Our main contribution in this paper is to design, specify and validate a proximity based access control model for ED environments. The proposed PBAC model *enhances the work-flow* in the ED by providing automated access control to the resources. Further, by incorporating different levels of authentication, the model *prevents the security pitfalls* normally associated with proximity based access control mechanisms. The proposed model also *facilitates the handling of the critical events* by

appropriately adjusting itself.

To concertize the model we *provide a detailed semi-formal specification* of the PBAC model with comprehensive policies for handling both administrative and access control tasks within the system. The policies are adaptive enough to be applied in both normal and critical system states. To validate the policies we *developed a prototype* with an Ultra Wide Band (UWB) based positioning system. We further field-tested this positioning system in a functioning Level-One Trauma Center ED in the Phoenix metropolitan area to determine its accuracy which facilitated the *determination of the shape and size of the proximity zone*.

B. Organization of the paper

Our paper is organized as follows, Section II presents the motivation for this work, followed by Section III which presents the concept of Proximity Based Access Control and its design issues. Section IV provides details of the access control model by present roles and their management issues. Section V presents the access control policies applicable for a PBAC based system. In Section VI we present a detailed discussion on the practical issues related to this work, followed by the related work and conclusion in Section VII and Section VIII respectively.

II. Motivation

In this section we present the need for automated authentication access to resources in an ED, describe ED work-flow, and demonstrate how PBAC can improve efficiency.

Patients follow certain well-defined service paths (Figure 1) in the ED, but the actual path often depends on their presenting condition. Patients may arrive by public or private vehicles, on foot, or by ambulance. Once identified as requesting emergency evaluation, patients are logged-in, triaged by a nurse (either in a triage area or in a treatment room) and registered at an appropriate time. The triage process determines the priority of when and what type of services a particular patient will need. Based on the triage assessment, patients may be sent to a waiting area or directly to a treatment room. Critical patients, who most often arrive by ambulance and require immediate medical attention, usually bypass triage and are taken directly to a treatment room or specialized area such as a trauma or resuscitation room. The process of tracking patients from the moment of arrival; to triage; to the waiting or treatment area; to the time they are seen by the physician and nurse; to various ancillary departments (such as radiology); and through hospital admission or discharge has traditionally been a cumbersome, incomplete and inaccurate manual process. Automated tracking of patients and staff throughout this process holds much promise [20].

Physicians, nurses, and other caregivers often require access to several data systems, each requiring a unique log-in process. Aside from remembering several passwords, these log-in processes distract staff from their natural work-flow. Session loading and unloading may also detract from patient care. An access control system that automatically logs-in a pre-authenticated user to a resource, based on the proximity of the user to that resource, will reduce distraction, improve efficiency and improve patient care.

Further, caregivers tend to leave computer resources open without closing their session after each use. Although typically the system automatically closes the session after a preset inactivity interval, patient information is vulnerable to inappropriate access during this time. Using PBAC can eliminate this vulnerability by automatically closing or suspending a session immediately after a user has left the vicinity of the resource.

The ED is a collaborative working environment where the caregivers cooperate on many different levels; therefore access control policies need to be adapted to these special requirements. For example, a resource being actively used by a nurse should not automatically be relinquished to a doctor (even though the doctor might have a higher priority access). Instead, typical work-flow would dictate that the nurse be notified on-line of the potential need of the resource by the doctor. Off-line communication could then determine appropriate release of that resource. This process eliminates the possibility of frequent spurious session interruptions in a busy area where user sessions could be pre-empted because of inadvertent movements of other users.

III. Proximity Based Access Control

Proximity Based Access Control (PBAC) is a technique for providing automated access to resources based on the proximity of a user to that resource. Proximity can be defined as a zone around the resource, within which, a user must be located in order to gain access. There are three main aspects of PBAC necessary to determine the accuracy of the access control automation process:

1) The design of the zones which define the proximity of resources.
2) The three-dimensional accuracy of positioning system employed to verify when a user is in the

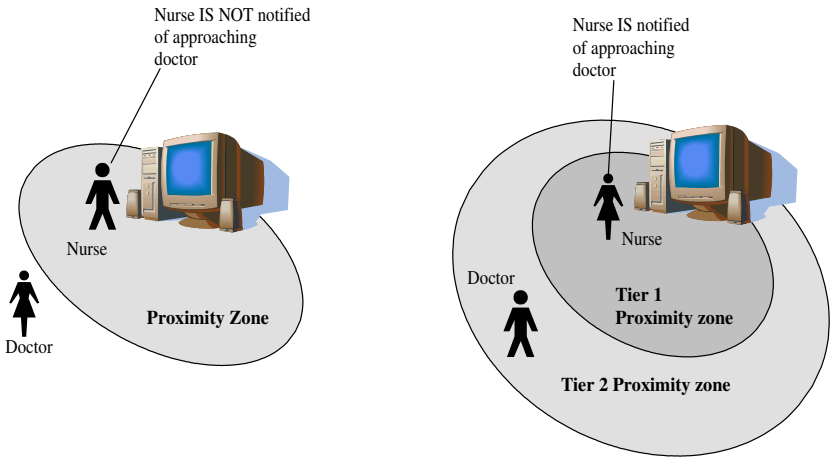

Fig. 2. Single and two- tiered Proximity Zone

proximity zone.

3) The security privilege level of access provided to users within proximity of a resource.

The first two aspects ensure that a user only gains access to a resource when in the correct position respective to that resource, while the last enforces information security and priority of use.

A. PBAC Zones and Positioning

The determination of a proximity zone around a resource is tied directly to the three-dimensional accuracy of the positioning system responsible for determining the location of the user. This accuracy of the positioning systems depends on the electromagnetic environment and varies dynamically over time. To compensate for errors, error contour maps could be generated for the positioning system over time and used to determine the accuracy of its location information. Several positioning systems are commercially available and can be classified into three main types: Radio frequency (RF) narrow-band, RF with ultrasound and Ultra-Wide Band (UWB). In indoor environments, UWB typically has better performance because: 1) UWB has short signal pulse making it less vulnerable to multi-path effects; 2) The interference noise is normalized over the wide signal band which has minimal effect on the Signal-to-Noise Ratio (SNR); 3) UWB operates in the 3-10GHz frequency range where few other devices would cause interference.

Apart from the positioning system, the proximity zones around resources are dependent on the access control policies for the resource. For example, suppose the access control policy of a resource mandates that a nurse yield the resource to a doctor and that the system display an on-line notification when the doctor is approaching the resource. In this scenario the system must be able to predict the movement of the doctor and notify the nurse well in advance to allow completion of work. A potential solution to this requirement would be to define a two-tier proximity zone around the resource. A small inner zone enveloping the resource would determine the resource access while a larger outer zone (e.g. the room where the resource is located) would detect anyone (i.e. the doctor) approaching the resource. Access to a vacant resource is only granted when the user enters the inner zone. However, once logged-in, the system could be configured to log-off the user only after they leave the outer zone. Establishing two-tiered proximity zones for each resource provides for the most flexibility when writing and revising access control policies. Figure 2 shows examples of single and two-tier resource proximity zones.

It should be noted that access policies of the resource only provide general guidelines for the design of the smart space, while their actual shapes and sizes are defined by the accuracy of the positioning system. Geometry of the space is a third factor affecting proximity zone design and supersedes these other requirements due to its immutable characteristics. Figure 3 depicts the input parameters in the determination of resource proximity zones.

B. Information Access Granularity

Simply defining PBAC zones as noted above is not sufficient to manage multiple users with varying degrees

of security access. Obviously for any given resource, people will have differing privileges. In the example from the previous section, the nurses session is closed by relinquishing the resource and the doctor is automatically logged-in. But the doctor may not be subsequently logged-off as long as they remain within the larger tier-2 zone thereby leaving the system open to inadvertent or malicious access by others. A similar scenario may occur if the doctor is in the proximity of the resource, but does not really intend to access it. To address this issue, we suggest three authentication levels as follows (Figure 4):

1) *No-Authentication*: User access is restricted to publicly available data. For example, bulletin announcements, Internet access, a masked public view tracking board screen, etc.
2) *Authentication Level-I*: The user is required to perform a single challenge/response (user name) session to be granted certain privileges commensurate with their organizational working group. For example, when a nurse enters the ED for the first time in the shift, she presents her badge (e.g. RFID badges) at a workstation to facilitate the required challenge-response establishing Authentication Level-I which is then associated with that user tag for the remainder of the shift. The security level and information available with Authentication Level-I is same for all caregivers working within a domain. Examples of domain include regions within the hospital, individuals, groups of caregivers and group of patients. Within the ED, if nurses were designated as a domain, then all ED nurses would have access to same set of information when authenticated at Authentication Level-I.
3) *Authentication Level-II*: Users accessing sensitive information or documenting in the patient record may require a higher level of authentication. For example, a doctor reviewing a patients chart or a nurse documenting a patient assessment. Under such circumstances it may be necessary for caregivers to undergo another challenge/response session to validate their credentials as a legitimate user for these more sensitive procedures.

Depending upon local hospital or departmental security policies and procedures, varying degrees of security can be established for a variety of scenarios. However, for most EDs, initial authentication at the beginning of the shift, with either single tiered PBAC or two-tiered PBAC where the second tier is limited to a single room to allow monitoring of log-inaccess by users should be adequate under most circumstances.

IV. Role Management in PBAC

In our approach to PBAC, we define two main types of roles - organizational and group. The organizational role is assigned to a user when they join the system and usually corresponds to the actual position held by the user within the organization, for example a person joining a hospital as a doctor gets an organizational role of a *doctor*. Group roles assigned to users are more specialized in nature and are based on a specific area or domain where the user works. For example, users working in the trauma resuscitation area of the ED form a group and get assigned to a specific group role. Similarly, groups can also be created by individual patients, i.e. all caregivers for a particular patient can be classified as a part of a group. Therefore, each user has one organizational role, but may have multiple group roles.

Each resource is assigned an access control list which is a table of possible roles (called resource-roles) and corresponding privileges. Access control decisions corresponding to privileges require the mapping of a users group role to a resource-role. When the user (in the domain) is authenticated at Authentication Level-II at a resource, the privileges obtained are based on the respective resource-role. For Authentication Level-I, each resource generates a common set of privileges based on the privileges of the individual resource-roles of each user in the domain. Figure 5 shows the scenario where the privileges corresponding to the resource-roles of all the users in the domain are input into a function f (such as union, intersection) to obtain the common privileges of the whole group. However, we do not define the function explicitly as it is implementation specific.

A. Resource Role Generation

PBAC is highly dependent upon the resource-role a user is mapped to for a particular resource. All access control decisions are made after the resource-roles are generated by each resource in a domain. To generate resource-roles, resources take into account the following:

- The users' group roles (group roles encompass the privileges of the organizational roles).
- System information context.

Figure 6 shows access control lists maintained by a resource and the mapping of a user's group role to a particular resource-role.

As mentioned, the privileges a user obtains for a resource is also dependent upon the context of the system.

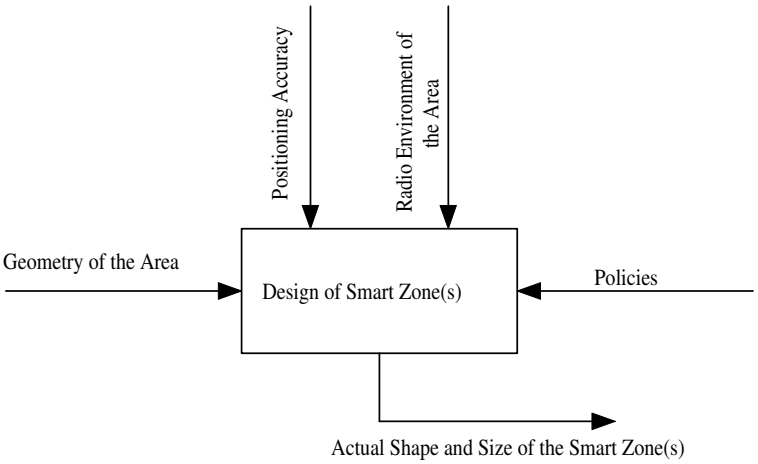

Fig. 3. Contributing factors in determining Proximity Zone

Information context allows the system to track dynamic changes and can be grouped into three categories: user context (e.g. location of the user (proximity), user's capabilities), resource context (e.g. capability of the resource, current load on the resource) and environmental context (e.g. number of users in the proximity of a resource at a given time). This classification, though accurate, is applicable only during normal operations. During critical situations, mapping group/organizational role to resource-roles based on these contexts may be counter-productive. For example, nurses brought in from other hospital departments in response to a disaster may not be granted access to resources in the smart-ED. To model context information during such disaster situations (for providing appropriate resource-roles), we define a term called Criticality.

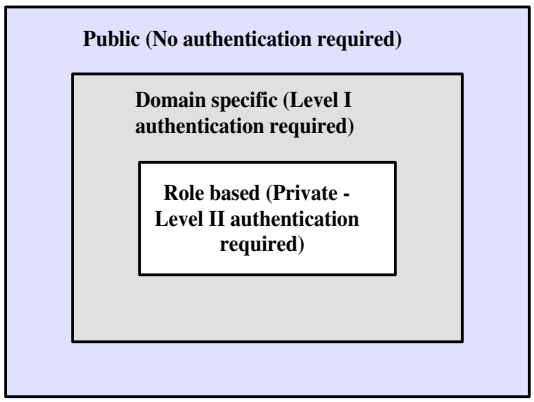

Fig. 4. Authentication Levels

Criticality is a measure of the level of responsiveness in taking corrective actions to control the effects of a critical event and is used to determine the severity of critical events. To quantify this attribute, we introduce the term *Window-of-Opportunity* (W_o), which is an application dependent parameter defining the maximum delay that can possibly be allowed to take corrective action after the occurrence of a critical event. Therefore, lower the Window-of-Opportunity of a critical event the higher its criticality. A Window-of-Opportunity = 0 indicates maximum criticality for a critical event while a Window-of-Opportunity = ∞ indicates no criticality.

The *resource-roles* assigned to a user increase as the criticality increases (We refer to the initially mapped resource-role for a user as the *base-resource-role* and the increased role as *promoted-resource-role*). The promoted-resource-role for a user is computed based on the level of criticality of the situation and this increase in role for a user is done irrespective of which level of authentication the user normally has within the system. However, to prevent instability, the promoted-resource-role does not change if the criticality remains the same or decreases. Once the critical event has been contained, the user's resource-role reverts back to base-resource-role.

To summarize our model, consider the following hospital scenarios. When a user comes in the proximity of a resource, the system obtains the current context information and maps the user to an appropriate *resource-role* which allows the user to use the resource with corresponding privileges. In case of an emergency however, patient in a cardiac arrest for example, the level of criticality is determined, which is used to decide the promoted-resource-role for the user.

V. Access Control Specifications

Each resource is assigned an Access Control List (ACL) which maps all possible resource-roles and their associated privileges. When a user comes within the proximity zone of a resource, the resource determines the role of this user and maps it on to a resource-role. Users can thus access resources based on the privileges associated with the resource-role. For the PBAC we define a set of policies to formalize aspects of the system outlined in this section.

A. Policies: Types and Implementation

In order to implement PBAC, we must define a set of policies to specify the exact rules. There are two types of policies:

- Administrative Policies - Rules for defining system administration functions, such as adding users, assigning roles, privileges, etc.
- Access Control Policies - Rules to control access to resources within the system (i.e. the decisions to account for the various roles, associated privileges and contextual information of the system at the time of the access).

1) Administrative Policies: These are a formal representation of the administrative policies for users obtaining an organizational role and group role; users being removed from an organizational and group role; and assigning resource roles to users. Below is a defined a set of state variables that the system maintains to manage these administrative processes:

- U is the set of all users in the system.
- G is the set of all groups within the system.
- OR is the set of all possible organizational roles in the system.
- $GR(i)$ is the set of group roles within a group $i \in G$ in the system.
- UOR is the set of tuples which stores the mapping between the user's id and her organizational role (<userid,user organizational role $>$) for all the users in the system.It is formally defined below:

$$UOR \rightarrow \{\{x, y\} | x \in U \wedge y \in OR\}$$

- $UGR(i)$ is the set of tuples which stores the mapping between the user's id and her group role (<userid,user group role in group i $>$). It is formally defined below:

$$UGR(i) \rightarrow \{\{x, y\} | x \in U \wedge i \in G \wedge y \in GR(i)\}$$

Adding and Removing Organizational Roles When a user is added to the system, they are assigned an organizational role based on the work perform (or will perform) within the system. Algorithm 1 specifies this process for a user, who is assigned an organizational role. This process can be carried out only by the system administrator. Similarly, Algorithm 3 specifies the removal of the organizational role of a user.

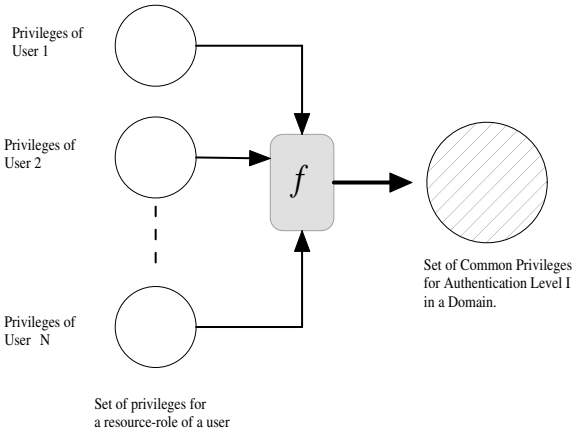

Fig. 5. Generation of domain specific privileges based on privileges of individual group roles in a group

Adding and Removing Group Roles Algorithms 2 and 4 specify the addition and removal of group role of a user. The user needs to be a part of the system (i.e. in the set U) before she can be added to any group. This operation can also be only executed by the system administrator.

2) Access Control Policies: When a user is in the proximity of a resource, they are given access to it based on the following access control policies. All these policies have been defined for a single tier proximity zone, extensions to multi-tiered zones is trivial. When a user comes within the proximity zone of a resource they are logged onto the resource. The function $checkRole$ is used to determine the appropriate role for the user and performs the following functions:

- Maps the user's group role to the appropriate resource-role.
- Generates the resource role for all the users in the group using a function f (to provide privileges corresponding to the Authentication Level-I).

The function AR then maps the returned resource role to appropriate privileges. The function $Enters(u, Z)$ returns true when a user u enters the zone Z of a resource, while the function $PBAC(u)$ stores the current privileges of the user u. When the user leaves the zone Z (function $Exits(u, Z)$ returns true) of a resource PBAC of the user becomes empty (ϕ). The Algorithm 5 defines

Algorithm 1: Adding User to an Organization and Assignment of an Organizational Role

Function Name : $addUserOrg$

Attributes : $u \in$ Set of Users, U_{admin}, $o \in$ Set of Organizational Roles

if $((o \in OR) \wedge (u \in U) \wedge checkRole(U_{admin}) = SysAdmin)$ **then**
  $U = U \cup \{u\} \wedge UOR = UOR \cup \{u, o\}$
end if

Algorithm 2: Adding User to a group number i

Function Name : $addUserGrp$

Attributes : $u \in$ Set of Users, U_{admin}, $g \in$ Set of Group Roles, $i \in$ Set of Groups

if $((i \in G) \wedge (g \in GR) \wedge (u \in U) \wedge checkRole(U_{admin},) = Sys)$ **then**
  $UGR(i) = UGR(i) \cup \{u, g\}$
end if

Algorithm 3: Remove User from Organization

Function Name : $removeUserOrg$

Attributes : $u \in$ Set of Users, U_{admin}

if $(checkRole(U_{admin},) = Sys)$ **then**
  if $((u \in U) \wedge (\forall x \in UORs.tu \in x))$ **then**
    $UOR = UOR - \{x\}, U = U - \{x\}$
  end if
  if $((i \in G) \wedge (\forall y \in UGR(i)s.t.u \in y))$ **then**
    $UGR(i) = UGR(i) - \{y\}$
  end if
end if

Algorithm 4: Remove User from Group

Function Name : $removeUserGrp$

Attributes : $u \in$ Set of Users, U_{admin}

if $((i \in G) \wedge checkRole(U_{admin},) = Sys)$ **then**
  $UGR(i) = UGR(i) - \{y\}$, $\forall y \in UGR(i)s.t.u \in y$
end if

Algorithm 5: Single User in Proximity to Unoccupied Resource

Scenario: User enters the proximity of a resource
if $(Enters(u, Z))$ **then**
  $PBAC(u) = AR(checkRole(u))$
end if

Scenario: User leaves the proximity of a resource
if $(Exits(u, Z))$ **then**
  $PBAC(u) = \phi$
end if

Algorithm 6: Single User in Proximity to Occupied Resource

if $(Enters(u2, Z) \wedge Contains(u1, Z) \wedge logout\_init(u1))$ **then**
  $PBAC(u1) = \phi$
  $PBAC(u2) = AR(checkRole(u2))$
end if

Algorithm 7: Multiple Users in Proximity to Unoccupied Resource

Policy: Choose a random user
if $(Enters(u*, Z))$ **then**
  $chosen\_user = Rand(u*)$
  $PBAC(chosen\_user) = AR(checkRole(chosen\_user))$
end if

Policy: Choose the user who is closest to the resource
if $(Enters(u*, Z))$ **then**
  $chosen\_user = Closest(u*)$
  $PBAC(chosen\_user) = AR(checkRole(chosen\_user))$
end if

Policy: Choose the user who logs in first
if $(Enters(u*, Z))$ **then**
  $chosen\_user = Earliest(login\_init(u*))$
  $PBAC(chosen\_user) = AR(checkRole(chosen\_user))$
end if

the function of automatic user login and logout on a unused resource. If another user ($u2$) enters in the zone Z (see Algorithm 6) of a resource when another user $u1$ is accessing it($Contains(u1, Z)$), then $u1$ has to explicitly logout ($logout\_init(u1)$) before $u2$ can login.

Algorithm 7 presents the scenario where multiple users enter the zone Z at the same time ($Enters(u*, Z)$), then the policy dictates giving access in three ways: randomly, to the user who is closest to the resource, or whoever requests of the resource first. When a user leaves a resource, the system checks to see how many other users are in the proximity and uses one of the three aforementioned techniques to give system access to the user.

3) Criticality Awareness: The aforementioned proximity based access control policies are sufficient when the system is working in a normal manner. However during emergency scenarios, they may not be sufficient as explained in the 4.1. To handle these critical events higher privileges may need to be assigned to users [on specific resources] to be able to control the emergency. The required level of access is provided in our system by promoting the resource-role of the user on specific resources. The initial resource-role (mapped from the user's group role) assigned to the user is referred to as the *base-resource-role* while the promoted one is called the *promoted-resource-role*. This whole process of increasing access privileges for containing critical events is called *role promotion*. In our policy specifications, the function $checkRole$ abstracts the idea of generating appropriate roles for both critical and non-critical situations.

In our previous work [19] we present a criticality aware access control model, which provides the details on handling criticality in access control models. We can use the same model here to extend the PBAC to be criticality aware. We do not provide the details in this paper, however a criticality aware PBAC will work as follows:

- The system is monitored continuously to detect the occurrence of critical events. In case of an occurrence, the system automatically finds appropriate user's who have the ability to control the effects of the critical event in the proximity and automatically provides them with higher access (role promotion) to specific resources in the domain.
- The privileges corresponding to this higher access may be even greater than privileges associated with both Authentication Level I and II for the user.
- As a user is being given privileges, which may not be available during normal system state, these higher privileges are revoked as soon as the critical event has resolved, or the user has taken all possible preventive actions using the resource [1].
- Every critical event has a window-of-opportunity associated with it. This is the upper bound of the time interval during which role of a user can be promoted. Any role promotion cannot under any circumstances exceed this value irrespective of whether criticality is controlled or not.

[1] As all possible actions have been taken with the resource, irrespective of the state of criticality, it cannot be used any more, therefore providing higher privileges on such a resource is not required

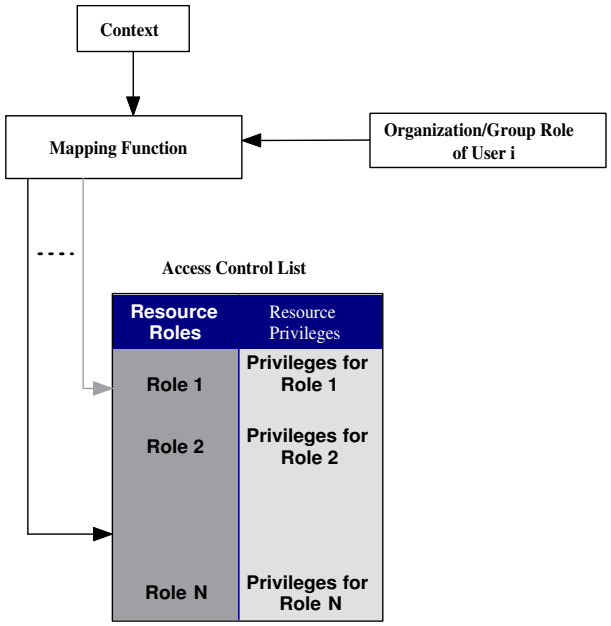

Fig. 6. Mapping of Group Role to Resource Role

- During the process of controlling criticality, the system maintains extensive logs of all the occurrences within the system in a secure manner to be able to detect malicious activity by a user with higher privileges.

VI. Discussion

The implementation of the access control policies is highly dependent on the underlying positioning system. We used a commercially available UWB-based positioning system developed by Ubisense Inc. for our experiments. Our goal at this stage is two fold: 1) to test the accuracy of the positioning system in an ED environment; 2) to develop a PBAC application by using the APIs provided by the Ubisense system.

A. Positioning System Accuracy in ED

The Ubisense positioning system uses UWB RF signals to locate objects equipped with Ubisense battery-powered transponder tags. Each tag periodically transmits UWB RF signal to the Ubisense sensors (also called base stations) which identify the tag and determines its location using Angle of Arrival (AOA) and Time Difference of Arrival (TDOA) of the signal [25]. A minimum of 4 sensors are required for a cell that defines the area within which objects may be tracked. One sensor is designated as the *master* sensor that ensures time-synchronization between all sensors (master and slaves). Further, Ubisense uses a separate control channel in the range of 908 MHz, which is used to transmit control messages to the tags.

In our field test experiment, we deployed the Ubisense positioning system in a functioning Level-One Trauma Center ED located in a major Phoenix metropolitan area hospital. In separate experiments, we used 4 sensors to create a tracking cell in two structurally different treatment areas within the ED. The following are our observations [2]

- The positioning capability of Ubisense UWB was not affected by the industrial structural walls (metal studs covered by industrial sheet-rock) of the ED. This was expected since non-metallic walls do not typically affect UWB signals, but industrial structural walls often found in hospitals was not assured.
- The positioning accuracy decreases as sensor tracking cell coverage area increases. A defined relationship between accuracy and coverage area has not yet been established.
- In most cases, the vertical orientation of the tag (or person carrying the tag) did not have an effect on positioning accuracy, although this was not always the case.
- Electromagnetic spectrum analysis of this ED in the 900-930 MHz frequency range showed activity only at 915MHz and 930MHz. These do not interfere with the Ubisense control channel at 908MHz.
- In our experiments with small tracking cells (350 sq feet), the positioning accuracy was within a range of 2-8 inches despite the presence of small metallic objects blocking the line-of-sight between the tag and sensors.

Based on the aforementioned experimental results, in the following sections, we discuss the design and implementation issues of our PBAC scheme.

B. Design of Zones

One of the important aspects of our proposed PBAC scheme is the design of the proximity zone around resources. The design of proximity zone has two aspects: 1) the shape of the proximity zone mandated by the application and its environment (policies, geometry of the area), and 2) the accuracy of the positioning system under the ED's radio environment. If S_{app} denotes the shape of a proximity zone and R_{app} is the set of distances from the resource to its boundary (mandated

[2]Due to the constant demand for treatment rooms where we were conducting our experiments, we could only perform a qualitative study of the accuracy of the positioning system.

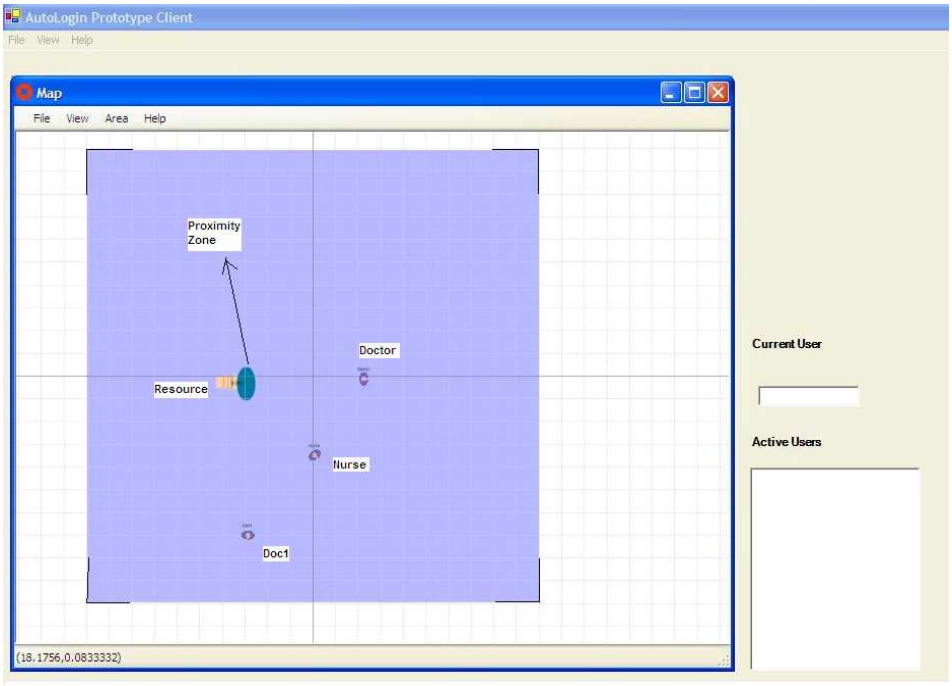

Fig. 7. All medical professionals outside the proximity of the resource

by the application), then we design the proximity zone as follows:

- The shape of the proximity zone (S) is left unchanged, i.e. $S = S_{app}$.
- The set of distances from the resource to the boundary of the proximity zone (R) is given by $R_i = i + \delta$ for all $i \in R_{app}$, where δ is the error imposed by the positioning system accuracy in ED.

For example, if the application mandated proximity zone as a circle with a radius of 5 feet around the resource, and δ is calculated as the maximum error in the positioning system (according to our experiments $\delta = 8$ inches), then we can compute the actual proximity zone as a circle with a radius of 5 feet and 8 inches.

C. PBAC Prototype Testing and Validation

We developed a prototype for the proposed PBAC scheme, which relies on the aforementioned positioning system. The working of the prototype was tested on the Ubisense tracking simulator by simulating various scenarios of medical personnel entering and leaving the proximity of a resource. We demonstrate the prototype using scenarios with three users, (two doctors (Doc1 and Doctor) and a nurse (Nurse)) and a resource. Extensions of these scenarios with large set of users and resources is trivial and therefore omitted for clarity.

1) Single User access: Figure 7 shows the screen-shot of the initial state of the system. In this state, no user has access to the resource as they are not in its proximity. As these users move about, this situation will change if and when a user comes within the proximity zone of the resource. Figure 9 shows one such state where the nurse has moved within the proximity of the resource while the two doctors have not. Our prototype uses the underlying position system to track the nurse's presence near the resource and updates its *Active Users* list which stores the identities of all the users within the proximity of the resource. As only the nurse enters the proximity of the unoccupied resource, access (to the resource) is granted to her based on the Steps 2 and 3 of Algorithm 5. The *Current User* attribute shows the name of the user who has access to the resource (Nurse).

2) Multi-user access: However if multiple users enter the proximity of an unoccupied resource simultaneously, there is a potential conflict with who gets access first. As shown in Figure 8, all the three users have now entered the resource proximity thereby updating the resource's Active Users list. To resolve the identity of the user who is provided access to the resource, we randomly choose one from the list of Active Users as given in first condition of Algorithm 7 (lines 1-5). We could have chosen any of the three methods (random, proximity to resource and login initiative) listed without any security

lapse however this is a very application dependent issue.

3) User in proximity without requiring access: So far we have described scenarios where the assumption is that the user enters the proximity zone to access the resource. However, if a user is only passing through the proximity of a resource, the system needs to ensure that such users are not logged in as it can cause a breech in the access. We address this situation at the policy level by specifying a function $Enters(u, Z)$ whose implementation ensures that only users present within the proximity zone for a certain time are provided access.

4) Temporary absence of user with resource access: It is possible that a user who has access to a resource moves out of the proximity zone temporarily. As the absence is temporary, user's session on the resource needs to be maintained for a preset amount of time. The $Exits(u, Z)$ function in our policies abstracts this idea out and ensures that a users' session is closed only after substantial absence from the proximity of a resource.

5) Authentication Issues: It should be noted that in these scenarios, all three users are in Authentication Level-I mode, and thus are granted the same set of privileges when they are allowed to access a resource. Therefore in the third scenario, when Doc1 is provided access to the resource (before Nurse and Doctor), the privileges granted are same as what Nurse or Doctor would have received (in case they were logged in). If a user needs to access more secure information than allowed at Authentication Level-I, they need to perform an additional set of challenge/response to move to Authentication Level-II. At this level a user can access secure information that is not available to others. The greater privacy requirements at this level mandates strict login and logout procedures (unlike Authentication Level-I) to prevent any loss of privacy. In actual implementation this additional challenge response can be easily done with minimal distractions using bidirectional smart tags like those provided by VeriSign [27], or Ubisense [23]. In order to incorporate this capability in our policies, we use the $login\_init$ function to abstract the idea of user performing the additional challenge response with the system.

VII. Related Work

In [20], Taylor presents a look at the Smart-Emergency Departments of the future. The paper presents many scenarios which describe various automations and workflow improvements in an ED environment. Some of the potential advances presented include: self registration, automated triage, smart medical decision making. The paper further emphasized the need of integrating various available technologies in achieving these improvements.

Smart spaces play an important role in providing the required automation in smart-EDs. Black, et. al. [15] used health-care as an example for describing issues relating to building an enterprise-wide pervasive computing application (which involves the setup of a smart environment spanning an entire enterprise). Some of the issues presented include reliability, scalability, security and privacy concerns, interaction with legacy back-end systems and the effect of a large number of interacting devices on the enterprise and beyond.

Further, a lot of interest in the research community has been directed toward smart spaces and some of the more prominent ones include Aware Home project where a smart home is aware of the whereabouts of its occupants [24], Microsofts Easy Living [25], Smart-Its project were the goal is to augment every day items with added intelligence using small-scale embedded devices thus increasing the intelligence of the environment around the user [26]. Several products are already available in the market which provides context awareness within an environment resulting in the deployment of smart spaces in offices, hospitals and homes, examples include Ubisense [23] and Radianse [22]. Though similar to these in implementation (i.e. technologies used), we describe a different approach toward defining the capabilities of smart spaces based on a set of policies applied to a collaborative environment. In the examples above, an entire environment (i.e. a house) is defined as a smart space and the focus was to develop context based services within them. We, however, focus on the scenario where the smart spaces are not omnipresent but are needed only in designated areas.

In the access control domain, Role Based Access control was first thoroughly studied in the seminal paper by Sandhu et al. [3]. This paper defined the basic components of RBAC such as user, roles, and privileges, their interactions (constraints and hierarchy). By decoupling the process of directly associating privileges with a user, RBAC provided an effective and easy way of managing security within a system. Further, it allowed easy implementation and enforcement of complex access control policies within the system. The concept of RBAC was generalized in [4] by incorporating subject roles, object roles and environment roles. As most systems are dynamic in nature, RBAC was further extended by including various context information in the access control decision making process. Some of the important work in CA-RBAC includes [5] which considered the

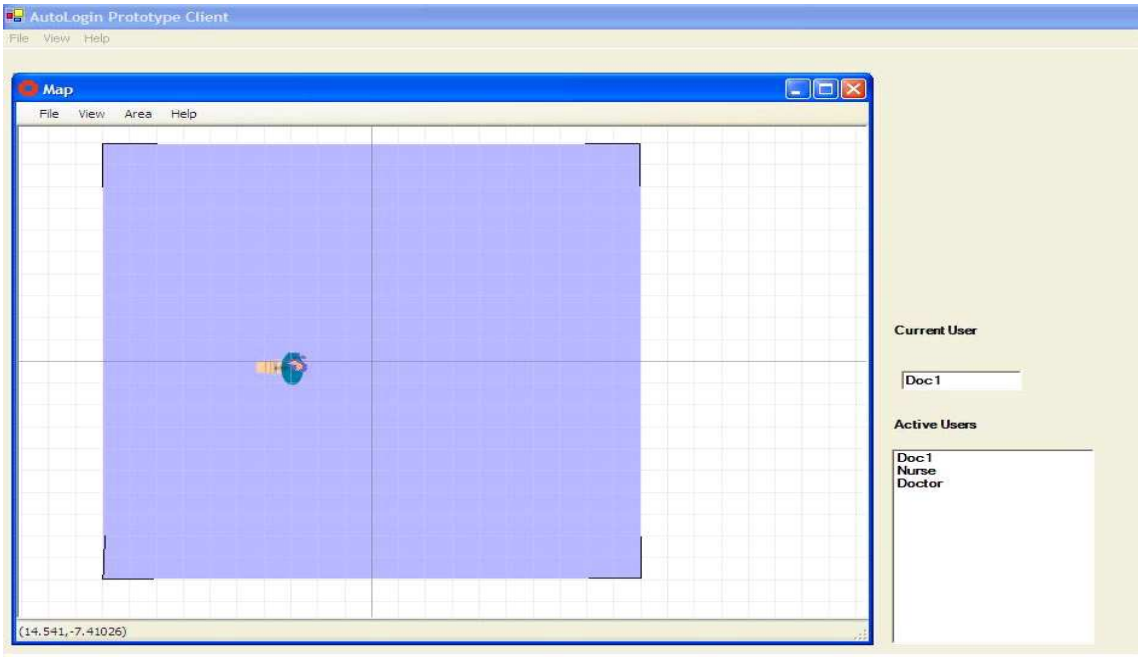

Fig. 8. All medical professionals are inside the proximity of the resource. User *Doc1* is assigned the resource at random.

spatial, temporal and resource context in access control decision making, [7] presents team based access control model which is context-aware. The idea of context-sensitive access control was formally specified in [6], which attempted to perform access control based on the context of the requested operation. McDaniel [8] suggests that context specification in CA-RBAC is implementation dependent. Strembeck et. al. [11][12] provide an integrated framework to engineer and enforce context constraints in RBAC.

Sampamane et. al. [9] present context-aware access control policies for smart spaces. They only consider spatial and subject context and define mode of access as *Individual*, *Shared* or *Collaborative* depending on the access privileges and the number of the subjects in the active space. The ideas from this work were further extended and implemented in [10], which presents an infrastructure for context aware access control and authentication in smart spaces. A dynamic context aware access control scheme for distributed health-care applications was presented in [13]. [18] presents a good survey of access control mechanisms listed above.

In [21], Bardram et. al. explore computer security in pervasive computing with focus on user authentication and present the concept of Proximity-Based User Authentication, as a highly user-friendly ideal for pervasive computing systems. They present a context-aware user authentication protocol, which (1) uses a JavaCard for identification and cryptographic calculations, (2) uses a context-awareness system for verifying the user's location, and (3) implements a security fall-back strategy. However, they do not concentrate on the specific requirements of ED in their design and further do not specify the policies which govern the automated access control decisions in such environments.

VIII. Conclusions and Future Work

A Proximity-Based Access Control scheme for secure resource access in a hospital emergency department is a viable technology to improve the ED work-flow, enhance data access, and improve patient care. We have defined the concept of proximity by identifying the contributing factors in the design of proximity zone to a resource. Further, we introduced authentication levels to prevent unauthorized access to resources based on proximity only. We presented a detailed semi-formal specification of the access control model in terms of policies. These policies were comprehensive in nature and controlled both administrative and access control functions of the system. Finally, we designed our system to be criticality aware, in that it has the ability to continuously monitor the system context information and upon detecting an unusual occurrence requiring flexibility in user access level, make appropriate changes in the policies to handle the situation. Finally, we validated the model by developing a prototype using the UWB-based positioning

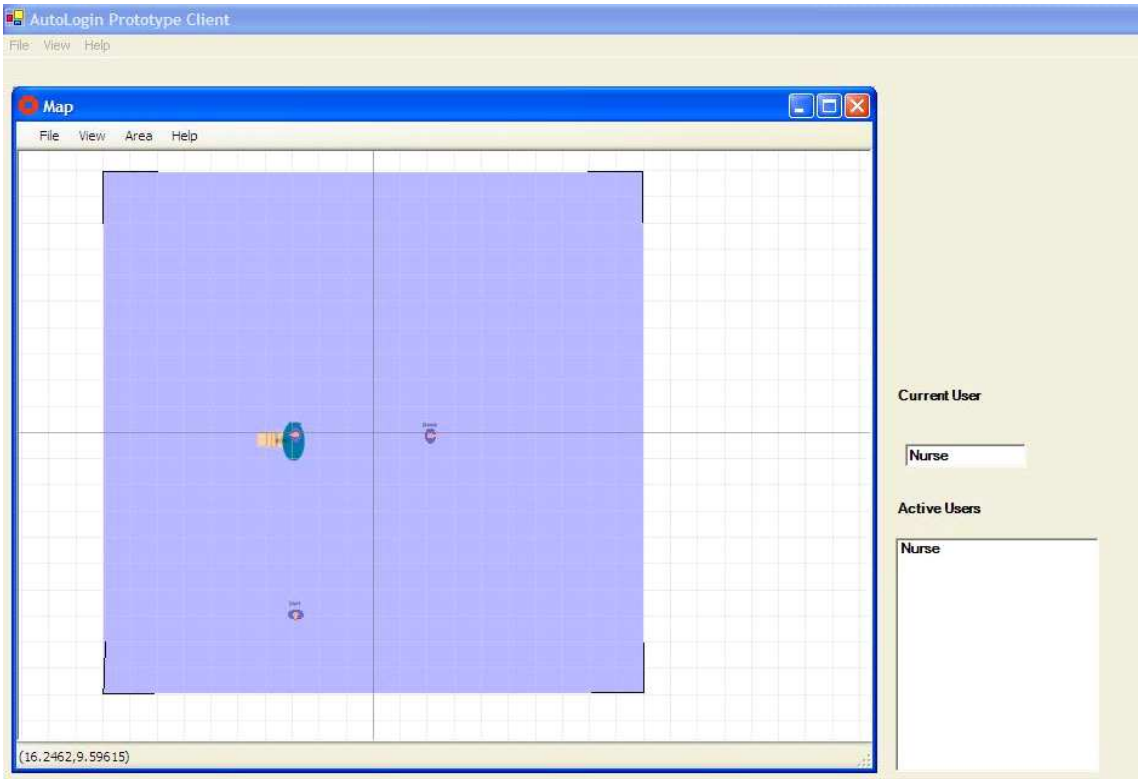

Fig. 9. *Nurse* enters the proximity of the resource

system developed by Ubisense Inc. In the future work needs to be done for: specifying a comprehensive model for designing proximity zones, and validating this in a functioning ED environment with our PBAC model.

ACKNOWLEDGMENT

We greatfully acknowledge the intellectual contributions of Valliappan Annamalai, Vikram Shankar of the IMPACT Lab at Arizona State University and the support of Zach Mortensen at MediServe Information Systems.

REFERENCES

[1] L. Cook. "Staying current on defibrillator safety". *In Journal of Nursing (33)11*, Nov 2003.

[2] E. Dijkstra. "Guarded Commands, non determinacy and formal derivation of programs". *In Communications of the ACM (18)8*, 1975.

[3] R. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman "Role Based Access Control Models". *In IEEE Computer*, Feb, 1996.pp 38-47

[4] M. J. Moyer and M. Abamad. "Generalized Role Based Access Control". *In Proc. of 21st Int. Conf. Distributed Computing System*, 2001

[5] M. J. Covington, W. Long and S. Srinivasan. "Secure Context-Aware Applications Using Environmental Roles". *In Proc. of 6th ACM Symp. on Access Control Models Tech.*, 2001

[6] A. Kumar, N. Karnik and G. Chafle. "Context Sensitivity in Role-based Access Control". *In ACM SIGOPS Operating System Review 36(3)*, July, 2002

[7] C. K. Georgiadis, I. Mavridis, G. Pangalos and R. K. Thomas. "Flexible Team-Based Organizational Access Control using Contexts". *In Proc. of 6th ACM Symp. on Access Control Models Tech.*, 2001

[8] P. McDaniel. "On Context in Authorization Policy". *In Proc. of 8th ACM Symp. on Access Control Models Tech.*, 2003

[9] G. Sampemane, P. Naldurg and R. H. Campbell. "Access control for Active Spaces". *In Proc. of ACSAC*, 2002

[10] J. Al-Muhtadi, A. Ranganathan, R. H. Campbell and M. D. Mickunas. "Cerberus: A Context-Aware Security Scheme for Smart Spaces". *In Proc. IEEE Percom*, 2003

[11] G. Neumann and M. Strembeck. "An approach to engineer and enforce context constraints in an RBAC environment". *In Proc. of 8th ACM Symp. on Access Control Models Tech.*, 2003

[12] G. Neumann and M. Strembeck. "An integrated approach to engineer and enforce context constraints in RBAC environments". *In ACM TISSEC 7(3)*, 2004, pp 392-427

[13] J. Hu and A. C. Weaver. "Dynamic, Context-aware Security Infrastructure for Distributed Healthcare Applications". *In Proc. 1st Workshop on Pervasive Security, Privacy Trust*, 2004

[14] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. "A Survey on Sensor Networks". *In IEEE Communications Magazine 40(8)*, 2002, pp 102-114

[15] J. P. Black, W. Segmuller, N. Cohen, B. Leiba, A. Misra, M. R. Ebling, and E. Stern. "Pervasive Computing in Health Care: Smart Spaces and Enterprise Information Systems". *In Proc. ACM MobiSys*, Workshop on Context Awareness, 6 pp. June 9 2004

[16] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai and S. K. S. Gupta "Poster - Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed". *In Proc. IEEE International Conference on Distributed Computing in Sensor Systems* (DCOSS), 2005

[17] N. Sastry, U. Shankar and D. Wagner "Secure verification of Location Claims". *In Proc. ACM Workshop on Wireless Security (WiSe 2003)* September 19, 2003.

[18] W. Tolone, G. Ahn, T. Rai and S. Hong "Access Control in Collaborative Systems". *In ACM Computing Surveys 37(1)*, March 2005, pp 29-41

[19] S. K. S. Gupta, T. Mukherjee and K. Venkatasubramanian "Criticality Aware Access Control Model for Pervasive Applications". *In Submission to IEEE Percom* 2006

[20] T. B. Taylor "A View of the Emergency Department of the Future.". *ACEP Section for Emergency Medical Informatics* 2000, Dallas, TX

[21] J. E. Bardram, R. E. Kjaer, and M. O. Pedersen "Context-Aware User Authentication - Supporting Proximity-Based Login in Pervasive Computing". *In Proceedings of Ubicomp 2003* Seattle, Washington, USA, 2003, pp 107-123

[22] Radianse Indoor positioning. *http://www.radianse.com/*

[23] Ubisense. *http://www.ubisense.net/*

[24] The Aware Home Project. *http://www.cc.gatech.edu/fce/ahri/*

[25] Easy Living Project. *http://research.microsoft.com/easyliving/*

[26] The Aware Home Project. *http://www.smart-its.org/*

[27] Unified Authentication Tokens. *http://www.verisign.com/products-services/security-services/unified-authentication/index.html/*