AP

*,   *,   **
*
**
e-mail : beomjinpark@hanmail.net, taekklee@ajou.ac.kr, mphong@ajou.ac.kr

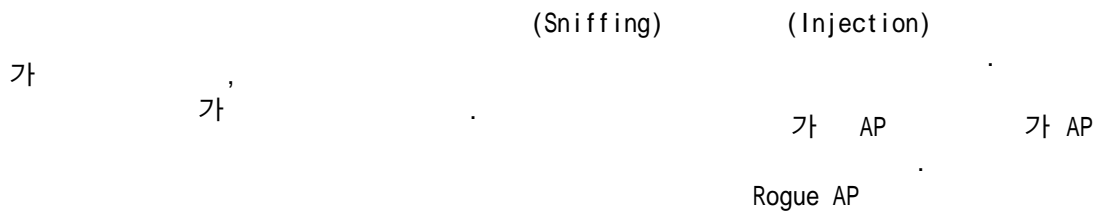# An Unauthorized AP Detection Approach Based on Internal Network Information in Wireless LAN

Beomjin Park*, Taekkyeun Lee*, Manpyo Hong**
*Dept. of Knowledge Information, Ajou University
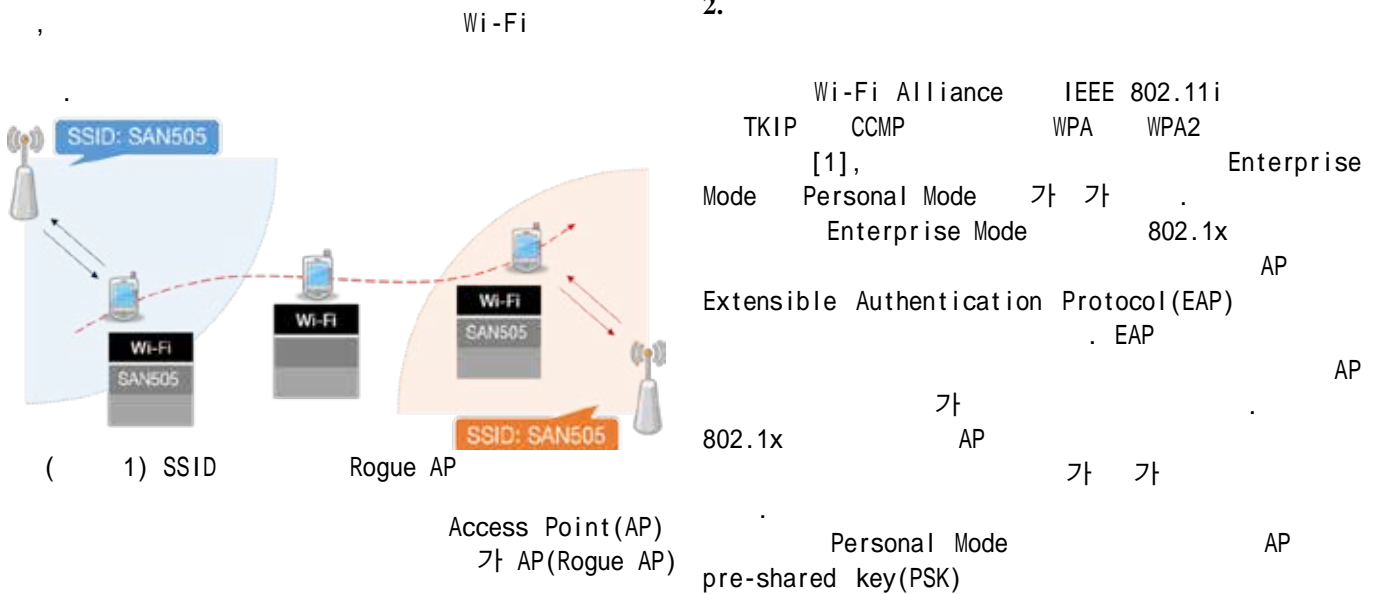**Graduate School of Information and Communication, Ajou University

AP   AP
.
.   AP
AP   .

1.

(Sniffing)   (Injection)
.
,
.   AP   AP
.
Rogue AP
.

.

,   W-Fi

.

(1) SSID   Rogue AP

Access Point(AP)
AP(Rogue AP)

2.

W-Fi Alliance   IEEE 802.11i
TKIP   CCMP   WPA   WPA2
[1],   Enterprise
Mode   Personal Mode   .
Enterprise Mode   802.1x
AP
Extensible Authentication Protocol(EAP)
. EAP
AP
.
802.1x   AP
.
Personal Mode   AP
pre-shared key(PSK)

AP

AP
AP   beacon
         . beacon
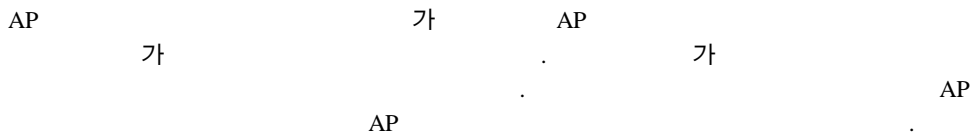
    rogue AP
       .

	WPA	WPA2
Enterprise Mode	IEEE 802.1x/EAP	IEEE 802.1x/EAP
Personal Mode	PSK	PSK

<   1> WPA   WPA2   [2]

3.

       ,
                                    .
Personal Mode
       AP
                              .
                    Personal Mode
         ,   AP
                     . AP
      IP
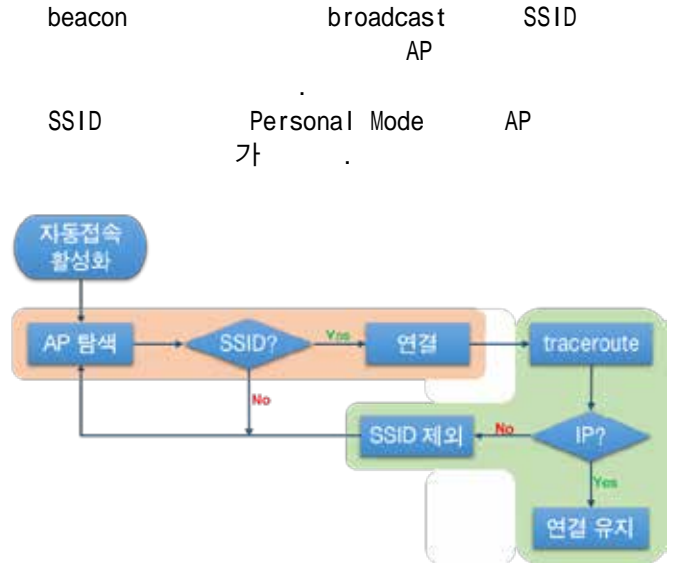   .
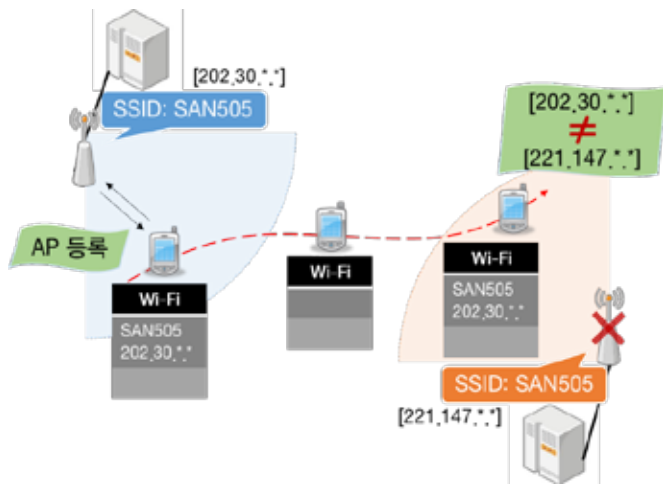
(2) IP   AP

  AP   IP
  Traceroute
       AP   .
     AP   1   2
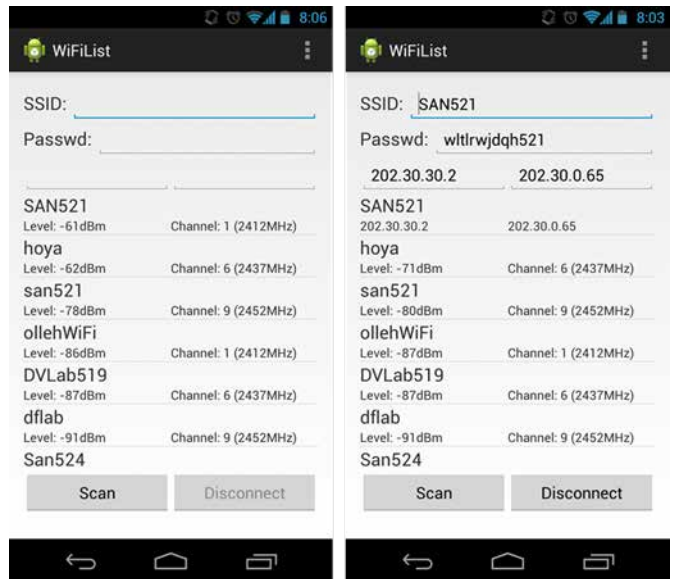   IP   ,   SSID
       IP
                   .   IP

beacon   broadcast   SSID
                              AP
                                      .
    SSID   Personal Mode   AP
                                    .

(3)

          3

              IP   .
  IP   ping   Time To Live(TTL)
                    URL
           .
       AP   SSID   IP
              SSID   , SSID
                                    IP
                                              AP
                                              .

4.

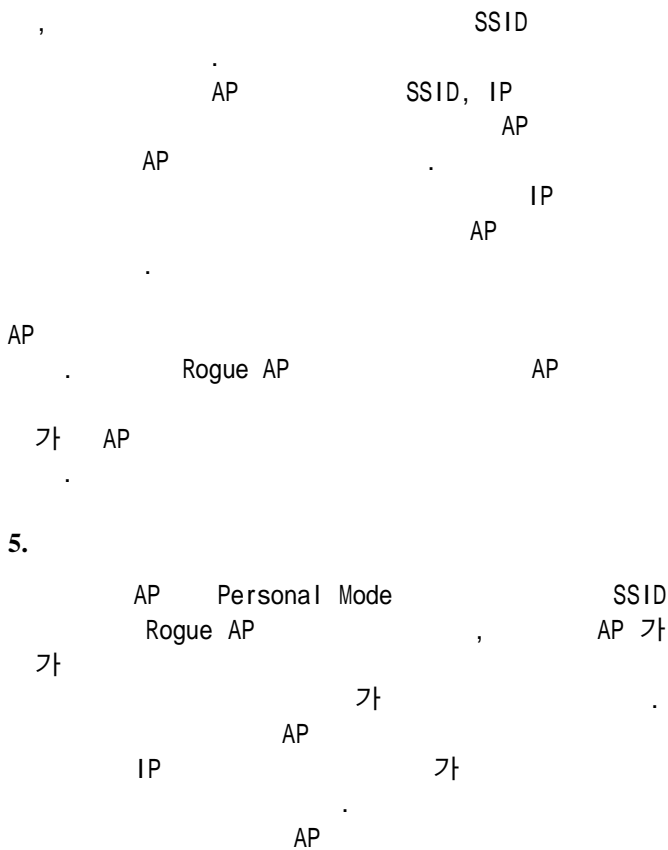Android 4.2.2
Galaxy Nexus   .

(4)

       AP   Wi-Fi Alliance   802.1x

,   SSID
                        .

            AP   SSID, IP
                                         AP

        AP   .
                                    IP
                            AP

        .

AP
        .   Rogue AP   AP

        AP
        .

5.

            AP   Personal Mode   SSID
        Rogue AP   ,   AP

                                            .
                    AP
        IP
                            .
                AP
        .

[1]   . "Wi-Fi CERTIFIED™   ".
    TTA   .
[2] Wi-Fi Alliance. "Deploying Wi-Fi Protected
    Access(WPA™) and WPA2™ in the Enterprise". March
    2005.
[3] 802.11i. "IEEE Standard for Information Technology-
    Telecommunications and Information Exchange Between
    Systems- Local and Metropolitan Area Networks-
    Specific Requirements Part 11: Wireless LAN Medium
    Access Control (MAC) and Physical Layer (PHY)
    Specifications Amendment 6: Medium Access Control
    (MAC) Security Enhancements". 23 July 2004.
[4] 802.11. "IEEE Standard for Information technology-
    Telecommunications and information exchange between
    systems Local and metropolitan area networks--Specific
    requirements Part 11: Wireless LAN Medium Access
    Control (MAC) and Physical Layer (PHY)
    Specifications". 12 June 2007.
[5]   . "IP   MAC
              ".   . 2013.
[6] ETRI. "   ". 2013.
[7] Songrit Srilasak. "Integrated Wireless Rogue Access
    Point Detection and Counterattack System". ThaiCERT.
    2008.
[8] Wi-Fi Alliance. "The State of Wi-Fi® Security Wi-Fi
    CERTIFIED™ WPA2TM Delivers Advanced Security to
    Homes, Enterprises and Mobile Devices". January 2012.