This is how I installed the kismet_drone on the wrt54g (v2.2) while running the kismet_server and kismet_client on a Linux box. (I was using version 2005.06.R1 of kismet.)

Contents

Preparing the wrt54g

Installing the drone

First, I installed the seavsoft firmware (Firmware_Alchemy-6.0rc6.bin) on the wrt54g v2.2 (I assume it will also work with the dd-wrt firmware).

I then using the web interface, set it up to use a static ip address, disabled the dhcp server and also enabled telnet access to the wrt. (You may prefer to leave the dhcp server running if you do not have ahother dhcp server on your network). I also turned off the firewall.

On the Linux desktop machine at a console, type

```
telnet <address of wrt>
```

Log in using user name 'root' and the same password as the one for the wrt's web interface (the default is 'admin').

Then at another terminal, download the MIPS binaries for the wrt. Download them from the kismet website http://www.kismetwireless.net/download.shtml . I used version 2005-06-R1a which was the latest version.

cd into the directory where you downloaded it to and unzip it.

```
tar -zxvf kismet-2005-06-R1a-wrt54.tar.gz
```

As I have a local web-server running on my desktop box, I decided to use it and wget to copy the kismet files over to the wrt. So I then copied the kismet_drone and conf/kismet_drone.conf files to the root of my web-server.

Go back to your other terminal with the telnet session to the wrt.

The /tmp directory is the only place on the wrt which is writable as it is stored on a ramdisk. This means that every time that you power down the wrt, you have to reload the kismet files to it.

```
cd /tmp
```

Get files onto wrt

```
wget http://<ip address of desktop box>/kismet_drone
wget http://<ip address of desktop box>/kismet_drone.conf
```

Put kismet_drone.conf file in /tmp/etc directory.

```
mv kismet_drone.conf /tmp/etc
```

and make drone executable

```
chmod  x /tmp/kismet_drone
```

(You could probably also use scp to load the files to the wrt instead of wget/web-server.)

Configure drone

You then need to edit the drones conf file (I used the vi editor).

```
vi /tmp/etc/kismet_drone.conf
```

Change the line

```
allowedhosts=127.0.0.1
```

to

```
allowedhosts=<address of desktop box>
```

and the line

```
source=wrt54g,eth2,Kismet-Drone
```

to

```
source=wrt54g,prism0,Kismet-Drone
```

(I have read that this line should be different if running another version of the hardware - this works with v2.2 of the wrt54g).

Running the drone

Now we start the drone...but first, we need to put the wireless interface into passive monitoring mode.

```
wl ap 0            #switch off access point mode
wl disassoc
wl passive 1
wl promisc 1
```

The driver for the wrt doesn't do channel hopping, so it needs to be done with a small script running on the wrt.

See channel hopping on kismet drone.

Then run the drone.

```
/tmp/kismet_drone
```

If this works, it will display some messages ending with 'Allowing connections from <desktop ip address>'. You will need to keep the telnet session open, as closing it will terminate the drone.

Preparing the desktop

Install server and drone

You will need to be logged in as root. As I use a debian based Linux distro, I started by using apt to install kismet.

```
apt-get install kismet
```

Unfortunately for me, the version of kismet available using apt was not the same as the version as the drone and the drone was unable to talk to the server as the protocols had changed between the two versions of kismet. The versions (probably) need to be the same. In the end, I installed kismet on my desktop from source from the kismet site (http://www.kismetwireless.net/download.shtml).

```
cd <download directory>
tar -zxvf <kismet source file>tar.gz
cd <kismet dir>
./configure
make
make install
```

Configure kismet

[note: I found that the config files were in /etc/kismet when installing using apt-get, but they were in /usr/local/etc when installing from source.] First, you need to make a kismet user for the server to run as.

```
adduser kismet
```

...and fill in the blanks. Then you need to edit the /usr/local/etc/kismet.conf file and change

```
suiduser=your_user_here
```

to

```
suiduser=kismet
```

Set the wireless source by changing

```
source=none,none,addme
```

to

```
source=kismet_drone,<wrt ip address>:3501,wrt54g
```

I found that kismet couldn't write its log files to the default directory, so changed the line

```
logtemplate=%n-%d-%i.%l
```

to

```
logtemplate=%h/%n-%d-%i.%l
```

so that the log files get saved in the kismet users directory (/home/kismet).

Run kismet server and client

Now everything should be ready. First you will need to run the server in the background. (I assume that you still have the kismet_drone running via a telnet session to the wrt (see the 'running the drone' section above.)) then run the GUI client.

```
/usr/local/bin/kismet_server
```