

Contents

1	Introduction	1
1.1	Selfish Misbehavior Detection in 802.11TM	2
1.1.1	FS Detector and Markov Chain Based Analytical Model	2
1.1.2	Adaptive Detector and Markov Decision Process Based Modeling	3
1.2	SIP Layer Attack Detection	4
1.2.1	Flooding Attack Detection	4
1.2.2	Stealthy Attack Detection	5
1.2.3	Resource-Drained Malformed Message Attack Detection	6
1.3	Overview of This Book	7
	References	7
2	Real-Time Misbehavior Detection in IEEE 802.11TM: An Analytical Approach	11
2.1	Selfish Misbehavior in 802.11TM	11
2.1.1	IEEE 802.11 TM DCF	11
2.1.2	Backoff Selfish Misbehavior in IEEE 802.11 TM DCF	12
2.2	Fair Share Detector Design	12
2.2.1	The Observation Measure	13
2.2.2	Fair Share Detector	13
2.3	Markov Chain Based Analytical Model	14
2.4	Theoretical Performance Analysis	16
2.4.1	Average False Positive Rate	16
2.4.2	Average Detection Delay	16
2.4.3	Missed Detection Ratio	19
2.4.4	Discussion on Detection of Multiple Misbehaving Nodes	21
2.4.5	System Configuration Under Performance Constraints	22
2.4.6	Detection Performance Against Network Size Change	23
2.4.7	Comparison with the Original CUSUM Detector	25
2.5	Simulation Results	27
2.5.1	Simulation Setup	27

2.5.2	Robustness Against Short-Term Unfairness	27
2.5.3	Performance Guarantee	29
2.5.4	Performance with UDP and TCP Traffic	31
2.6	Summary	33
	References	34
3	Adaptive Misbehavior Detection in IEEE 802.11TM	
	Based on Markov Decision Process	35
3.1	Adaptive Detector Design	35
3.2	Markov Decision Process Based Modeling	36
3.2.1	Transition Probability	36
3.2.2	Reward Function	38
3.2.3	Optimization Problem Formulation	41
3.3	Theoretical Performance Analysis	42
3.3.1	Average False Positive Rate	42
3.3.2	Average Detection Delay	43
3.3.3	Missed Detection Ratio	45
3.3.4	Multiple Misbehaving Nodes Scenario	46
3.4	Simulation Results	46
3.4.1	Multiple Misbehaving Nodes Scenario	47
3.5	Summary	48
3.6	Related Work of Selfish Misbehavior Detection in 802.11 TM	49
	References	50
4	SIP Flooding Attack Detection	53
4.1	SIP Flooding Attack	53
4.1.1	Multimedia Communications with SIP	53
4.1.2	Flooding Attack	54
4.2	Basic Techniques	55
4.2.1	Sketch	55
4.2.2	Hellinger Distance	55
4.3	Detection and Prevention Scheme Design	56
4.3.1	Three-Dimensional Design	56
4.3.2	Threshold Under Attack	57
4.3.3	Attack Detection	60
4.3.4	Attack Prevention	61
4.4	Performance Evaluation	63
4.4.1	Normal Traffic Behavior	63
4.4.2	Ineffectiveness of Rate-Based Approach	64
4.4.3	Flooding Attack Detection and Prevention	64
4.4.4	DDoS Attack Detection and Prevention	67
4.4.5	Multi-attribute Attack	69
4.5	Summary	69
	References	69

- 5 SIP Stealthy Attack Detection and Resource-Drained Malformed Message Attack Detection** 71
 - 5.1 Stealthy Attack Detection 71
 - 5.1.1 Stealthy Attack 71
 - 5.1.2 Detection Scheme Design 72
 - 5.1.3 Performance Evaluation 74
 - 5.2 Resource-Drained Malformed Message Attack Detection 77
 - 5.2.1 Resource-Drained Malformed Message Attack 77
 - 5.2.2 Detection Scheme Design 78
 - 5.2.3 Performance Evaluation 80
 - 5.3 Summary 83
 - 5.4 Related Work of SIP Layer Attack Detection 83
 - References 85

Intrusion Detection for IP-Based Multimedia
Communications over Wireless Networks

Tang, J.; Cheng, Y.

2013, X, 86 p. 31 illus., Softcover

ISBN: 978-1-4614-8995-5