

BINUS INTERNATIONAL
UNIVERSITAS BINA NUSANTARA

Computer Science

Networking

Sarjana Komputer Thesis

Odd Semester 2006/2007

**Analysis Of Wireless Dual Authentication Protocol as one of Authentication
Services in Wireless Mesh Networks**

Gema Ramadhan Adrian 0800778872

Abstract

Wireless Mesh networks currently become the recent phenomenon of wireless network environment because of its many benefits and features. In opposite way, many disadvantages such as security and unfairness problem still can be found on the network. I conduct research to find problems and solutions for the problem of the network. For testing the problem of the network, I compare between the authentication in the solution and the commonly used authentication protocol. The result shows that the solution is better and more secure than the commonly used authentication protocol.

Key words

Wireless Dual Authentication Protocol, Extensible Authentication Protocol, Wireless Mesh Network.

Preface

I want to thank God Almighty, Allah SWT, for His blessings that I was able to finish this thesis, and to people that stayed on my side, who helped me in completing this thesis, directly and indirectly. First of all, I would like to thank my mother, Retno Miastuti. Without her, this thesis would just still be a dangling hope for me. Then, I would like to thank my brother and sister, Ramadhiansjah Adrian and Miranda Apriyanti, and her family, her husband Indra Ilham and their dearest daughter Kayla Putri Virmindra, who kept motivating me throughout the whole process. And also thanks for the help from all of my friends, and also from pak muwardi who has given me strong motivation to keep writing this thesis. The last, I would highly thank the person who kept sticking by me and had been an inspiration to me, Anisa Putri Larasati Sulaiman.

TABLE OF CONTENTS

Cover Page	
Title Page	i
Certificate of Approval for Hardcover Copy	ii
Statement of Examiner	
Abstract	iii
Preface	iv
Table of Contents	v
List of Tables	viii
List of Figures	ix
CHAPTER 1 INTRODUCTION	1
1.1 Background	1
1.2 Scope	6
CHAPTER 2 THEORETICAL FOUNDATION	7
2.1 Type of Network	7
2.1.1 Wireless Mesh Network	7
2.1.2 Multi-Hop Wireless Network	7
2.1.3 Wireless Ad-Hoc Network	7
2.1.4 Wireless Sensor Network	8
2.1.5 Hybrid Wireless Network	8
2.2 Devices	8
2.2.1 Hub	8
2.2.2 Access Point	9
2.2.3 Mobile Station	9
2.2.4 Wireless Hot Spot	9
2.2.5 Wired Connectivity Gateway	9
2.2.6 Node	10
2.2.7 Radio Interface	10
2.2.8 TAP	10
2.2.9 Authentication Server (AAA)	10
2.2.10 Supplicant	10
2.2.11 Router	10
2.2.12 Host	11
2.3 Type of Attacks	11
2.3.1 Internal Attackers	11
2.3.2 External Attackers	11
2.3.3 Passive Attacks	11
2.3.4 Active Attacks	11
2.3.5 Impersonation	12
2.3.6 Sinkhole Attack	12
2.3.7 Wormhole Attack	12
2.3.8 Selfish and Greedy Attack	13
2.3.9 Sybil Attack	13
2.3.10 Sleep Deprivation	13

	2.3.11	DOS and Flooding.....	13
2.4		Network.....	14
	2.4.1	LAN.....	14
	2.4.2	Infrastructure.....	14
	2.4.3	Wired Network.....	14
	2.4.4	Routing Mechanism.....	14
	2.4.5	Fairness Metric.....	15
	2.4.6	Routing Metric.....	15
	2.4.7	Hop.....	15
	2.4.8	NLOS.....	15
	2.4.9	ACK.....	15
	2.4.10	Load Balance.....	16
	2.4.11	Quality of Service.....	16
	2.4.12	IEEE 802.11.....	16
2.5		Characteristic of Network.....	17
	2.5.1	Fault Tolerance.....	17
	2.5.2	Key Caching.....	17
	2.5.3	Flow Unfairness.....	17
2.6		Internet.....	17
	2.6.1	Broadband.....	17
	2.6.2	Internet.....	18
	2.6.3	Bandwidth.....	18
	2.6.4	TCP.....	19
2.7		Secure Criteria.....	19
	2.7.1	Availability.....	19
	2.7.2	Integrity.....	19
	2.7.3	Confidentiality.....	19
2.8		Authentication.....	20
	2.8.1	PMK.....	20
	2.8.2	Authentication.....	20
2.9		Authentication Protocol.....	20
	2.9.1	Media Access Control (MAC).....	20
	2.9.2	Wireless Dual Authentication Protocol.....	20
	2.9.3	RADIUS Protocol.....	21
	2.9.4	Mac Protocol.....	21
	2.9.5	Extensible Authentication Protocol.....	21
CHAPTER 3 PROBLEM ANALYSIS.....			22
3.1		Wireless Mesh Network.....	22
	3.1.1	Advantages of Wireless Mesh Network.....	34
	3.1.2	Disadvantages of Wireless Mesh Network.....	35
	3.1.3	Threat Motives of Wireless Mesh Network.....	37
3.2		Authentication.....	37
	3.2.1	Authentication Approaches.....	38
	3.2.2	IEEE 802.11 Authentication Architecture.....	42
3.3		IEEE 802.11 Network Components and Architectural Models..	45
3.4		Standardization Activities.....	46

3.4.1	IEEE 802.11s Mesh Networks.....	46
3.4.2	IEEE 802.15 Mesh Network.....	48
3.4.3	IEEE 802.16 Mesh Network.....	48
3.5	Summary of Problem Analysis.....	49
CHAPTER 4 SOLUTION DESIGN		50
4.1	Unfairness Problem.....	51
4.1.1	Assumption.....	54
4.2	Wireless Dual Authentication Protocol.....	56
4.2.1	Wireless Dual Authentication Protocol Procedure.....	58
4.2.2	Authentication Protocol.....	62
4.2.3	Deauthentication Protocol.....	64
4.2.4	Roaming Protocol.....	65
4.2.5	Assumptions.....	66
4.3	Overhead.....	66
CHAPTER 5 TESTING and IMPLEMENTATION		68
5.1	Extensible Authentication Protocol (EAP).....	68
5.2	Comparison Between WDAP and EAP Scheme.....	69
5.3	Desired Properties of EAP.....	72
5.4	Case Studies of EAP.....	73
5.4.1	Case Study of Western Australian Schools.....	73
5.4.2	Case study of Wi-Fi Hot Spot Authentication using GSM SIMs.....	75
5.4.2.1	Scenario of Wi-Fi Hot Spot Authentication using GSM SIMs.....	77
5.5	Unfairness Problem between WDAP and EAP.....	80
5.6	Comparison between WDAP and RSN.....	81
CHAPTER 6 EVALUATION		84
CHAPTER 7 CONCLUSION AND RECOMMENDATION.....		90
REFERENCE.....		93
CURRICULUM VITAE.....		99

List of Tables

Table 1 Examples of Attack.....	60
Table 2 Comparison of WDAP and EAP.....	87

List of Figures

Figure 1 Classification of Multihop Wireless Networks.....	22
Figure 2 The Wireless Mesh Network Core.....	23
Figure 3 Interflow and Intraflow Interference.....	25
Figure 4 Unfairness Problem.....	27
Figure 5 Examples of Attacks.....	30
Figure 6 The Dispersion of Bandwidth.....	32
Figure 7 Authentication Approaches.....	39
Figure 8 Authentication Scheme.....	43
Figure 9 Wireless Mesh Network.....	52
Figure 10 Collision-Free Algorithm Flowchart.....	54
Figure 11 Entities of WDAP.	57
Figure 12 Authentication Sub-Protocol.....	50
Figure 13 De-Authentication Sub-Protocol.....	64
Figure 14 Roaming Sub-Protocol.....	65
Figure 15 Entities of EAP.....	68
Figure 16 EAP Exchanging Messages Process.....	70
Figure 17 The Scenario of Wi-Fi Hot Spot Authentication using GSM SIMs.....	77
Figure 18 The Scenario of Wi-Fi Hot Spot Authentication using GSM SIMs.....	78
Figure 19 Taxonomy of RSN.....	81
Figure 20 Latency Diagram.....	82