Adaptive Frequency Hopping Scheme for Wireless Distribution System (WDS) in WLAN

Jutamas Kongtep

Abstract—**This paper presents an adaptive frequency hopping scheme for Wireless Distribution System (WDS) in WLAN with IEEE 802.11g. At least two access points are interconnected to form a WDS to automatically adapt channel by time under synchronization between Master and Slave equipments. This result in a signal's lingering at a predefined frequency for a short period of time in each channel because of dramatically change to specified channel all the time that protects noise with neighbor channels and avoids intruders which resolves a problem in general form of WDS is vulnerable considering the attacks or interferences due to perpetually use the same frequency channel. Moreover, presents highly secured WPA2 authentication with AES encryption, all above solutions to enhance security level of WLAN in WDS mode.**

Index Terms—**Adaptive Frequency Hopping Scheme, Wireless Distribution System, WDS, WPA2, AES.**

I. Introduction

Owing to the advanced technology of WLAN system and the characteristics that provide to comfortable users so WLAN has been admired, security need to be concerned to improve the secured and proper pattern also. Frequency Hopping Spread Spectrum (FHSS) is a method of transmitting radio signal by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. Adaptive Frequency Hopping Spread Spectrum (As used in Bluetooth) improves resistance to radio frequency interference by avoiding using crowded frequencies in the hopping sequence such as the GSM cellular system uses frequency hopping as a form of frequency interleaving in view to avoid that two phone calls in adjacent cells constantly interfere with each other. A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. The notable advantage of WDS over other solutions is it preserves the MAC addresses of client frames across links between access points. Apple technologies, if the AirPort Extreme is your "main" wireless router, each AirPort Express that is setup to "extend" communicates directly to the AirPort Extreme.

II. Wireless Distribution System (WDS) and Frequency Hopping Scheme

Wireless Distribution System (WDS) is the simple access point characteristic that can be connected together and repeat signal to provide WLAN signal area more. WDS gets performance much more than Repeater Mode about speed and signal level.

A. *WDS is Vulnerable Considering the Attack/interference Due to the Same Frequency Channel*

WDS gets risk of attack or noise because of same frequency usage all of time. Fig. 1, show the transmitted hopped frequencies are generated by a digital frequency synthesizer, which is controlled by serial or parallel "words", each containing *m* binary digits. These *m*-bit words produce one of $M = 2^m$ frequencies for each separate word or symbol combination of the digits. The number of radio frequencies available for a frequency hopper is frequently $M = 2^m$ where m=2, 3….. although not all of these are necessarily used in a particular application. The instantaneous change of transmitted discrete RF frequencies is attained at the chip rate f_c, the baseband data rate is f_b (kb/s). Frequency hopping spread spectrum systems are categorized into Slow Frequency Hopping (SFH) and Fast Frequency Hopping.

Slow Frequency Hopping (SFH), in an SFH spread system the hop rate f_H (chip rate) is less than the baseband message bit rate f_b. Thus two or more (in several implementations, more than 1000) baseband bits are transmitted at the same frequency before hopping to the next RF frequency. The hop duration, T_H, is related to the bit duration T_b by

$$T_H = kT_b \text{ for } k = 1,2,3\ldots\ldots \text{ and } f_c = f_H = 1/T_H \quad (1)$$

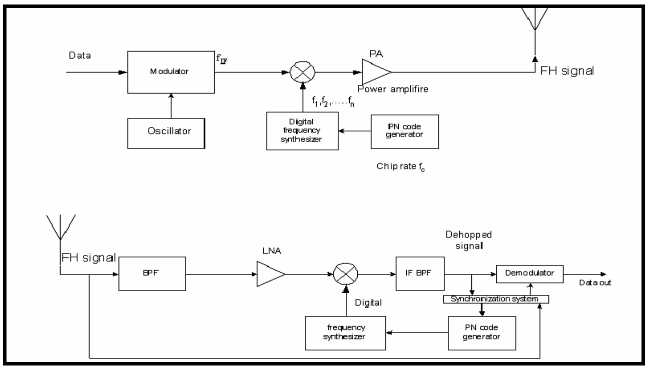


Fig. 1. Block diagram of frequency hopping system

Fast Frequency Hopping (FFH), in an FFH spread spectrum system the frequency chipping rate, f_c, (Chipping

Manuscript received July 16, 2012; revised August 26, 2012.

J. Kongtep is with Computer Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand (e-mail: jutamas.kongtep@gmail.com).

rate is the same as hopping rate) is greater than the baseband data rate f_b. In this case one message bit T_b is transmitted by two or more frequency hopped RF signals. The hop duration or chip duration ($T_H = T_c$), is defined by

$$T_c = T_H = \frac{1}{k} T_b \text{ for } k = 1, 2, 3\ldots\ldots \text{ and } f_c = f_H = 1/T_c \qquad (2)$$

B. The Advantage and Disadvantage of Frequency Hopping

1) The advantage

- Robust technology with little influence from noises, reflections, other radio stations or other environment factors. The number of simultaneously active systems in the same geographic area (Collocated systems) is significantly higher than the equivalent number for DSSS systems.
- Is a technology the one to be selected for installations designed to cover big areas where a big number of collocated systems are required, typical applications for FHSS include cellular deployments for fixed Broadband Wireless Access, where the use of DSSS is virtually impossible because of its limitations.
- Low power density, the effect of the low power density of the transmitted signal is that such a signal will not disturb (Interfere with) the activity of other systems' receivers in the same area and that such a signal can not be detected by intruders, providing a high level of intrinsic security.
- Work with narrow band signal, a narrow band interference signal present on a specific frequency will block only one specific. The frequencies to be used in the hopping sequence, to "tune in", a listener should know the number of frequencies selected in the system, the actual frequencies, the hopping sequence, as well as the dwell time to avoid intruders.

2) The disadvantage

- Providing lower capacities than DSSS.
  Resolve: Enhance overall aggregate rate or throughput by reduce the effects of environment factors as base of FHSS characteristics, FHSS is a very robust technology with little influence from environment factors.
- For the eavesdroppers, the hop sequence could actually be determined, there are a limited number of hop sequences, the hop sequence can be uniquely identified by determining the beacon timing.
  Resolve : Rely on encryption and authentication procedures to ensure network security.

C. Adaptive Frequency Hopping Scheme for WDS is Vulnerable Considering the ATTACk/interference Due to Work better as Get Rid of Authentication

WDS should get rid of authentication to work better but risk of attack so authentication method and encryption need to consider. WPA2 (Wi-Fi Protected Access 2) has replaced WPA, requires testing and certification by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with robust, WPA2 uses AES for encryption, it is stronger than the RC4 encryption scheme shared by WEP and WPA. AES aka the Rijndael algorithm is a secure, fast symmetric cipher that is easily implemented in hardware, AES has its own mechanism for dynamic key generation. It's also resistant to statistical analysis of the cipher text and counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits, AES operates on a 4×4 array of bytes, termed the state (Versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

D. Ideas / Concepts

- Concept1: Use Frequency Hopping Scheme by automatically change frequency range or channel on both routers on Wireless Distribution System for WLAN to extend signal distance. Owing to avoid signal or data detection of intruder because of WLAN connection will keep in one channel for a moment then automatically change to the other channels put in order to synchronize only between authorized Master and Slave machines so unauthorized person can not detect signal or has not enough time to decode in limited time period. (Delay time of each channel)
- Concept2: Besides security of Frequency Hopping Scheme, this research uses WPA2 authentication with complex AES encryption also to enhance security level even if WDS mode normally good at performance when get rid of encryption or unsophisticated coding (Risk of security). All above, this research is verified to use all security techniques like formerly mention in WDS mode.

III. Methods

A. Configure and Setup Network Connection between Linksys WRT54GL Routers in WDS Mode

- Upgrade firmware to DD-WRT V24 SP2 (To establish WDS mode), 14 channels : channel 1-14.
- Create WDS connection, 1'st as Master and 2'nd as Slave. The routers are synchronized with each other.
- Specify Wireless Mode, Network Configuration, SSID, IEEE802.11, authentication with WPA2 and encryption with AES on 2 routers at the same time. Because of WDS mode uses the same frequency of 2 routers all the time that gets risk of hacker to use several time to attack network so uses frequency hopping to adapt frequency by time.
- Modify DD-WRT V24 SP2 firmware to automatically adaptive frequency channel on frequency hopping

scheme (Avoid attack), if Master router changes frequency channel, Slave router will change frequency channel too.

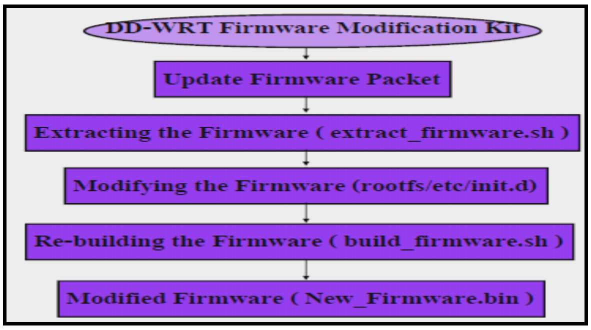
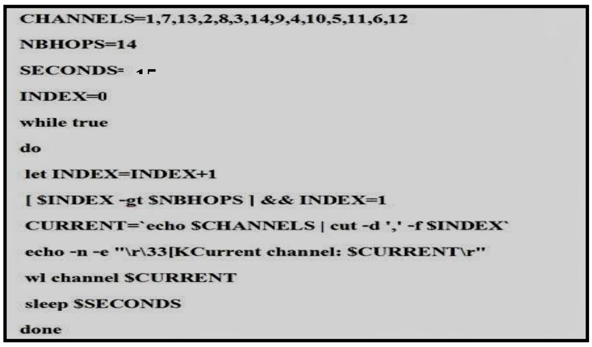

DD-WRT Firmware Modification Kit
Update Firmware Packet
Extracting the Firmware (extract_firmware.sh)
Modifying the Firmware (rootfs/etc/init.d)
Re-building the Firmware (build_firmware.sh)
Modified Firmware (New_Firmware.bin)

Fig. 2. Router firmware modification flow chart

Fig. 2 shows firmware modification of routers : download DD-WRT V24 SP2 for Linksys WRT54GL, extracts file on Ubuntu. Then modify DD-WRT V24 SP2 firmware by adaptive frequency hopping scheme to automatically change frequency range or channel to avoid signal detection. (Modify source code in rootfs/etc/init.d) and rebuild firmware package, upgrade to both routers. Use “Startup Command Line” to control and link with modified firmware for flexible usage propose, show in Fig. 4.



```
CHANNELS=1,7,13,2,8,3,14,9,4,10,5,11,6,12
NBHOPS=14
SECONDS= 15
INDEX=0
while true
do
 let INDEX=INDEX+1
 [ $INDEX -gt $NBHOPS ] && INDEX=1
 CURRENT=`echo $CHANNELS | cut -d ',' -f $INDEX`
 echo -n -e "\r\33[KCurrent channel: $CURRENT\r"
 wl channel $CURRENT
 sleep $SECONDS
done
```

Fig. 3. Pseudo code of adaptive frequency hopping scheme to automatically change frequency range or channel to avoid signal detection

Fig. 3 the total channel 14 channels (Channel 1 to 14), the step of hop sequence separates oneself from others at least 3 channel like this : Channel 1, 7, 13, 2, 8, 3, 14, 9, 4, 10, 5, 11, 6 and 2 with cycle to protect noise from adjacent channel. Specify delay time = 15 seconds.

Initial index = 0, then steps up to 1 in each cycle. Index =1, shows about the first specify channel (From 14 channels) and then change to that channel. Keeps in channel for a while with delay time before change to other channels.

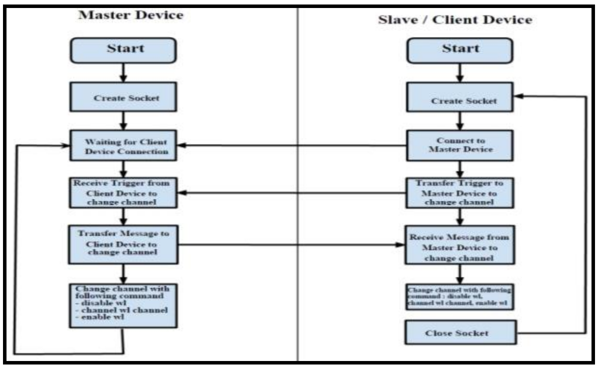
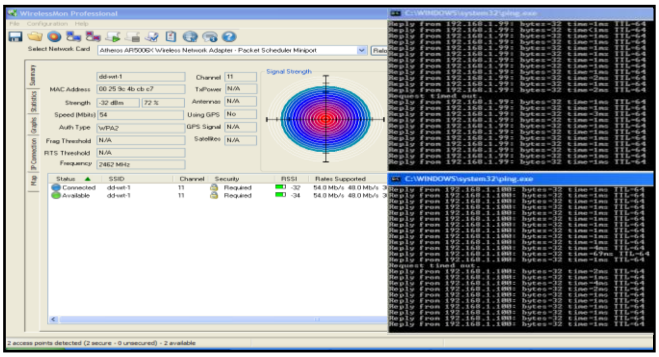

Master Device
Slave / Client Device
Start
Create Socket
Waiting for Client Device Connection
Receive Trigger from Client Device to change channel
Transfer Message to Client Device to change channel
Change channel with following command
- disable wl
- channel wl channel
- enable wl
Start
Create Socket
Connect to Master Device
Transfer Trigger to Master Device to change channel
Receive Message from Master Device to change channel
Change channel with following command : disable wl, channel wl channel, enable wl
Close Socket

Fig. 4. Master and slave router synchronization flow chart

Fig. 4 shows about router synchronization, create socket on both Master and Slave Router then Master waits for Slave connection until link is established. After that, Slave sends trigger to Master then Master receives trigger to change channel. Master sends message to Slave and then slave receives message to change channel. Step of adaptive frequency range or channel : disable wl, channel wl channel and enable wl respectively. After change to the same channel of both routers then take delay time about 15 seconds before the new connection is established, Slave will close socket and take delay time until create socket again.

B. Experiment

Test WDS connection of modified routers in automatically adaptive frequency channel with WPA2 authentication and AES encryption. (Master router IP : 192.168.1.99 and Slave router IP : 192.168.1.100)



Atheros AR5006X Wireless Network Adapter - Packet Scheduler Miniport

	dd-wrt-1	Channel	11
MAC Address	00 25 9c 4b cb c7	TxPower	N/A
Strength	-32 dBm 72 %	Antennas	N/A
Speed (Mbits)	54	Using GPS	No
Auth Type	WPA2	GPS Signal	N/A
Frag Threshold	N/A	Satellites	N/A
RTS Threshold	N/A		
Frequency	2462 MHz		

Status	SSID	Channel	Security	RSSI	Rates Supported
Connected	dd-wrt-1	11	Required	-32	54.0 Mb/s 48.0 Mb/s 3
Available	dd-wrt-1	11	Required	-34	54.0 Mb/s 48.0 Mb/s 3

2 access points detected (2 secure - 0 unsecured) - 2 available

C:\WINDOWS\system32\ping.exe

```
Reply from 192.168.1.99: bytes=32 time<1ms TTL=64
Reply from 192.168.1.99: bytes=32 time<1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=2ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=2ms TTL=64
Request timed out.
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=3ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
Reply from 192.168.1.99: bytes=32 time=1ms TTL=64
```

C:\WINDOWS\system32\ping.exe

```
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=4ms TTL=64
Reply from 192.168.1.100: bytes=32 time=69ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Request timed out.
Reply from 192.168.1.100: bytes=32 time=2ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=4ms TTL=64
Reply from 192.168.1.100: bytes=32 time=2ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
Reply from 192.168.1.100: bytes=32 time=1ms TTL=64
```

Fig. 5. Show master and slave router connection with “Ping” Test on WDS mode go to channel-11

Fig. 5 shows Time-to-live (TTL) that tells the packet has been in the network too long and should be discarded, TTL shows network or router that is hopped, Linksys WRT54GL routers are small equipments with LINUX base and when use WDS mode then 2 routers become 1 network so TTL = 64 – 0 = 64. Round-trip time (RTT) is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received. In this situation (Fig. 5.), test connection between router and client that consists of 24 packages : Minimum = 0 ms because of some packages can not be transmissible for a moment that occurs in joint of adaptive frequency hopping and then new channel is established so the packages can be transferable in normal mode. Approximate RTT on Master Router : Minimum = 0 ms, Maximum = 3 ms, Average = (All time points / 24) = 1.125 ms, approximate RTT on Slave Router : Minimum = 0 ms, Maximum = 69 ms, Average = (All time points / 24) = 4.125 ms. The unsuccessful transmissions that are shown “Request time out” during changed frequency channel period on, after that can recover connection in few seconds to synchronize between routers and can be used in normal mode. (Prompt to transfer signal in normal mode)

IV. Conclusion

This paper presents an adaptive frequency hopping scheme for Wireless Distribution System (WDS) in WLAN to enhance security level of 2 routers on WDS mode with experimental method. To adapt frequency by time under synchronization between Master and Slave equipments. And because of spectrum random, frequency always adapts that protects noise with neighbor channels. For authentication, presents highly secured WPA2 authentication with AES encryption, all above solutions to up security level of WLAN in WDS mode.

ACKNOWLEDGEMENT

First and foremost I offer my sincerest gratitude to my advisor, Assoc. Prof. Dr. Surin Kittitornkun who has supported me thoughout my paper with his kindness. I attribute the level of my Masters degree to his encouragement and effort. The Department of Computer Engineering, King Mongkut's Institute of Technology Ladkrabang has provided the support and equipments I have needed to produce and complete my papers. Finally, I thank my parents for supporting me throughout all my studies at University and comfort me to complete my writing up.

REFERENCES

[1] *Part 15.2: Coexistence of Wireless Personal Area Networks with other Wireless Devices Operating in Unlicensed Frequency Bands*. ANSI/IEEE Standard 802.15.2-2003.

[2] P. Popovski, H. Yomo, and R. Prasad, "Strategies for Adaptive Frequency Hopping in the Unlicensed Bands," *IEEE Wireless Communications*, vol. 13, no. 6, December 2006.

[3] A. C.-C. Hsu, D. S. L. Wei, C.-C. J. Kuo, N. Shiratori, and C-Ju Chang, "Enhanced Adaptive Frequency Hopping for Wireless Personal Area Networks in a Coexistence Environment," in *Proceeding of Global Telecommunications Conference (GLOBECOM)*, 2007.

[4] L. Stabellini, L. Shi, A. A. Rifai, J. Espino, and V. Magoula, "A New Probabilistic Approach for Adaptive Frequency Hopping," in *Proceedings of International Symposium on Personal Indor and Mobile Radio Communications*, PIMRC, 2009.