Contents

Abstract (in Chinese) i

Abstract (in English) ii

Acknowledgements iii

Contents iv

List of Tables vi

List of Figures vii

1. Introduction 1

2. Related Works 6

2.1 IEEE 802.1x Architecture………..…………..………………………….. 6

2.2 IEEE 802.1x Authentication……...…..………..………………………... 8

2.3 IEEE 802.1x Key Management……………………………………... 11

2.4 EAP-TLS Authentication Protocol……….………………………. 12

2.4 IEEE 802.11i Overview……….…………………………………….. 15

3. Proposed Key Management Method 17

3.1 Designed Issues……….…………….….………………………………… 17

3.1.1 Design Goals…………………….……………………………… 18

3.1.2 Key-Mapping Table…..…………………………………………… 19

3.1.3 Clock Synchronization………………………………………….. 19

3.1.4 Hash Function…..………………………………………………….20

3.1.5 The Challenge Text Of Authentication ……………………… 21

3.2 Authentication Management……………..…….…………………………….. 22

3.2.1 The Operation Of Proposed Authentication.…………………. 25

3.3 Periodic Key Updated..………………..……………….…………………… 27

3.3.1 Initial Step…..……….……….…………………………………. 28

3.3.2 Synchronous Step…..……….……….…………………………….. 29

3.3.3 Revocation Step………………………………………………… 30

3.3.4 An Illustrated Example……………….……..……………….... 30

4. Performance Analysis 33

4.1 The Cost Of Cryptographic Algorithm……..……..………………….. 33

4.2 IEEE 802.11 and RRKM………..……..…….………………………….. 34

4.2.1 Mutual Authentication…..…………………………………… 34

1896

4.2.1 Key Management…………………………………………….. 36

4.3 EAP-TLS and RRKM……………………………………………….. 37

5. Conclusions 39

References 41