

CONTENTS

	Page
Certificate	ii
Declaration	iii
Acknowledgement	iv
Abstract	v
List of Tables	xi
List of Figures	xii
List of Abbreviations	xv
CHAPTER1 INTRODUCTION	1
1.1 Need of the Study	
1.2 Statement of the Problem	
1.3 Methodology of the Routing Protocols	
1.4 Objective of the Study	
1.5 Limitations of the Study	
1.6 Organization of the Thesis	
CHAPTER 2 REVIEW OF LITERATURE	10
2.1 Traditional Unicast Routing Protocols	
2.2 Multicast Routing Protocols	
2.3 Secure Routing Protocol	
2.4 The Network Layer Routing Protocols	
2.4.1 Wireless Routing Protocol	
2.4.2 Fisheye State Routing	
2.4.3 Ad – Hoc On Demand Distance Vector (AODV)	
2.4.4 Dynamic Source Routing (DSR)	
2.4.5 Zone Routing Protocol (ZRP)	
2.4.6 Comparison of Two on Demand Routing Protocols	
2.5 Protecting the Network Layer from Malicious Attacks	

2.5.1 Watch Dog and Path rater

2.5.2 SCAN

2.6 Summary

CHAPTER 3 GENERIC ATTACKS 33

3.1 Model and Assumptions

3.1.1 Network Model

3.1.2 Security Model

3.2 Umpiring System Security Models

SELF_USS AND ETUS

3.3 Implementation of Generic Security

Attacks In ETUS

3.4 Simulation Model

3.4.1 The Traffic and Mobility Models

3.4.2 Performance Metrics

3.4.2.1 Throughput

3.4.2.2 Failure to deduct

(false negatives) probability

3.4.2.3 False accusation

(false positives) probability

3.4.2.4 Communication overhead

3.5 Summary

CHAPTER 4 ELIMINATING SELFISH NODES USING TOKEN BASED UMPIRING TECHNIQUE 62

4.1 Overview of Proposed TBUT System

4.2 Token Based Umpiring Technique Model (TBUT)

4.3 Implementation of TBUT

4.3.1 Route Discovery

4.3.2 Selfish Quarantine

4.4 Experiments

4.4.1 Throughput

4.4.2 Failure to Deduct (False Negatives)
Probability

4.4.3 False Accusation (False Positives)
Probability

4.4.4 Communication Overhead

4.5 Summary

4.5.1 Cross Layer Security Schemes

4.5.2 Reliable Spectrum Schemes

4.5.3 Incentive – Based Security Schemes

CHAPTER 5 CROSS LAYER UMPIRING SYSTEM DESIGN 80

5.1 Cross Layer Umpiring System

5.1.1 CLUS Model

5.1.2 Route Reply Phase

5.1.3 Data Forwarding Phase

5.2 Models and Assumptions

5.2.1 Network Model

5.2.2 Security Model

5.3 Simulation Experiments

5.3.1 Throughput

5.3.2 Failure to Deduct (False Negatives)
Probability

5.3.3 False Accusation (False Positives)
Probability

5.3.4 Communication Overhead

5.4 Summary

CHAPTER 6 SIMULATION RESULTS ANALYSIS OF VARIOUS MODELS 98

6.1 GETUS and TBUT Analysis

6.2 Analysis of Results for CLUS

6.3 Summary

CHAPTER 7 CONCLUSIONS AND SCOPE FOR FURTHER STUDY	103
7.1 Conclusions	
7.2 Scope for Further Study	
7.2.1 Cross layer Security Schemes	
7.2.3 Reliable Spectrum Schemes	
7.2.3 Incentive-Based Security Schemes	
REFERENCES	106
PUBLICATIONS	119