A Spatial Role-based Authorization Framework for Sensor Network-assisted Indoor WLANs

Yi Ren, Vladimir Oleshchuk, and Frank Y. Li
Dept. of Information and Communication Technology, University of Agder, N-4898 Grimstad, Norway
Email: {yi.ren, vladimir.oleshchuk, frank.li}@uia.no

***Abstract*—In this paper, we propose a spatial role-based authorization framework which specifies authorization based on both role and location constrains in a wireless local area network with assistance from a sensor network. The framework performs a location-restricted verification scheme before granting a user with privileges for crucial resources access. Analysis and simulation results show that our framework can provide double-check safeguard to confidential information, so that potential attackers cannot access the resource outside the permitted region, even though their role is verified.**

I. Introduction

With the development of wireless communications, an increasing number of Wireless LANs (WLANs) has replaced traditional wired networks in many office buildings. This trend introduces more security challenges in an organization. For instance, in wired networks, an intruder has to connect to a port to access the network resource. If the intruder cannot access a port, he cannot access data even if he gets credentials. WLANs, however, broadcast messages by using radio channel. Therefore, intruders can access to network resource from any location within the coverage. Although many schemes such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, etc. were developed for guaranteing reasonable level of security, an intruder who gets credentials still can access resource from physically remote location. Moreover, in wired networks, if an intruder connects to a port and begins transmitting packets, these packets can be traced to the port connected, and the intruder's machine can be physically located and disconnected. However, in wireless networks, the intruder's machine is associated with a given Access Point (AP), and it is not enough to physically locate it.

To prevent the above mentioned security threats, we propose a spatial role-based framework for office buildings based on sensor network-assisted indoor WLANs. Our scheme can be used for different scenarios. For example, in a school, a teacher may want students to take an on-line exam using a WLAN. Access privileges and locations have to be constrained for preventing candidates from looking for answers on the Internet and from "ringers" who take tests for other students outside exam room by using their credentials.

The framework performs authorization checks before allowing a localization service to locate a mobile terminal within a specific position covered by a wireless network. The key purpose of checking location is to confirm that the requesting mobile terminal is within area associated with access permission. The location verification scheme proposed in this paper provides additional safeguard that protect critical information. Performance evaluation of the proposed scheme in an office environment is also given in this paper.

The remainder of the paper is organized as follows: In Section II, we introduce necessary background and related work. In Section III, we present the overview of our authorization framework. In Section IV, we describe an application scenario of our framework. The performance of our framework in an office environment is evaluated in Section V, and finally the paper is concluded in Section VI.

II. Related work

To set the scene of this paper, we begin with some background information on distance estimation techniques, role based authorization, and location determination which are relevant to our framework.

A. Distance estimation techniques

Many proposals about distance estimation based on different techniques have been developed. Generally speaking,there are four main categories namely, Received-Signal-Strength (RSS), Time-Difference-of-Arrival (TDoA), Time-of-Arrival (ToA), and Angle-of-Arrival (AoA). This section introduces two of these approaches in brief.

Received Signal Strength: RSS [1] measures the distance based on the strength of signal received. Let us denote this received signal strength by $P_r(d)$. The received signal strength can be expressed by $P_r(d) = \frac{cP_t}{d^\alpha}$, where P_t is the transmitted signal strength, d is the distance between transmitter and receiver, c is the path loss model parameter, and α is the path loss coefficient. Therefore, the distance d can be calculated as $d = \sqrt[\alpha]{\frac{cP_t}{P_r(d)}}$.

Time Difference of Arrival: TDoA [2] computes the distance based on the arrived time difference of broadcast radio(Radio Frequency, RF) and Ultrasound (US). When the transmitter sends the RF and US signals at the same time, the receiver will receive two signals at different times because the speeds of these two signals are different. The arrived time difference of RF and US can be calculated as $T_{US} - T_{RF}$, where T_{US} is the arrived time of US, and T_{RF} is the arrived time of RF.

B. Role based authorization

Traditional authorization specifies the access rights of individual users. In mobile computing environment, the Spatial Role Based Access Control (SRBAC) model where spatial location of users were used as authorization parameters was first proposed in [3], and later elaborated in [4]. SRBAC supports spatial constraints on enabling and disabling of roles, and can be used to constrain the set of permissions available to the roles that a user may activate at a given location. The authors in [5] proposed a location mapping function between physical and logical locations allows roles depending on the user's logical location. They based on the Google Maps API to get the location of users.

C. Location determination

There are several location awareness schemes with different techniques for both indoor and outdoor position estimation of mobile terminals.

The authors in [6] proposed a hybrid TDoA/RSS solution to estimate location of mobile terminals. In this scheme, sensors compute the distance between them and transmitters which send the signals they received based on RSS and TDoA. As

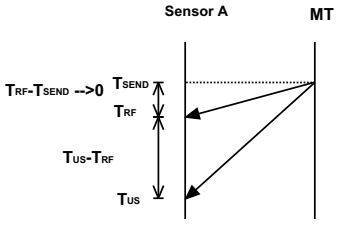


Fig. 1. Example of TDOA.

shown in Fig. 1, $Distance = (T_{US} - T_{SEND}) * V_{US}$, where T_{US} denotes the time when US signal arrivals the sensor, T_{SEND} denotes the time when transmitters send the US signal, and V_{US} denotes the speed of the sound signal. However, since time synchronization is a difficult task in sensor networks, sensors which receive the signals can't compute the distance by using T_{SEND}. Since the speed of RF is much faster than the speed of US and the time of RF propagation is almost equal to zero for short distances, the authors assume $T_{RF} - T_{SEND} = 0$ (the time of RF propagation), and use $T_{US} - T_{RF}$ instead of $T_{US} - T_{SEND}$. Thus the distance between sensor and transmitters can be computed as $Distance = (T_{US} - T_{RF}) * V_{US}$.

Using three non-collinear sensor nodes with known positions, a set of three equations is derived based on the trilateration and Pythagorean Theorem. The mean square error can be computed based on the set of three equations. Furthermore, in order to get more accurate location of the mobile terminals, the author gets the mean of I iterations which are collected in different time. Therefore, RSS can be expressed as $d(mean) = \frac{1}{I}\sum_{i=1}^{I} d(i)$, where $d(mean)$ denotes the mean of distance estimated by RSS; and TDoA can be expressed as $D(mean) = \frac{V_{US}}{I}\sum_{i=1}^{I}(T_{US}(i) - T_{RF}(i))$, where $D(mean)$ denotes the mean of distance determined by TDoA.

III. Overview of the Authorization Framework

In this section we introduce the network architecture of our framework, and demonstrate how our framework authorizes access based on both role and location, and finally propose an improved time and power based localization scheme.

A. Network architecture

Based on the network architecture described in related research [7], we propose a three-tier hierarchical network architecture for our framework. This architecture, as depicted in Fig. 2, consists of two kinds of networks: sensor networks and a WLAN. The sensor network is divided into several

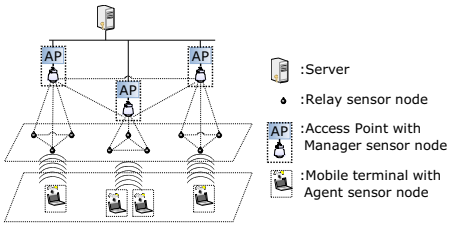


Fig. 2. An architecture for spatial role-based authorization scheme where the location of a mobile terminal is determined by joint operation of agent, relay and manager sensor nodes.

groups. There are three types of sensor nodes in each group: agent sensor nodes, relay sensor nodes, and manager sensor nodes. The agent sensor nodes attached to the mobile terminals communicate with the relay sensor nodes and send e.g. RF and US signals which will be sensed by relay sensor nodes. The relay sensor nodes distributed in the coverage area of an AP are responsible for recording the arrived time difference of the RF and US signals broadcasted by agent nodes, sensing the strength of the arrived signals, and forwarding them to the manager node of their group. Each group has a group leader called manager sensor node, which is attached to AP. The manage sensor node is used to collect distance messages, estimate the location of the mobile terminals, broadcast messages to the sensor nodes, and transmit the location messages to the AP attached to it.

The choice of communication technology is critically important. There are several aspects that should be considered such as energy efficiency, adequate data rate, reduced size and low price of sensor nodes. Because of that ZigBee (IEEE 802.15.4) may be seen as suitable communication technology for sensor networks.

B. Location verification service

The location determination in our framework is considered as a Location Verification Service, which relies on the sensor networks. The relay sensor nodes distributed in the office environment which is covered by WLANs are responsible for sensing and estimating the location of the agent sensor nodes. When they receive the requests from their neighbor agent sensor nodes, they begin to record the arriving time difference of e.g. RF and US signal and sense the strength

of them, and then they send the messages which contain the distance information of the agent sensor nodes to the manager sensor nodes which are the nearest ones from them via other relay sensor nodes. Manager sensors attached to APs collect messages from their neighbor relay sensor nodes and transmit to the server via the AP attached by them.

Whenever a user with mobile terminal wants to access the protected important information, the location verification service will perform a set of checks. These checks include authenticating whether the username and password of the requesting user are matched, confirming whether the role has the permission to access the location service, determining whether the location of the requesting mobile terminal is allowed. These processes are illustrated in Fig. 3, and explained step-by-step as follows:

1. A user with mobile terminal wants to access the protected important information and is asked to send username and password to the Server.

2. The Server requests the user's authorization data from the Authorization Database (ADB).

3. The ADB returns the user's authorization data. The Server authenticates whether the role of the user has the right to request the permission of the location service. The Server rejects the access request if the user hasn't the privilege.

4. The Server grants the certificate of Location Verification Service to the Mobile Terminal if the role of the user has the privilege.

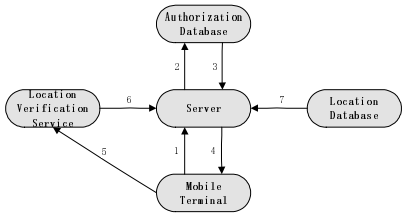


Fig. 3. Example of a location verification service where a user with mobile terminal trying to access the protected important information is constrained by his present location.

5. The Mobile Terminal which receives the certificate of Location Verification Service forwards it to the Location Verification Service to request service.

6. The Location Verification Service calculates the current location of the Mobile Terminal, and sends the position of the Mobile Terminal to the Server.

7. The Server sends a request to the Location Database about the authorization regions of the accessed information. The Server rejects the access request if the position of the mobile terminal is not in these regions and allows the user access the protected important information if the position of the mobile terminal is in these permitted regions.

C. Role based authorization

In our scheme, as shown in Fig. 4, privileges are assigned to users according to both their roles and their locations. That is the privilege of a user depending dynamically on which

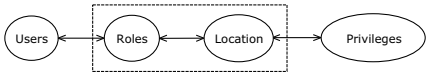


Fig. 4. User, role, location and permission relationships

geographic zone it is currently located in, even though the role is static for the same user.

Definition 1: The role and location based authorization model is defined as follows:

- $USERS$, $ROLES$, $LOCS$, and $PRGS$ (users, roles, locations, and privileges);
- $USERS$, the set of $U = \{u_1, u_2, ..., u_i\}$;
- $ROLES$, the set of $R = \{r_1, r_2, ..., r_j\}$;
- $LOCS$, the set of $L = \{l_1, l_2, ..., l_k\}$, and $l_m \cap l_n = \phi$ for $m \neq n$;
- $PRGS$, the set of $P = \{p_1, p_2, ..., p_t\}$;
- $UA \subseteq USERS \times ROLES$, the relation that associates users with roles, UA: User Assignment;
- $PA \subseteq PRGS \times ROLES \times LOCS$, the relation that assigns a privilege to a role available in location. PA: Privileges Assignment;
- $assigned\_users : (r : ROLES) \rightarrow 2^{USERS}$, the mapping of role r onto a set of users;
- $assigned\_privileges : (r : ROLES, l : LOCS) \rightarrow 2^{PRGS}$, the mapping of role r and location l onto a set of privileges. Formally: $assigned\_privilege(r,l) = \{p \in PRGS | (p,r,l) \in PA\}$;
- $assigned\_roles : (l : LOCS) \rightarrow 2^{LOCS}$, the mapping of location l onto a set of roles;
- $session\_user(s : SESSIONS) \rightarrow USERS$, the mapping of session s onto the session's associated user;
- $session\_roles(s : SESSIONS) \rightarrow 2^{USERS}$, the mapping of session s onto a set of roles. Formally: $session\_roles(s_i) \subseteq \{r \in ROLES | (session_user(s_i), r) \in PA\}$;
- $session\_location(s : SESSIONS) \rightarrow LOCS$, the mapping of session s onto the session's associated location.

Role and location authorization: A session can never have a privilege unless it is assigned the right role and also in the permitted location.

User Assignment (UA): $\forall s : SESSIONS, u : USERS, r : ROLES$

$r \in session\_roles(s) \wedge u \in session\_user(s) \Rightarrow u \in assigned\_users(r)$

- *Assigned user*: $SESSIONS \times ROLES \times USER \rightarrow BOOLEAN$;
- $Assigned\ user(s,r,u) = 1$ if session s can be assigned user u when it is assigned a role r, 0 otherwise.

Privileges Assignment (PA): $\forall s : SESSIONS, p : PRGS, r : ROLES$, and $l : LOCS$

$r \in session\_roles(s) \wedge u \in session\_privileges(s) \wedge l \in session\_location(s) \Rightarrow u \in assigned\_privileges(r,l)$

- *Assigned privilege*: $SESSIONS \times ROLES \times LOCS \times PRGS \rightarrow BOOLEAN$;
- *Assigned privilege* $(s,r,l,p) = 1$ if session s can be

assigned privilege p when it is assigned a correct role r and is in specified location l, 0 otherwise.

Fig. 5 illustrates the set of dynamic mapping and static relations that are necessary for a user to get a privilege. The dotted arrows depict dynamic mappings, and the solid arrows depict static relations.

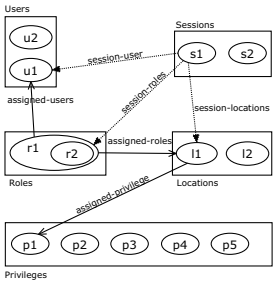


Fig. 5. User u_1 can get privilege p_1 because $p_1 \in assigned\_privileges \wedge r_1 \in assigned\_roles \wedge u_1 \in assigned\_users \wedge l_1 \in session\_locations(s_1) \wedge r_1 \in session\_roles(s_1) \wedge u_1 \in session\_user(s_1)$.

D. Mobile terminal authorization

In order to protect the location messages in the sensor network, all the distance and location messages transmitted need to be encrypted. Since sensors are constrained in computation and energy resource, asymmetric key cryptography is too expensive to adopt. Instead, we use symmetric key cryptography solutions.

There are four kinds of keys: 1) *a global symmetric key* share with all sensor nodes to provide data confidentiality; 2) *a session key* shared between the agent sensor node and the group leader manager sensor node is used to provide agent node and manager node authorization; 3) *a pairwise key* shared between the relay sensor node and the group leader manager sensor node used to provide data confidentiality; 4) *a pairwise group key* shared between the manager node and its neighbors' group leader.

After the network deployment, the network planner has to set the parameters of the relay sensor nodes that let the nodes know their coordinates (x_i,y_i). When the user of a mobile terminal wants to access some data which need location verification, the server would ask the user to send his U_{Na}, P_u , and G_m which were broadcast by the manager sensor node, and then verify whether they are available. If the user is permitted to use the location verification service, the server would send a session key, which is computed with pseudorandom function H to the agent node u and the manager node m as $K_{u,m} = H(U_{Na}, G_m)$, where $K_{u,m}$ denotes the session key shared between agent node u and manager node m, U_{Na} denotes the user's user name, and G_m is the index of manager sensor node m's group. The agent receives Ku,m, then broadcasts signal as $E_{K_0}(E_{K_{u,m}}(S_{num}), S_{num})$, where E_{K_0} denotes the encryption value using key K_0, and S_{num} denotes the sequence number of agent sensor node's signal. The relay sensor nodes sense these signals, compute the distance between them and the mobile terminals, and send the distance message to the manager node as $E_{K_r}(E_{K_{u,m}}(S_{num}), d)$, where d denotes the distance between the agent sensor node and the relay sensor node. The manage node receives the messages sent from relay sensor nodes, and estimates the location of the mobile terminal.

E. An improved time and power based localization scheme

The scheme which performs location verification must be able to obtain the location of the requesting mobile terminal in order to confirm whether the position of the requesting mobile terminal is allowed within the wireless network.

The authors in [6] proposed a time and power based localization scheme (TPLS). TPLS is based on TDOA and RSS using RF and US signals to determine and to detect the distance differences from the wireless mobile terminal to three sensor nodes. These distance differences are averaged through time iterations in order to reduce random effects of the noise, shadowing and fading. They found that when the number of iterations approaches 250, the average error distance converges with an error of 0.5m. However, the users of the location service suffer from a waiting time of 250 iterations despite the time is short (maybe 20 seconds, but it is not acceptable). We propose a new method so that the iterations not only based on the time iteration but also based on the combination of the distance messages of the relay sensor nodes.

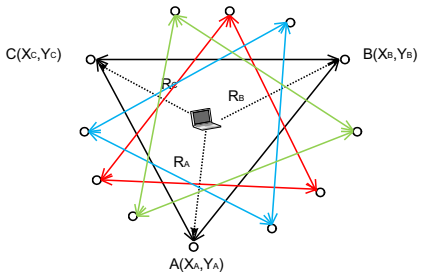


Fig. 6. Random combinations of relay sensor nodes.

As shown in Fig. 6, the manager sensor node, which collects the distance message d_u^r of agent sensor node u which is sent from the relay sensor node r of its group, randomly selects three distance message of the messages received. The iterations I can be expressed as $I = \binom{n}{3} = \frac{n!}{3!(n-3)!}$, where n is the number of neighbor relay sensor nodes of agent sensor node located. Therefore, the manager sensor node can compute more iterations in much shorter time. Users who want to obtain the right to access the restricted information can pass the location verification quickly without waiting for a long period.

IV. Application Scenarios

Role and location based authorization schemes will likely play an important role in future WLANs for authorization. Users with mobile terminals can enjoy various services and different information because of their roles to which they assigned and locations in which they currently locate, as one example illustrated below.

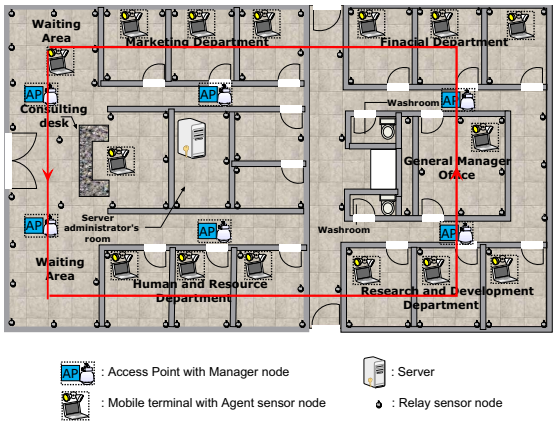


Fig. 7. A work path of a mobile terminal in an office environment.

A. Indoor office building

Let us consider an application scenario in an office space, as shown in Fig. 7. We just consider a simple scenario that there are four departments in a company. The total office space can be divided into 6 zones, which are public zone, human and resource department zone, research and development zone, general manager office, financial department zone, and marketing department zone. In the office space of the company, laptops or other mobile terminals are needed to attach to agent sensor nodes which broadcast signals to their neighbor relay sensor nodes if their users want to enjoy the service and information which are needed to location verification. In contrast, guests of the company, who are not allowed and do not need to access important data, can use their laptops without the agent sensor nodes with the guest role account which has the lowest privilege and is the most restricted in the waiting area which is restricted by the location verification as well. Therefore, employees in different departments assigned to different roles can access the services and information associated with their corresponding departments. Eight privileges are denoted as P0, P1, P2, P3, P4, P5, P6, and P7. The definitions of these 8 privileges are given below:

- P0 is specified with no permission, users who get P0 can't access WLAN including the Internet.
- P1 is specified to guest role, user without username and password will be assigned P1 automatically in public zone. P1 only has the privilege which can access the Internet or be specified some permission of the resource of the company by the administrator.
- In public zone, clerks of the company with username and password will be assigned P2 which can access Internet and Intranet information of the company.
- P3-P5 are assigned to different departments, and have the privilege to access crucial data of corresponding department if and only if they located in specified zone.
- P7 is assigned to general manager who has the privilege to access all key data of company only from general manager office.

TABLE I
PRIVILEGES WITH RESOURCES

	P0	P1	P2	P3	P4	P5	P6	P7
External Internet		√	√	√	√	√	√	√
Public resource of the company			√	√	√	√	√	√
Intranet of the marketing dep.				√				√
Intranet of the human and resource dep.					√			√
Intranet of the financial dep.						√		√
Intranet of the R&D dep.							√	√

As shown in Table 1, different privileges have variable permission to access the resources. The key data of each department only gives access permission to the user who has the corresponding privilege of that department or the privilege of the general manager. For example, P5 is assigned to financial department, and has the permission to access the crucial data of financial department only from the zone of the marketing department and some other zones specified by the administrator.

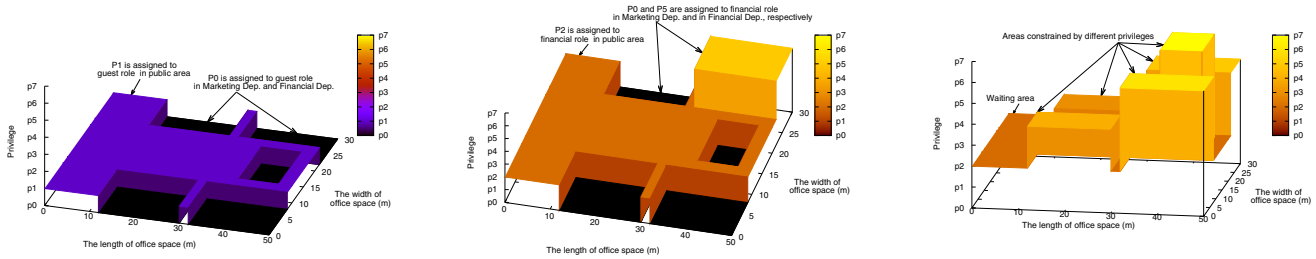
V. PERFORMANCE EVALUATION

We implemented our authorization framework in OPNET 14.0. Unless otherwise stated, the simulation[1] is set up as follows. As shown in Fig. 7, we use 77 relay sensor nodes and 6 manager sensor nodes uniformly distributed in the office space which is 50m in length and 30m in width, respectively. Two users are considered in our simulation, user 1 is assigned to guest role, user 2 is assigned to financial clerk role. We assume that a user with mobile terminal follows the red line and walks anticlockwise around the office space using the guest role and financial clerk role, respectively. The user starts at coordinate (6, 4), gets cross (41, 4), (41, 26), (6, 26), and finally back to (6, 4) at the speed of 1m/s. The total length of the journey is 114m, and we can easily know that the total time is 114 second. We sample the result every 0.05 second, and get 2281 hits for each simulation.

In Fig. 8 and Fig. 9, the results show that these two users spend 114 seconds to complete the journey. As our framework expected, these two users get the same privileges P0 they cannot access any resource when they go through department zones. In public zone and financial department, they get different privileges. The user with guest role who gets P1 can only access the external Internet in public zone and P0 in financial department zone; the user with financial clerk role getting P2 can access the Internet and public resource of the company in public zone and P5 has the permission to enjoy the confidential information of financial department in financial department zone.

In Fig. 10, we got privilege maps of performance results with guest role, financial role, and general manager role, respectively. As shown in Fig. 10(a), a user with guest role who got P1 in public zone can access the Internet rather than the resource of the company, and P0 in department zone . In

[1]In this simulation, we do not consider the factor of office wall of each department; and the user can get cross the wall follow the red (deep dark) line.



(a) A privilege map of guest role. (b) A privilege map of financial role. (c) A privilege map of general manager role.

Fig. 10. Privilege maps of performance results with guest role, financial role, and general manager role.

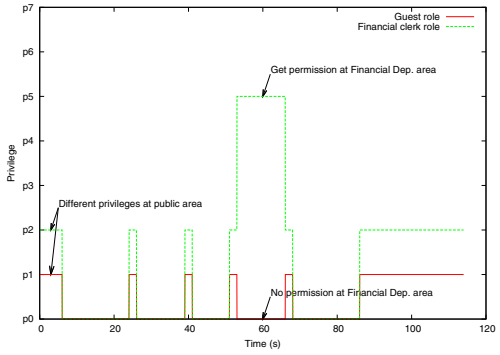


Fig. 8. Performance results with time and privilege.

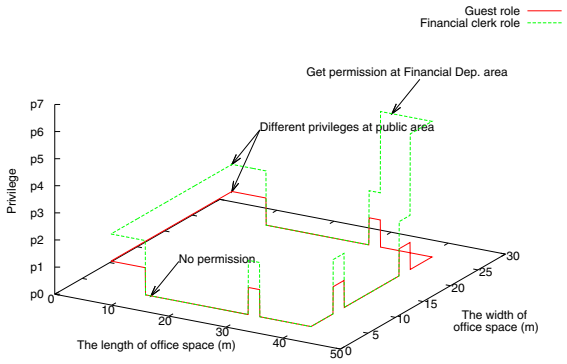


Fig. 9. Performance results with office space coordinate and privilege.

Fig. 10(b), a user with financial role who got P2 in public zone, got P5 in financial Dep. zone where he can enjoy confidential data of financial Dep. and got P0 in other department zones which means that even if a marketing clerk as an intruder got credential of financial role, he still got P0 in marketing Dep. zone. In Fig. 10(c), a user with the highest privilege general manager role who got corresponding privileges in different department zones can access data of corresponding department but still can access public resource of the company in public for he got privilege P2. Therefore, the confidential data of departments will not be revealed outside the department zones, even if the credentials are revealed.

VI. Conclusions

In this paper, we have proposed a spatial role-based authorization framework for using sensor network-assisted indoor WLANs. With this framework, administrators not only can constrain intruders with correct credentials access to the confidential information when they are out of the zone specified but also can locate where the intruder mobile terminals are. Users have to not only use the legal username and password but also be located at the specified zones in order to access confidential resources. With this scheme, crucial resources are protected by two level authorization mechanisms. Our framework also improves the time and power based localization scheme from time iteration to random combination iteration which takes a shorter time to position mobile terminals, and performs location authorization checks before allowing a user to access crucial resource. To evaluate the performance of our framework, we conduct several simulations in an office environment. The simulation results show that the proposed framework can constrain users' privileges depending on their location, and provide additional safeguard for access to crucial information.

References

[1] G. Giorgetti, S. Gupta, and G. Manes, "Optimal RSS threshold selection in connectivity-based localization schemes," in *Proc. of ACM MSWiM'08*, Vancouver, Canada, October 2008, pp. 220–228.

[2] S. Ergut, R. Rao, O. Dural, and Z. Sahinoglu, "Localization via TDOA in a UWB Sensor Network using Neural Networks," in *Proc of ICC'08*, Beijing, China, May 2008, pp. 2398–2403.

[3] F. Hansen and V. Oleshchuk, "Spatial Role-based Access Control Model for Wireless Networks," in *Proc. of VTC'03-Fall*, vol. 3, Orlando, Florida, USA, Oct 2003, pp. 2093–2097.

[4] ——, "SRBAC: A Spatial Role-based Access-control Model for Mobile Systems," *Proc. of the 7th Nordic Workshop on Secure IT Systems (NORDSEC03)*, 2003.

[5] I. Cruz, R. Gjomemo, B. Lin, and M. Orsini, "A Location Aware Role and Attribute Based Access Control System," in *Proc. of ACM GIS'08*, Irvine, CA, USA, November 2008, pp. 1–2.

[6] A. El Moutia, K. Makki, and N. Pissinou, "TPLS: A Time and Power Based Localization Scheme for Indoor WLAN Using Sensor Networks," in *Proc. of IEEE Conference on Technologies for Homeland Security'07*, Woburn, MA, USA, May 2007, pp. 117–122.

[7] S. Zhao, K. Tepe, I. Seskar, and D. Raychaudhuri, "Routing Protocols for Self-organizing Hierarchical Ad Hoc Wireless Networks," *IEEE Sarnoff Symposium*, 2003.