

## Improving Mobile Device Classification using Security Events for Preventing Wireless Intrusion

Hyeokchan Kwon, Sin-Hyo Kim,

*Electronics and Telecommunications Research Institute,  
218 Gajeong-ro, Yuseong-gu, Daejeon, Korea  
{hckwon, shykim}@etri.re.kr*

### Abstract

*In current wireless intrusion prevention system (WIPS), the mobile devices are classified into one of three or four categories by classification algorithm for preventing wireless intrusion. But such a classification mechanism has difficulty to delicate control the wireless access of mobile device to an access point because of its simple classification. And it cannot estimate potential security threats arising from security vulnerability of mobile device itself. In this paper we improve mobile device classification for preventing wireless intrusion. In the proposed algorithm, the mobile devices are classified into nine categories. To do this we utilize the security related events of the device from the mobile device management (MDM) and authorization server.*

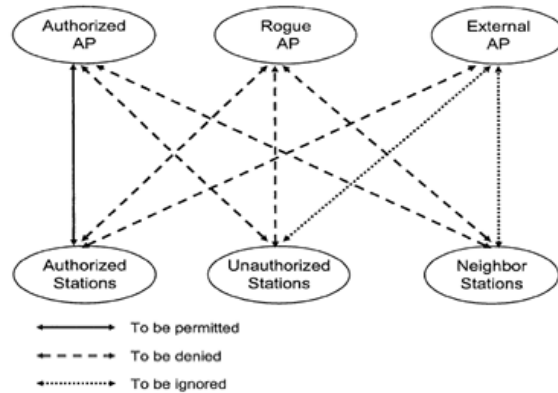
**Keywords:** *WIPS, MDM, device classification, wireless security, wireless access control, wireless intrusion prevention*

### 1. Introduction

The wireless intrusion prevention system (WIPS) has a function of detection and prevention of wireless intrusion such as man-in-the middle attack, denial of service attack, rogue access point based attack, illegal information leakage and so forth. WIPS consists of security management server and security sensors. The security management server manages security sensor, policy and monitors security status, threat of wireless network. The security sensors monitor radio frequency signals for the presence of rogue access point, unauthorized device, unauthorized association, malicious traffic and so on.

In current WIPS system, the mobile devices are classified into one of three or four categories by classification algorithm for preventing wireless intrusion. Generally, such a classification includes *authorized*, *unauthorized*, *guest* and *external* device. In case of AirTight [1], a representative wireless intrusion prevention system, classifying the mobile devices into three categories: *authorized*, *unauthorized* and *neighbor*. In case of access point (AP), it is classified into three categories: *authorized*, *rogue* and *external*. Figure 1 shows the AP and device classification criteria and association policy of AirTight [1].

In general, an “authorized device” refers to the device allowed by the wireless network administrator. An “unauthorized device” refers to the device not allowed by the wireless network administrator. A “guest device” refers to the device which is pre-defined as a “guest”. An “external device” refers to the device not allowed by the wireless network administrator, and located on the outside of the managed physical domain and/or not connected with network segment to be protected. In some product, the guest and external device are integrated and classified into the neighbor device.



**Figure 1. AP and Device Classification of AirTight**

Current classification mechanism has difficulty to delicate control the wireless access of mobile device to an access point because of its simple classification. And it cannot estimate potential security threats arising from security vulnerability of mobile device itself such as jailbreaking, rooting, misplaced and so on.

In this paper we improve mobile device classification for preventing wireless intrusion. In the proposed algorithm, the mobile devices are classified into one of nine categories. To do this we utilize the security related event of the device from the mobile device management (MDM) and authorization server (AS). The security-related event of the device includes status of device such as authentication, jailbroken, rooted, lost, misplaced, acting AP role (tethering/hot-spot), deletion of MDM agent illegally and so on. Each category can be combined, and the categories are mapped into security level which is defined in this scheme to set-up the security policy for device access control to the authorized access point in the managed network.

Currently, WIPS and MDM are individual products and each is independently deployed and operated. The related research on the WIPS mechanism by utilizing additional device-related events from the MDM has also not yet been investigated.

The contents organized as follows. In Section 2, introduce MDM and WIPS system. And the system architecture and mobile device classification algorithm is provided in Section 3. Finally, conclusion is given in Section 4.

## 2. MDM vs. WIPS

In this section, we compare the WIPS with MDM system. Kwon [5] addressed the architectural and functional difference of WIPS and MDM. Table 1 and 2 compares WIPS and MDM with architectural and functional view respectively [5].

From the architectural point of view, the target object to be managed by WIPS and MDM is different. The WIPS manages wireless network, whereas MDM manages mobile device. The ways to detect and prevent wireless threat are also different. In case of WIPS, the wireless sensors continuously monitor RF (Radio Frequency) signal in the air to detect wireless security threats. When a wireless threat is found, it takes actions such as reverse attack to rogue access point, so that they cannot connect wireless network. The information of detection and prevention of wireless threat is reported to WIPS server in real time. The functions of WIPS server include creation of security/sensor policy, management of white-list, providing dash board and so forth. In case of MDM, MDM agent installed in mobile device detects and prevents the security threats. The prevention function includes remotely lock and

wipe mobile device when lost or misplaced, content access control and so on. Generally, MDM solution includes configure device settings, update device software, enforce security policies, secure mobile access to corporate resources, and so on [6]

From the functional point of view, the wireless threats which can be detected by WIPS and MDM are also different. A WIPS can detect rogue AP, wireless DoS attack, misconfigured AP, mis-association, unauthorized association and so on. In case of MDM, it can detect jailbroken or rooted device, lost or misplaced device and so forth.

**Table 1. Architectural Difference of WIPS and MDM**

	WIPS	MDM
Component	Wireless security management server, Wireless sensor	Mobile device management server, software agent installed on mobile device (MDM agent)
Management Target	Wireless LAN Overall wireless device (including access point and mobile station)	Authorized mobile station (mobile device with MDM agent)
Detection/Prevention method	By wireless sensor system Detection by analyzing the RF (radio frequency) signal Prevention through wireless packet transmission by wireless sensors (e.g., wireless sensor blocks connection to rogue access point by transmitting spoofed disconnection frame such as deauthentication, deassociation and so on)	by MDM agent (e.g., remotely lock and wipe managed device when lost or misplaced)

**Table 2. Functional Difference of WIPS and MDM (P: Provided, N/P: Not Provided)**

Functionality	WIPS	MDM
Detection of Rogue AP	P	N/P
Detection of Wireless DoS	P	N/P
Detection of misconfigured AP connectivity	P	N/P
Detection of mis-association and unauthorized association	P	N/P
Indoor location tracking of mobile devices	P (room-level)	N/P or P (building-level)
Detection of jailbroken or rooted device	N/P	P
Detection of lost or misplaced device	N/P	P
Control wireless interface (HSDPA, Wibro, Wi-Fi, etc.)	N/P	P
Remotely lock on a mobile device	N/P	P
Remote wipe on a mobile device	N/P	P
Application and content access control	N/P	P

Through the cooperation of MDM and WIPS with different capabilities, we can expect more secure management of wireless network. In this paper WIPS utilizes the device related

security event from MDM server to classify the mobile device in order to more delicate access control to the authorized access point.

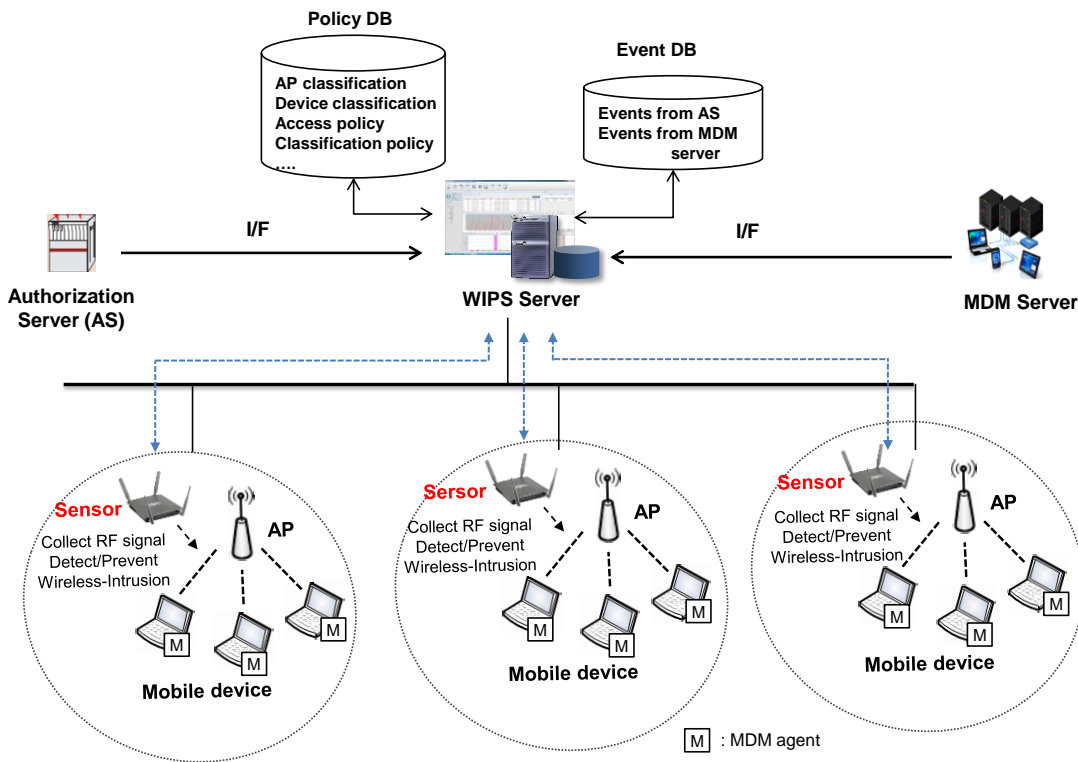
### 3. Mobile Device Classification Scheme

In this section, we present mobile device classification scheme in WIPS system.

#### 3.1. System Architecture

Figure 2 shows the system architecture of the proposed scheme. In Figure 2, WIPS server utilizes the security-related events from the MDM server and authorization server (AS). In this scheme, MDM server informs WIPS of device status information in real time such as jailbreaking/rooting, lost, misplaced, acting AP role (tethering/hot-spot), deletion of MDM agent illegally and so on. The authentication server informs WIPS of the list of authorized device.

The received events are stored in the event database in WIPS server, and WIPS server classifying the mobile device by analyzing the information in the event database, and the classification information is stored in the policy database. The Table 3 shows the list of device-related security event from authorization server and MDM server.



**Figure 2. The System Architecture for Classifying the Mobile Device**

In the proposed algorithm, the mobile devices are classified into one of nine categories and access points are classified into one of five categories. Table 4 shows the classification of mobile device and detailed classification criteria in this mechanism. And Table 5 shows the classification of mobile device and detailed classification criteria in this mechanism.

**Table 3. Device-related Event from Authorization Server (AS) and MDM Server**

Interface	Event
AS → WIPS	List of authorized device
MDM Server → WIPS Server	List of authorized device (i.e., list of device with MDM agent) Jailbroken/rooted device, Lost/misplaced device, Deletion of MDM agent illegally Act as a wireless access point by using wi-fi tethering or hotspot application

**Table 4. The Classification of Mobile Device**

	classification	Classification criteria
1	Authorized device (AS)	Authorized device by the authorization server
2	Authorized device (Manual)	The device classified as 'authorized' by the WIPS server itself manually beforehand
3	Authorized device (MDM)	Authorized device by MDM server (i.e., device with valid MDM agent)
4	Guest device	The device classified as 'guest' by the WIPS server itself manually beforehand
5	Risky device	Jailbroken/rooted or Lost device MDM agent installed in the device is deleted illegally
6	Tethering device	The device act as a wireless access point by using wi-fi tethering or hotspot application
7	External device	The device not allowed by the wireless network administrator, but located on the outside of the managed physical domain (e.g., campus, building) and/or not connected with network segment to be protected.
8	Black-list device	The device listed in the blacklist
9	Uncategorized device	Uncategorized device

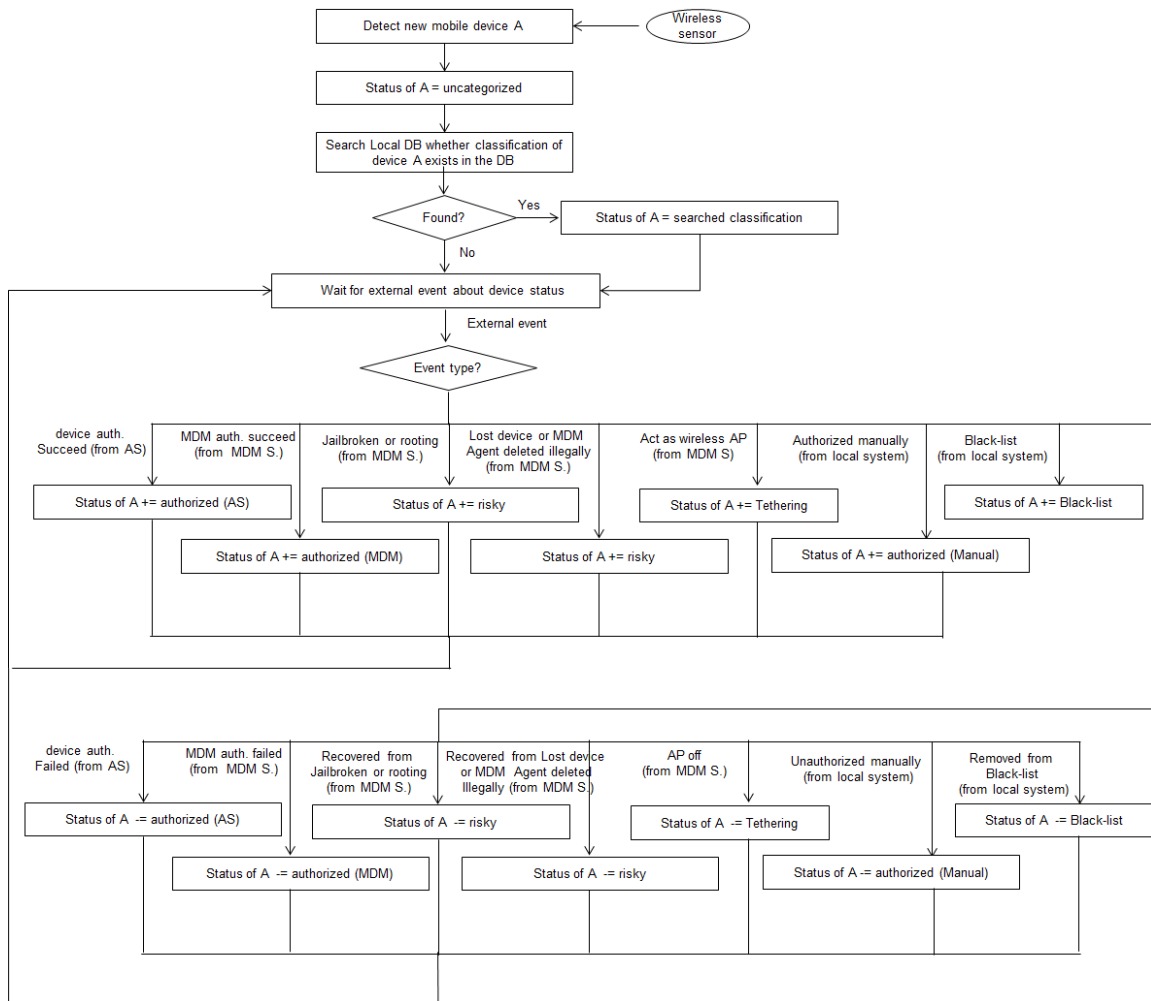
**Table 5. The Classification of Access Point**

	classification	Classification criteria
1	Authorized AP	Authorized access point by the network administrator
2	Rogue AP	The access point that is not authorized by the network administrator, but located on the managed network domain
3	Tethering/Soft AP	Soft access point or the device act as a wireless access point by using wi-fi tethering or hotspot application.
4	External AP	The access point not allowed by the wireless network administrator, but located on the outside of the managed physical domain (e.g., campus, building) and/or not connected with network segment to be protected.
5	Uncategorized AP	Uncategorized access point

The WIPS server classifying the mobile device by analyzing the information of the event database which contains the received device-related information from authorized server and MDM server. This paper mainly focuses on the classification of mobile device. From the nine classifications in Table 4, the classification 'authorized (AS)', 'authorized (MDM)', 'risky' and 'tethering' can only be classified through the interworking with authentication server and/or MDM server.

### 3.2. Classification Algorithm

The device classification algorithm is shown in figure 3. When WIPS detect new device A, the ‘uncategorized’ classification is assigned to the state of the device A. Then WIPS queries the local database whether the classification of device A already exists in the database. If found it, the retrieved classification of A is assigned to the state of A. If not found it, it waits for device-related security event from MDM or authorization server. When the external event is arrived, it changes status of device A based on the received event and the classification algorithm in Figure 3.



**Figure 3. Classification Algorithm**

Each category can be combined, and the categories are mapped into security level which is defined in this scheme to set-up the security policy for device access control to the authorized access point in the managed network. The higher number of security level means the higher security risk.

The follows is an example of security policy. The symbol ‘&’, ‘|’ means ‘and’, ‘or’ respectively.

- *Authorized (MDM) & Risky | Tethering device* → *Security level 2*: A device that is classified as authorized (MDM) and classified as risky or tethering is mapped into security level 2.
- *Authorized (AS)* → *Security level 1*: A device that is authorized by authorization server is mapped into security level 1.

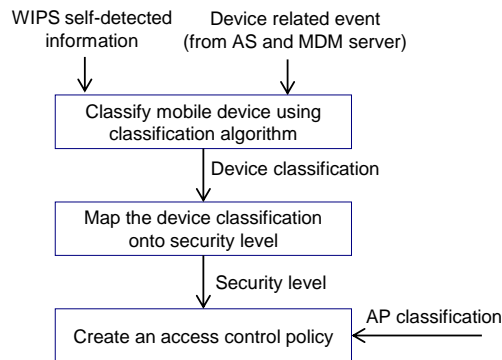
After the completion of the device classification, WIPS decides whether to allow the device connect to the managed wireless network domain by using security policy.

In this paper, we defined four levels of access control

- Permit : *permit* access
- Prohibit : *prohibit* access
- Inform : *inform* network administrator of connectivity information
- Ignore : *ignore* the connectivity

The fundamental step to set up an access control policy is shown in Figure 4. The access control policy in figure 4 is created by network administrator, and it defines access control between security level and AP classification. For example, in Figure 4, the access control policy permit level\_2 devices to access authorized AP and prohibit level\_3 devices to access rogue AP and so on. Figure 5 shows an example of access control policy using the security level and access point classification. This policy is created by network administrator. In Figure 5, the policy permit level\_1 devices to access authorized AP and prohibit level\_2 devices to access rogue AP. In case of level 5 device, the policy permit access to external AP but inform this connectivity information to network administrator.

From this scheme, wireless intrusion prevention system can identify and take countermeasure against potential security threats in advance on a wireless network arising from vulnerable mobile device.



**Figure 4. Set-up an Access Control Policy**

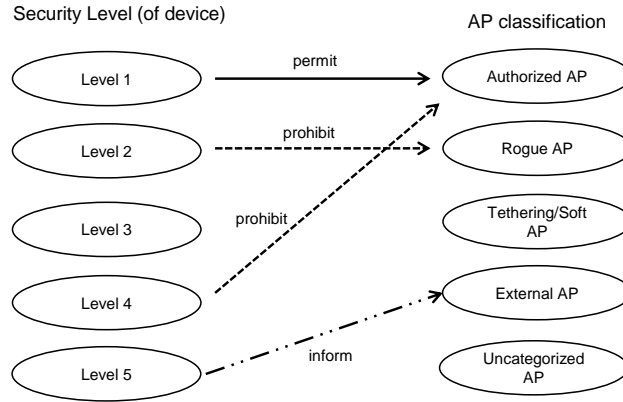


Figure 5. Example of an access control policy

We implement prototype of the proposed scheme. The server window in figure 6 shows the detected device list and its classification and statistics.

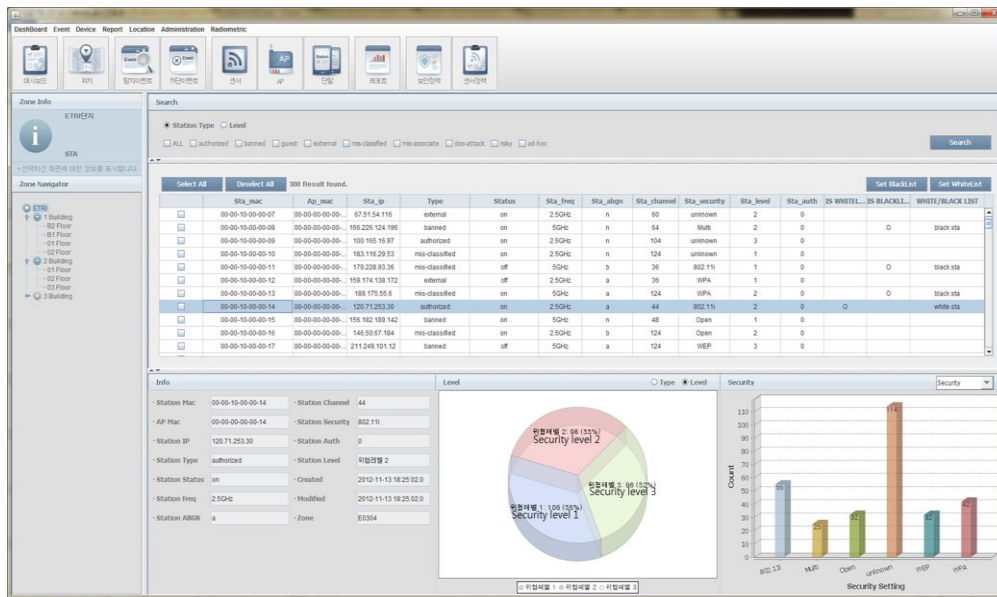


Figure 6. Security Management Server

#### 4. Conclusion

In this paper we improve mobile device classification for preventing wireless intrusion efficiently. In the current WIPS product such as AirTight, Anyclick, AirDefense etc. the mobile devices are classified into one of three or four categories by their classification algorithm. But such classification mechanism has difficulty to delicate control the wireless access of mobile device to an access point because of its simple classification. And it cannot estimate potential security threats arising from security vulnerability of mobile device itself.

In the proposed algorithm, the mobile devices are classified into nine categories. To do this we utilize the security related event of the device from the mobile device management (MDM) and authorization system (AS). To make security policy for preventing wireless intrusion the following steps are also presented: First step, classify mobile device using classification algorithm. Second step, Maps the device classification into security level. Third step, Create an access control policy using the security level and access point classification.

The advantage of this approach is to identify and take countermeasure against potential security threats in advance on a wireless network arising from vulnerable mobile device. Such security threats arising from the vulnerable device can include jailbroken, rooted, lost, misplaced, mis-configured device and so on. The proposed scheme can be applied to wireless intrusion prevention system, smart work, BYOD (Bring Your Own Device) service and so on. Currently, we are refining and extending the classification algorithm to consider additional analysis of device activity and so on.

## Acknowledgements

This research funded by the MISP (Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013

## References

- [1] AirTight, "Method and system for monitoring a selected region of an airspace associated with local area networks of computer devices", U.S. Patent 7,002,943 (2006).
- [2] R. Beyah and A. Venkataramen, "Rogue-Access-Point Detection—Challenges, Solutions, and Future Directions", IEEE Security & Privacy, vol. 9, no. 5, (2011), pp. 56-61.
- [3] T. S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces, Elsevier, vol. 28, no. 6, (2006), pp. 670-694.
- [4] Anyclick AIR, <http://unet.kr/>, UNETsystem.
- [5] H. Kwon and S. Kim, "Efficient mobile device management scheme using security events from wireless intrusion prevention system", 7th Int'l Conf. on Ubiquitous Information TEchnologies & Applications (CUTE), Hong Kong, China, (2012), December 20-22.
- [6] "Enterprise Mobile Device Management", <http://www.air-watch.com/solutions/mobile-device-management>, airwatch, (2012).
- [7] M. S. Islam and S. A. Rahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology, vol. 36, (2011), pp. 1-8.
- [8] B. Park, "Techniques and Practices for Securing Wireless Networks", International Journal of Advanced Science and Technology, vol. 48, (2012), pp. 133-138.
- [9] AirDefense services platform, [http://www.motorolasolutions.com/US-EN/Services/Run/Network+Infrastructure+Management/IT/AirDefense\\_Services\\_Platform](http://www.motorolasolutions.com/US-EN/Services/Run/Network+Infrastructure+Management/IT/AirDefense_Services_Platform), Motorola.
- [10] K. Rhee, H. Kim and H. Na, "Security Test Methodology for an Agent of a Mobile Device", International Journal of Security and Its Applications, vol. 6, no. 2, (2012), pp. 137-142.

## Authors



**Hyeokchan Kwon**, received PhD degree in computer science from Chungnam National University in 2001. Since 2001, he is currently a principal researcher in electronics and telecommunications research institute (ETRI) in Korea. His research interests include wireless intrusion prevention system, WLAN security and digital content protection.



**Sin-Hyo Kim**, Sin-Hyo Kim received her M.S. degree in computer science from Chungnam National University in 2000. Since 1990, she is currently a principal researcher in electronics and telecommunications research institute (ETRI) in Korea. Her current research interests are in the areas of wireless LAN security, cyber security and privacy.