

# 訊息在傳輸上的安全機制實作

李昀昱、戴江淮

E-mail: 9806191@mail.dyu.edu.tw

## 摘要

由於資訊科技越來越發達，越來越多的資料都是用無線通訊來傳輸。例如:Wi-Fi、Zigbee、藍芽等。在傳送過程中，資料很容易被駭客竊取，所以訊息傳送的安全變的極為重要。在本文中，以軟體VB(Visual Basic)語法來撰寫程式，做出有視覺介面的平台，並且搭配赫立訊科技Zigbee儀器(IP-Link 2220H)來做測試。利用RS-232傳輸線把電腦與Zigbee儀器(IP-Link 2220H)連接。從電腦發送訊息或是指令，藉由Zigbee儀器(IP-Link 2220H)傳送到別台的Zigbee儀器(IP-Link 2220H)。在傳送時，有兩個很重要資訊容易被竊取。一個是路徑，另一個是訊息。因此，把真正的路徑和訊息都用雜湊演算法加以加密的話。這樣可以防止被有心人竊取資訊，讓資料在傳送上更加安全。

關鍵詞：Wi-Fi、ZigBee、雜湊演算法

## 目錄

封面內頁	
簽名頁	
授權書	iii
中文摘要	iv
英文摘要	v
誌謝	vi
目錄	vii
圖目錄	ix
表目錄	xi
第一章 緒論	1
1.1 研究背景	1
1.2 研究目的	2
1.3 研究方法	3
1.4 章節結構	4
第二章 文獻回顧	5
2.1 現代密碼學	6
2.1.1 RC4演算法	7
2.1.2 數據保密標準(DES)	10
2.1.3 雜湊演算法	11
2.2 訊息認證	13
2.2.1 對稱性加密	14
2.2.2 訊息認證碼	15
2.2.3 雜湊函數	17
第三章 ZigBee儀器格式	20
3.1 IP-link2220(2220H)模組簡介	20
3.1.1 網路架構	21
3.2 IP-link2220(2220H)傳輸模式	21
3.2.1 二進位模式	21
3.2.2 透明廣播模式	22
3.2.3 透明點對點模式	22
3.3 赫立訊通用訊框格式	23
3.3.1 赫立訊指令請求訊框	24
3.3.2 赫立訊指令回覆訊框	26

3.3.3 赫立訊資料請求訊框 . . . . .	27
3.3.4 赫立訊資料確認訊框 . . . . .	28
3.4 指令格式 . . . . .	29
第四章 訊息傳輸實作 . . . . .	32
4.1 操作界面簡介 . . . . .	32
4.2 訊息傳輸過程與結果(一) . . . . .	33
4.3 訊息傳輸過程與結果之改良版(二) . . . . .	40
第五章 結論與未來展望 . . . . .	45
參考文獻 . . . . .	46
附錄A . . . . .	47

## 參考文獻

- [1]戴江淮編著，網路安全，全威股份有限公司2007/08[2]戴江淮編著，RFID工程概論，學貫行銷股份有限公司2008/05[3]戴江淮編著，行動路由技術，博碩文化股份有限公司 2005/02。
- [4]蔣挺、趙成林編著，紫蜂技術及其應用，北京郵電學院出版社June 2006。
- [5]鄭安文編著，密碼學-加密演算法，全華科技圖書股份有限公司93/03[6] 大葉大學電信工程學系碩士班-李國鳴，Zigbee訊息傳輸實作與探討。
- [7]大葉大學電信工程學系碩士班-陳秀玲，Zigbee家電控制。
- [8]武偉亭，Helicomm IP-Link2220(2220H) ZigBeeTM M2M Terminal用戶手冊，July, 2007.
- [9]王國榮編著，Visual Basic 6.0 入門、實務與資料庫。
- [10] 彭明柳編著，Visual Basic 6 中文專業版徹底研究。
- [11] Helicomm, IP-Link 122X Embedded Wireless Module User Manual Version 2.1.00, June, 2007.
- [12] ZigBee Alliance. The ZigBee specification Version V1.2. January 17, 2008.
- [13] <http://home.educities.edu.tw/vbtester/indexw1024.htm> 阿戊的VB實驗網頁[14] <http://user.infor.org/~tmt514/vb/> VB講義