Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 198580, 8 pages
http://dx.doi.org/10.1155/2014/198580

Research Article

An Efficient and Secure *m*-IPS Scheme of Mobile Devices for Human-Centric Computing

Young-Sik Jeong,[1] Jae Dong Lee,[2] Jeong-Bae Lee,[3] Jai-Jin Jung,[4] and Jong Hyuk Park[2]

[1] *Department of Multimedia Engineering, Dongguk University, Seoul 100-715, Republic of Korea*
[2] *Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea*
[3] *Department of Computer Engineering, Sun Moon University, Asan 330-150, Republic of Korea*
[4] *Department of Multimedia Engineering, Dankook University, Cheonan 330-714, Republic of Korea*

Correspondence should be addressed to Jong Hyuk Park; parkjonghyuk1@hotmail.com

Received 14 October 2013; Accepted 4 January 2014; Published 23 March 2014

Academic Editor: Jianhua Ma

Recent rapid developments in wireless and mobile IT technologies have led to their application in many real-life areas, such as disasters, home networks, mobile social networks, medical services, industry, schools, and the military. Business/work environments have become wire/wireless, integrated with wireless networks. Although the increase in the use of mobile devices that can use wireless networks increases work efficiency and provides greater convenience, wireless access to networks represents a security threat. Currently, wireless intrusion prevention systems (IPSs) are used to prevent wireless security threats. However, these are not an ideal security measure for businesses that utilize mobile devices because they do not take account of temporal-spatial and role information factors. Therefore, in this paper, an efficient and secure mobile-IPS (*m*-IPS) is proposed for businesses utilizing mobile devices in mobile environments for human-centric computing. The *m*-IPS system incorporates temporal-spatial awareness in human-centric computing with various mobile devices and checks users' temporal spatial information, profiles, and role information to provide precise access control. And it also can extend application of *m*-IPS to the Internet of things (IoT), which is one of the important advanced technologies for supporting human-centric computing environment completely, for real ubiquitous field with mobile devices.

1. Introduction

Rapid developments in wireless and mobile IT technologies have led to their application in many real-life areas, such as disasters, home networks, mobile social networks, medical services, industry, schools, and the military. In today's contemporary information-oriented society, mobile devices are increasingly being utilized in diverse business and social areas of life. Business/work environments have become wire/wireless, integrated with wireless networks. Although the increase in the use of mobile devices that can use wireless networks increases work efficiency and provides greater convenience, wireless access to networks represents a security threat.

In wired networks, solutions such as intrusion prevention systems (IPSs), instruction detection systems (IDSs), and firewalls are used to prevent illegal external access. In wireless network environments, wireless IPSs are used to reinforce security against accessing mobile devices. Wireless IPSs have also been developed to prevent security threats that may occur in wireless environments. However, they are vulnerable to attack because they use pattern-based engines to detect potential attacks. Furthermore, business/work environments are too diversified to enable accurate detection and prevention of attacks. In essence, the same rules cannot be applied to all mobile business devices because of considerations of time, space, and individual roles [1, 2].

Table 1: Characteristics of MAC, DAC, and RBAC.

	MAC	DAC	RBAC
Access authority	System	Owner	Central authority
Criteria of access	Security level	Identity	Role
Strategy	Stiff	Flexible	Flexible
Merits	Secure	Easy implementation, flexible response	Easy management
Demerits	Difficult implementation and management, high cost, and low performance	Possible illegal behavior	Existence of conflict roles

In this wireless IPS study, trends and related security threats and requirements in mobile business work environments are discussed. An efficient and secure mobile-IPS (*m*-IPS) is proposed for businesses utilizing mobile devices in mobile environments for human-centric computing, which should provide the ease of utility of mobile devices for protecting from threats. The *m*-IPS system incorporates temporal-spatial awareness in human-centric computing with various mobile devices and checks users' temporal-spatial information, profiles, and role information to provide precise access control. And it also can extend application of *m*-IPS to the Internet of things (IoT), which is one of the important advanced technologies for supporting human-centric computing environment completely, for real ubiquitous field with mobile devices.

This paper is organized as follows. In Section 2, we discuss related works: research trends of access control. We discuss wireless security threats and requirements in Section 3. We explain the detailed proposed scheme: *m*-IPS scheme including main concept, system architecture, service scenario, and evaluation in Section 4. Finally, the conclusion should be provided in Section 5.

2. Related Work

Access control techniques are traditionally subdivided into mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC). In MAC, only the administrator has access and directly controls network access by other users after checking access classes. This technique has disadvantages such as the following: control is difficult if the numbers of users increase or if there are diverse access classes. Therefore, it is not well suited to commercial applications. DAC regulates access to objects based on the identity of the subjects or the organizations to which they belong. With DAC, users can illegally pass on access permissions to other individuals or groups. RBAC allows users to access information related to the specific roles that they have been assigned. In real-life settings, RBAC may not be appropriate because of conflicts that may occur between roles [2–5]. The characteristics, merits, and demerits of access control techniques are set forth in Table 1.

Wireless IDSs monitor the radio spectrum for the existence of illegal access points (APs) and malicious devices and the presence of wireless attack tools. In general, wireless IPSs refer to systems that implement not only detection but also prevention based on the level of risks after automatic classification. These systems aim at preventing unauthorized access to local area networks of wireless devices and other information assets. A wireless IPS is composed of a server, a database, sensors, and a console. The server collects raw data from multiple sensors and analyzes the collected data. The database is used to store information obtained from the sensors and servers. The sensors monitor wireless signals and the information obtained from the server. The console provides an interface for the administrator and users who need information from the server or sensors [6, 7].

Chen et al. proposed a wireless IPS framework using signature detection rules based on specific device information that can reduce false-positive rates and intelligent prior attack recognition engines that can predict and prevent attackers [1]. Silas et al. described wireless security threats and a method to respond to these threats through wireless IPSs [7]. Nyanchama and Osborn proposed a common framework for wireless IPSs and described core technologies used in the framework [6]. Kirkpatrick et al. proposed a wireless IDS using short message service technology, which proactively detects common wireless attacks, such as WEP cracking, MAC address spoofing, and war driving [8]. Timofte proposed a wireless transport layer-based IPS model that can detect and block user traffic through a logical single path between all wireless devices and the destination [9]. Zhang et al. described four major blocking techniques in wireless networks and assessed their blocking performances by a device manufacturer based on test beds for these methods and discussed the implications of their experimental results for wireless IPS designs [10]. Hsieh et al. proposed a model for wireless attack detection and prevention using honey pot-based intelligent prior attack recognition engines and tried to minimize false-positive rates using this model [11]. Tahir [12] provides our understanding of domain and introduced spatial domain roles. It is emphasized that purpose should be attached to spatial roles that should be represented within organizational domains that may have multilevel and multidomain relationships. And it is also shown how our extended RBAC model can make use of the notion of spatial domain to allow administrator to flexibly partition the objects according to geographical boundaries.

3. Wireless Security Threats and Requirements

In this chapter, wireless security threats and requirements are discussed in detail prior to constructing a temporal-spatial awareness-based efficient m-IPS scheme to enable more secure use of mobile devices in business and social life.

3.1. Threats in Wireless Security. General wireless security threats that may occur in business and social life using mobile devices include rogue evil twin APs, ad hoc networks, RF jamming, deauthentication, MAC spoofing, WEP key cracking, and sniffing [1, 2]. Table 2 classifies wireless security threats with respect to confidentiality, integrity, and availability (three elements of security) that may occur in business and social life using mobile devices.

The following are examples of security threats that may additionally occur in business and social life using mobile devices if temporal-spatial and role elements are not considered in wireless IPSs.

Case 1. When temporal-spatial elements are not considered: in an office environment using mobile devices that provide service to users, logs may increase rapidly due to floating populations. This will cause system overloads and adversely affect the ability of the wireless IPS to detect illegal devices and judge the level of threat. If mobile device security is necessary in nonpermanent spaces, such as meeting rooms at particular times, wireless device detection and blocking based on uniform rules will be difficult.

Case 2. When roles are not considered: existing wireless IPSs use access control lists (ACLs) of user names and groups to provide mobile device security. However, ACLs cannot detect malicious acts that are carried out by devices registered: on the so-called white list of privileged users. For instance, an attacker could acquire the device of a finance department staff member with diverse access rights and then bypass the firewall and wirelessly access the server of this department to revise, copy, or delete files. Access cannot be prevented because the request will have come from a device viewed as secure.

3.2. Requirements for Wireless Security. To prevent wireless security threats in business and social life using mobile devices, three elements of security, confidentiality, integrity, and availability, plus access control based on temporal-spatial and role elements, are required. With regard to confidentiality, wireless signals can be propagated to many unspecified users in mobile offices, and sensitive data, such as personal information and financial details, stored in wireless terminals are quite likely to be leaked. Wireless terminals are more vulnerable than wired terminals to security attacks from wireless sniffing and evil twin APs. All businesses have to take steps to help prevent such attacks [1, 6, 7, 10, 11]. Regarding integrity, the so-called Man in the Middle attacks may cause system failure and work confusion. These involve illegal changes and deletions in data and forged data insertion during wireless communication transmission between mobile devices. Security measures that can guarantee integrity during data transmission in wireless spaces are necessary [1, 6, 7, 10, 11]. With respect to availability, Denial of Service attacks damage system availability and productivity, thereby reducing system resources and accessibility to information. Therefore, in business and social environments that depend on wireless communication using mobile devices, measures are required to prevent RF jamming on layer 1 and layer 2 of Open System Interconnection (7 layers) systems and to prevent attacks, such as DoS using deauthentication packets [1, 13–15].

To reduce false-positive ratesand system loads in business and social settings where diverse mobile devices, roles, and environments exist, the mobile-intrusion prevention system (m-IPS) is needed toensure better access control based on temporal, spatial, and contextual roles for efficiency and security. The access control should be able to respond to diverse exceptions that may occur in offices [2, 5, 6].

Table 2: Classification of wireless security threats during business work using mobile devices.

Threat classification	Confidentiality	Integrity	Availability
Rogue AP	o	o	—
Ad hoc network	o	—	—
Evil twin/honeypot AP	o	o	—
RF jamming	—	—	o
Deauthentication	—	—	o
MAC spoofing	o	o	—
WEP key cracking	o	o	—
Sniffing	o	—	—

o: effect, —: no effect.

4. m-IPS Scheme Based on Temporal-Spatial Awareness and C-RBAC

In this chapter, aspects of the TA-RBAC-based m-IPS scheme that can detect mobile device security threats in business and social settings, including use of case scenarios, are discussed in detail. The components and constraints of m-IPS systems are outlined as follows.

(i) *Components:*

(1) *user*: the person with authority to check time, locations, and roles

U = {user1, user2,. . ., user N};

role: the specific work/tasks assigned to individual members

R = {role1, role2,. . ., role N};

(2) *authority*: the permissions allocated to the user, consisting of time (t) and location (L) values

P = {perm1, perm2,. . ., perm N}

perm = (t, location);

(3) *time*: one of the conditions that constitute authority. T values consist of start values (ST),

end values (ET), and repeating cycles (C). The cycles are divided into days, weeks, and months
$T = \{t1, t2, \ldots, tn\}$
$t = (ST, ET, C)$
$ST, ET =$ (year, month, day, hour, minute)
Cycle = (day, week, month);

(4) *location*: is one of the conditions that constitute authority. L values mean permitted places and consist of floor and room values
$L \subseteq F \times R$
$L = \{$location1, location2,. . ., location $N\}$
location = (floor, room)
$F = \{$floor1, floor2,. . ., floor $N\}$
$R = \{$room1, room2,. . ., room $N\}$.

(ii) *Constraints:*

(1) *user-role*: $UR \subseteq U \times R$
$UR = (ur1, ur2, \ldots, ur\ N)$
$ur =$ (user, role)

(2) *role-permission*: $RP \subseteq R \times P$
$RP = (rp1, rp2, \ldots, rp\ N)$
$rp =$ (role, perm)
$rp =$ (role, perm (T (ST (year, month, day, hour, minute), ET (year, month, day, hour, minute), C (day, week, month)), location (floor, room))).

4.1. Contextual Role-Based Access Control. In RBAC, the user-role relationship is more dynamic than the role-permission relationship. As a result, context can be categorized into static constraints, for example, user nationality, salary, and so on, and dynamic constraints, for example, time, location, and purpose, of the user for which access request has been made. One approach to enforce the dynamic context oriented policies is to rapidly change the permission assignment relations that depend on the dynamic contexts. Another approach is to define permissions that should consider the static and dynamic behavior of context constraints. Based on this, the adoption of the existing well-known access control models and technologies is sensible as it provides a means to extend from traditional to context-based access control policies and facilitates obligation policies enforcement [2, 3, 12].

Mobile computing environments are characterized by many aspects, one of which is their potential size. Several definitions of the concept domain have been given in the literature.

Definition 1 (domain). Domain is a logical bound defined over some space that contains at least one mobile device object, whereas space and mobile device object are identifiable by the mobile computing environment.

Definition 2 (temporal domain). Temporal domain describes a logical bound that surrounds at least one or a list of mobile device objects and contains temporal roles identified by the mobile computing environment.

Definition 3 (spatial domain). Spatial domain describes a logical bound that surrounds at least one or a list of mobile device objects and contains spatial roles identified by the mobile computing environment.

In general, RBAC is a very useful access control model but due to the distributed and heterogeneous nature of organizations, subject centric (traditional RBAC) is not sufficient. With the rapid advancement in technologies today, organizational resources are widely distributed in mobile computing environments. Also users can send request to access the resources at any time from any location. Under these circumstances, an extension of RBAC model is necessary in order to properly manage the organizational resources in multidomain environment keeping in mind the confidentiality, integrity, and availability. We used the C-RBAC model [12], an extension of traditional role-based access control model that allows security administrators to define context oriented access control policies enriched with the notion of purposes. By adding purpose roles, we extend traditional access control model that helps organizations to know *which* user can perform *what* operation on *which* object with *what* purpose. In this paper, we used the following CRBAC core elements [12, 16]: (1) user, roles, permissions, and user-to-role mappings; (2) mobile device objects which are the set of all mobile device objects; (3) role-to-permission mappings with the same meaning as permission-to-role mappings in this model; (4) the set of all entities related to the authorizations; (5) the set of all mappings; and finally (6) the set of sessions as tuple of <*user, role, permission*>. Figure 1 should be used as the basics of extended C-RBAC model in this paper.

4.2. System Architecture. The existing wireless IPSs use pattern-based detection engines to determine whether to block mobile devices. They then record the results in ACLs and DB and provide functions to block or allow entirely. However, this method is vulnerable to attacks by individuals purporting to be permitted users, who can then easily act without any restriction on time, space, or roles. Furthermore, the existing IPS methods are unable to make allowances for exceptional circumstances with respect to time, spaces, or roles that may occur with mobile devices used in work and social settings. An *m*-IPS scheme is proposed in this study to address these difficulties in control and wireless security threats. The scheme determines the locations of mobile devices based on wireless signals picked up by sensors and first checks whether the locations and current time are allowed values. The profiles of the mobile devices accessed in mobile environments are then compared with stored profiles. Finally, the permissions allocated to the mobile devices are checked to ensure precise and safe access control of individual mobile devices. The *m*-IPS scheme is largely composed of *m*-IPS-ME agent, *m*-IPS-ME AP, *m*-IPS-ME sensors, *m*-IPS-ME server, and *m*-IPS-ME DB. Figure 2 shows the architecture of the *m*-IPS for the mobile environment with TA-RBAC.

The ***m*-IPS-ME agent** stores and manages the profiles of user devices. The profiles are used to check permissions when devices access networks. In addition, the *m*-IPS-ME

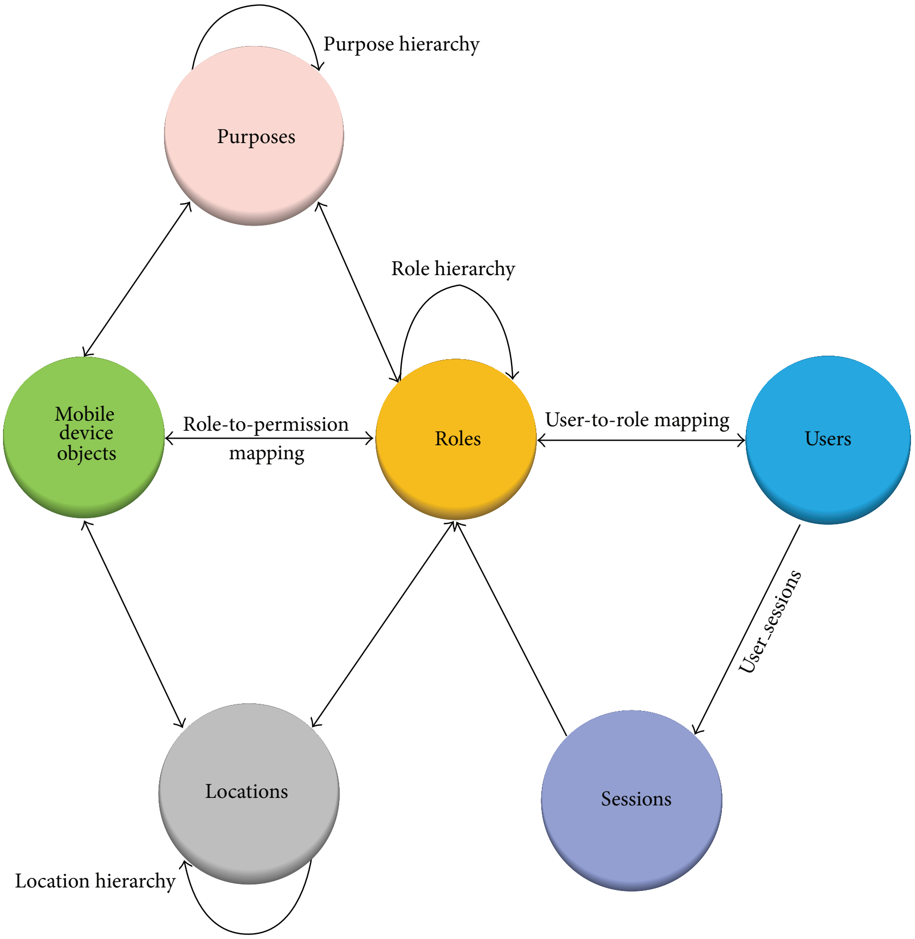

Figure 1: Contextual role-based access control model.

model features an access module for controlling the agent. The *m*-IPS-ME AP performs the communication function for the agent to access the wireless network. The ***m*-IPS-ME sensor** detects the location of the mobile device through the scanning module when the agent accesses the wireless network. The sensor management module controls the agent's communication based on the information sent from the server. The ***m*-IPS-ME server** registers the device profiles in advance. When the agent requests access to the network, the server compares the profile and the role information of the agent with the role information stored in the ***m*-IPS-ME DB** to allow communication by relevant devices to the sensor AP in case the two sets of information are identical to each other.

Table 3: Term and explanation.

Term	Explanation
***m*-IPS-ME Agnt**	*m*-IPS mobile environments with TA-RBAC agent
***m*-IPS-ME AP**	*m*-IPS mobile environments with TA-RBAC AP
***m*-IPS-ME Sensor**	*m*-IPS mobile environments with TA-RBAC sensor
***m*-IPS-ME Svr**	*m*-IPS mobile environments with TA-RBAC server
***m*-IPS-ME DB**	*m*-IPS mobile environments with TA-RBAC database

4.3. Service Scenario.

The service scenario of the proposed *m*-IPS TA-RBAC system for the mobile environment is reviewed in this section. The coefficients employed in the service scenario are defined in Table 3.

Figure 3 illustrates the service scenario of the model. When the user wishes to access the wireless network in an office, meeting room, or social environment, the model checks whether the user's location and the current time are within the allowed ranges. Thereafter, the model compares the profile requested by the agent with the profile information stored in the database to see if they are the same. The agent role information should also match.

The detailed operation processes based on service scenario are as follows:

(1) ***m*-IPS-ME Agnt→*m*-IPS-ME AP**: Req_Conn (profile_agnt)

***m*-IPS-ME AP→*m*-IPS-ME Svr**: Req_Conn (profile_agnt)

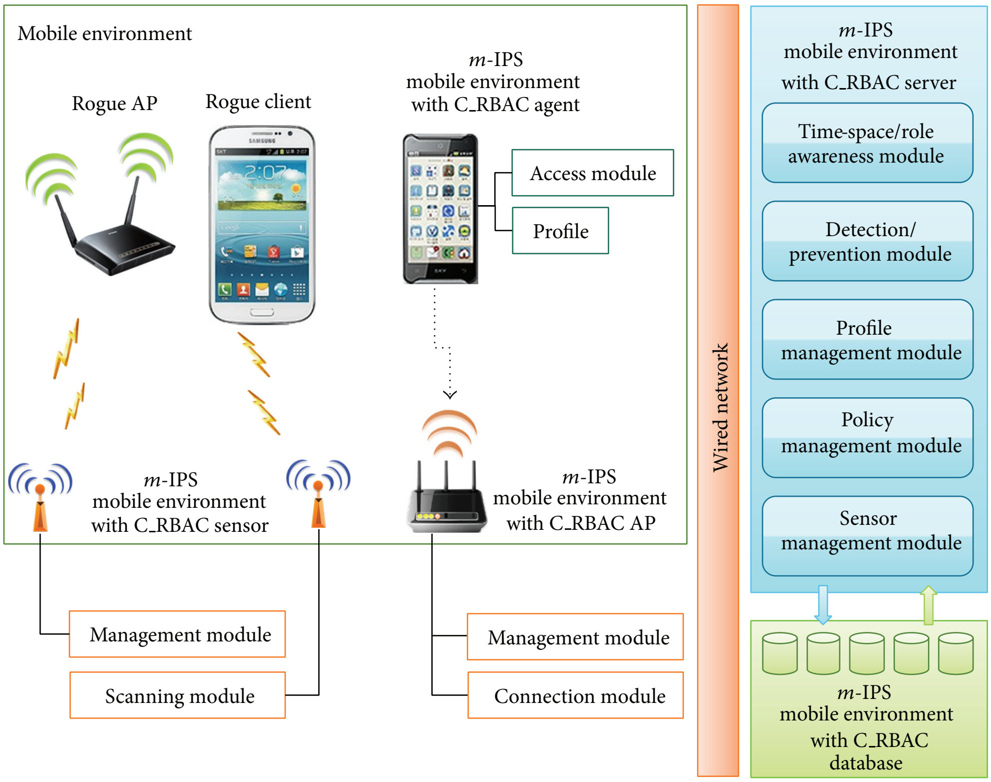

Figure 2: *m*-IPS for mobile environment with temporal-spatial awareness-RBAC (TA-RBAC) architecture.

The *m*-IPS-ME Agnt sends the profile_agnt information to the ***m*-IPS-ME Svr** through ***m*-IPS-ME AP** and requests a connection;

(2) ***m*-IPS-ME Svr→*m*-IPS-ME DB**: Req_Profile

***m*-IPS-ME DB→*m*-IPS-ME Svr**: Resp_Profile (profile_db)

To check the user's profile, the ***m*-IPS-ME Svr** sends a request to the ***m*-IPS-ME DB** for the profile of the relevant user to receive profile_db;

(3) ***m*-IPS-ME Svr→*m*-IPS-ME sensor**: Req_Positioning

To identify the location of the *m*-IPS-ME Agnt, the *m*-IPS-ME Svr sends a request to the *m*-IPS-ME sensors to measure the signals;

(4) ***m*-IPS-ME sensor**: Scanning

Multiple ***m*-IPS-ME sensors** measure the intensity of the signals from the ***m*-IPS-ME Agnt;**

(5) ***m*-IPS-ME sensor→*m*-IPS-ME Svr**: Resp_Position (sig)

Multiple ***m*-IPS-ME sensors** transmit the information on the intensity of the signals from the ***m*-IPS-ME Agnt** to the ***m*-IPS-ME Svr**;

(6) ***m*-IPS-ME Svr**: Positioning( )

It analyzes ***m*-IPS-ME sensor** signals to determine the location;

(7) ***m*-IPS-ME Svr→*m*-IPS-ME DB**: Req_Allowed List(pos,time)

***m*-IPS-ME DB→*m*-IPS-ME Svr**: Resp_Allowed List(pos,time)

The ***m*-IPS-ME Svr** checks whether the location of the ***m*-IPS-ME Agnt** and the current time are within the allowed ranges according to the ***m*-IPS-ME DB;**

(8) ***m*-IPS-ME Svr**: Decision( )

***m*-IPS-ME Svr**: Compare(profile_agnt, profile_db)

After checking whether the location and the current time are within the allowed ranges based on the identified time and location information, the ***m*-IPS-ME Svr** judges whether to implement the second stage of authentication. In addition, the ***m*-IPS-ME Svr** compares the profile of the agent collected as set forth under (2) to the profile in the DB to judge whether to implement the third stage of authentication;

(9) ***m*-IPS-ME Svr→*m*-IPS-ME DB**: Req_AllowedList (role)

***m*-IPS-ME DB→*m*-IPS-ME Svr**: Resp_AllowedList (role)

The ***m*-IPS-ME Svr** checks whether the role of the agent is identical to the **DB** role information in the ***m*-IPS-ME DB**;

(10) ***m*-IPS-ME Svr→*m*-IPS-ME sensor**: Req_sensor_control

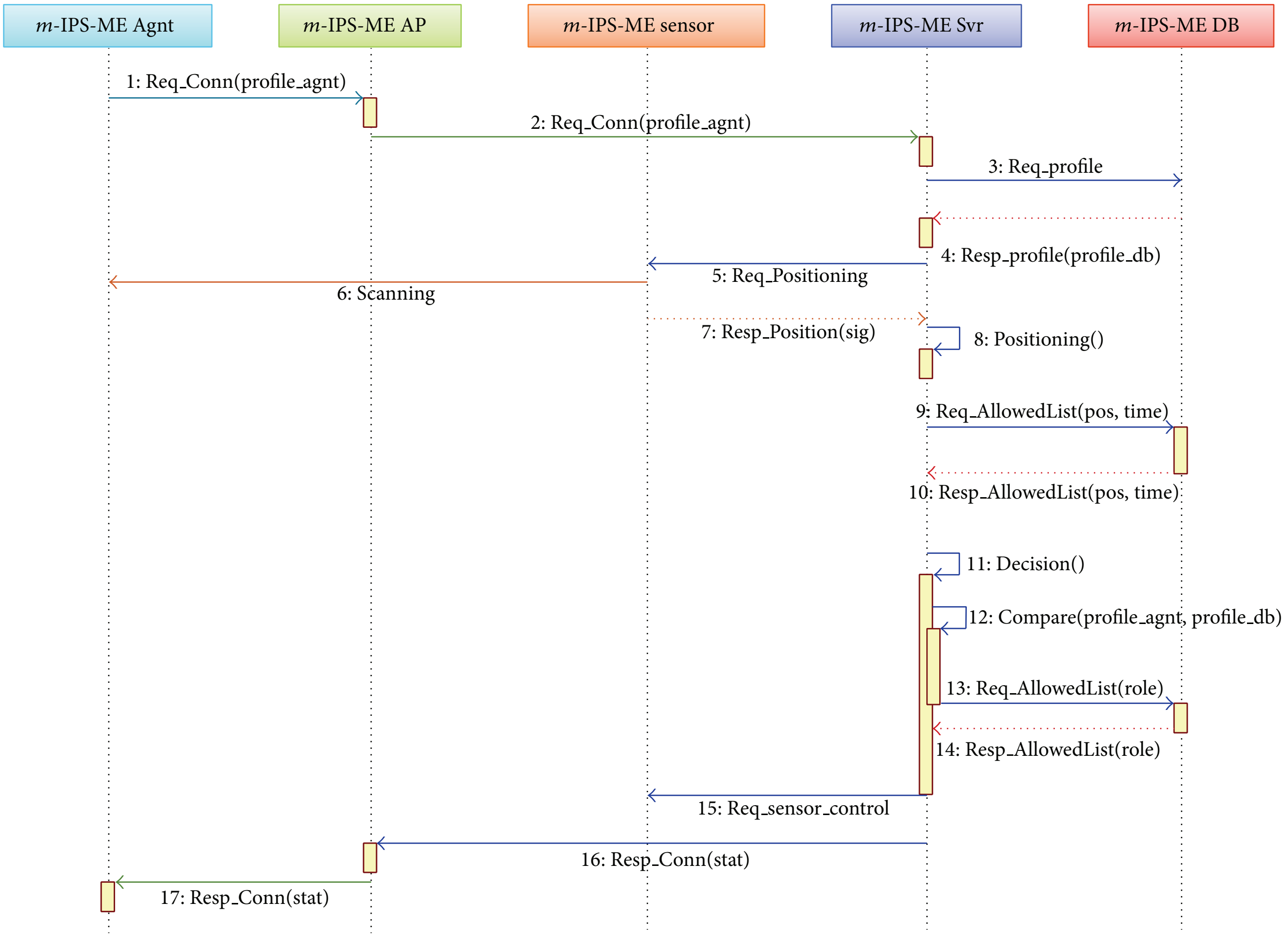
m-IPS-ME Agnt
m-IPS-ME AP
m-IPS-ME sensor
m-IPS-ME Svr
m-IPS-ME DB
1: Req_Conn(profile_agnt)
2: Req_Conn(profile_agnt)
3: Req_profile
4: Resp_profile(profile_db)
5: Req_Positioning
6: Scanning
7: Resp_Position(sig)
8: Positioning()
9: Req_AllowedList(pos, time)
10: Resp_AllowedList(pos, time)
11: Decision()
12: Compare(profile_agnt, profile_db)
13: Req_AllowedList(role)
14: Resp_AllowedList(role)
15: Req_sensor_control
16: Resp_Conn(stat)
17: Resp_Conn(stat)

FIGURE 3: Service scenario.

Depending on whether the connection is allowed, the ***m*-IPS-ME Svr** requests the ***m*-IPS-ME Sensor** to restrict or not signals from the ***m*-IPS-ME Agnt**;

(11) ***m*-IPS-ME Svr→*m*-IPS-ME AP**: Resp_Conn(stat)

***m*-IPS-ME AP→*m*-IPS-ME Agnt**: Resp_Conn(stat)

The ***m*-IPS-ME Svr** transmits connection information(stat) to the ***m*-IPS-ME Agnt** through the **wireless IPS-MO_AP**.

4.4. Evaluation for Efficiency and Security. In Table 4, the existing methods described in Section 2 and the proposed method are compared and analyzed. The methods were judged based on whether they can prevent wireless security threats that may occur in business/work and social settings utilizing mobile devices as set forth in Section 3. The method proposed by Wen-chu Hsieh focused only on detection by wireless IDSs and thus requires additional systems for prevention. The method proposed by Chen et al. improved false-positive rates using signature detection and planned recognition-based wireless IPSs but did not consider information on temporal-spatial elements and roles. Thus, false-positive rates are still not improved in mobile business and social environments where flexible access control is necessary. As shown in Table 4, the performance of the *m*-IPS scheme described in this paper is superior to that of Sandhu et al. [3] and Nyanchama and Osborn [6]. The notation ○ means the strong secure mechanism for providing to mobile environments, and △ means the medium secure method for mobile devices of mobile business, and finally × is the weak point for security threats in mobile devices.

5. Conclusion

The use of diverse wireless devices, such as smartphones and smart pads, has increased rapidly in a short period. Work environments have also changed, with wired and wireless networks coexisting. Wireless IPSs are used to provide secure communication in these environments. However, the existing wireless IPSs are universal security systems equipped to deal only with general security. They have many problems due to the absence of temporal-spatial and role elements, and they are ill equipped to deal with security associated with wired/wireless composite work environments and offices. In the future, security threats in work environments are expected to become more frequent and to cause more damage.

Table 4: Characteristics comparison and analysis among the existing methods and the proposed method.

Criteria	Method		
	Wen-chu Hsieh [3]	Nyanchama and Osborn [6]	*m*-IPS
Rogue AP	△	○	○
Evil twin	△	○	○
MAC spoofing	△	○	○
MIMT	△	○	○
DoS attack	△	○	○
Honeypot	△	○	○
Access control with *m*-IPS and C_RBAC	×	×	○

○: strong, △: medium, and ×: weak.

In this paper, the concept and the configuration of a wireless IPS were discussed, in addition to security threats and requirements in mobile environments by using mobile devices. Therefore, an efficient and secure mobile-IPS (*m*-IPS) has been proposed for businesses utilizing mobile devices in mobile environments for human-centric computing. This system incorporates temporal-spatial awareness and checks users' temporal-spatial information, profiles, and role information to provide precise access control. This research is meaningful in that access control is provided by checking users' temporal-spatial information, profiles, and role information, thereby leading to safer use of mobile devices in offices. To further improve the security of mobile devices, additional studies on the access modules used with these devices are necessary.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the CPRC (Communications Policy Research Center) support program supervised by the KCA (Korea Communications Agency) (KCA-2013-003).

References

[1] G. Chen, H. Yao, and Z. Wang, "An intelligent WLAN intrusion prevention system based on signature detection and plan recognition," in *Proceedings of the 2nd International Conference on Future Networks (ICFN '10)*, pp. 168–172, January 2010.

[2] E. Georgakakis, S. A. Nikolidakis, D. D. Vergados, and C. Douligeris, "Spatio temporal emergency role based access control (STEM-RBAC): a time and location aware role based access control model with a break the glass mechanism," in *Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11)*, pp. 764–770, July 2011.

[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Computer role-based access control models," *IEEE Computer Society*, vol. 29, no. 2, pp. 38–47, 1996.

[4] X. Zhou, Y. Ge, X. Chen, Y. Jing, and W. Sun, "A distributed cache based reliable service execution and recovery approach in MANETs," *Journal of ConvergenceNo*, vol. 3, no. 1, pp. 5–12, 2012.

[5] A. U. Bandaranayake, V. Pandit, and D. P. Agrawal, "Indoor link quality comparison of IEEE 802. 11a channels in a multi-radio Mesh network testbed," *Journal of Information Processing Systems*, vol. 8, no. 1, pp. 1–20, 2012.

[6] M. Nyanchama and S. Osborn, "The role graph model and conflict of interest," *ACM Transactions on Information and System Security*, vol. 2, no. 1, pp. 3–33, 1999.

[7] S. Silas, K. Ezra, and E. B. Rajsingh, "A novel fault tolerant service selection framework for pervasive computing," *Human-Centric Computing and Information Sciences*, vol. 2, no. 5, pp. 1–14, 2012.

[8] M. S. Kirkpatrick, G. Ghinita, and E. Bertino, "Privacy-preserving enforcement of spatially aware RBAC," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 5, pp. 627–640, 2012.

[9] J. Timofte, "Wireless intrusion prevention system," *Revista Informatica Economica*, vol. 47, pp. 129–132, 2008.

[10] Y. Zhang, G. Chen, W. Weng, and Z. Wang, "An overview of wireless intrusion prevention systems," in *Proceedings of the 2nd International Conference on Communication Systems, Networks and Applications (ICCSNA '10)*, pp. 147–150, July 2010.

[11] W. Hsieh, C. Lo, J. Lee, and L. Huang, "The implementation of a proactive wireless intrusion detection system," in *Proceedings of the 4th International Conference on Computer and Information Technology (CIT '04)*, pp. 581–586, IEEE Press, September 2004.

[12] M. N. Tahir, "C-RBAC: contextual role-based access control model," *Ubiquitous Computing and Communication Journal*, vol. 2, no. 3, pp. 67–74, 2007.

[13] D. Lijun, Y. Shengsheng, X. Tao, and L. Rongtao, "WBIPS: a lightweight WTLS-based intrusion prevention scheme," in *Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 2298–2301, IEEE Press, September 2007.

[14] A. Vartak, S. Ahmad, and K. N. Gopinath, "An experimental evaluation of Over-The-Air (OTA) wireless intrusion prevention techniques," in *Proceedings of the 2nd International Conference on Communication Systems Software and Middleware*, pp. 1–7, IEEE Computer Society, January 2007.

[15] G. Chen, H. Yao, and Z. Wang, "Research of wireless intrusion prevention systems based on plan recognition and honeypot," in *Proceedings of the International Conference on Wireless Communications and Signal Processing (WCSP '09)*, pp. 1–5, IEEE Computer Society, November 2009.

[16] D. Zou, L. He, H. Jin, and X. Chen, "CRBAC: imposing multi-grained constraints on the RBAC model in the multi-application environment," *Journal of Network and Computer Applications*, vol. 32, no. 2, pp. 402–411, 2009.