

SECURED COLLISIONLESS DATA TRANSMISSION IN SLOTTED TIME COMMUNICATION NETWORK USING SOFTWARE HARDWARE CO-DESIGN

A THESIS

Submitted by

ARUL .S

*in partial fulfilment for the award of the degree
of*

DOCTOR OF PHILOSOPHY



**Department of Electronics and Communication Engineering
FACULTY OF ENGINEERING & TECHNOLOGY**

**Dr.M.G.R.
EDUCATIONAL AND RESEARCH INSTITUTE,
UNIVERSITY**

(Decl. u/s 3 of the UGC Act, 1956)

CHENNAI – 600095

NOVEMBER 2013

DECLARATION BY THE CANDIDATE

I declare that the thesis entitled “**Secured Collisionless Data Transmission in Slotted Time Communication Network using Software Hardware Co-design**” submitted by me for the degree of Doctor of Philosophy is a bonafide record of research work carried out by me during the period from January-09 to September-13 under the supervision of **Dr. S. RAVI** and has not formed the basis for the award of any degree, diploma, associate-ship, fellowship, titles in this or any other University or other similar institution of higher learning and devoid of any plagiarism.

I have also published my papers in International Journals, (Scopus rated) as per list of publications in the Annexure.

Signature of the Research Scholar

(S. ARUL)

BONAFIDE CERTIFICATE

Certified that the thesis titled “**Secured Collisionless Data Transmission in Slotted Time Communication Network using Software Hardware Co-design**” is the bonafide work of **Mr. ARUL S**, who had carried out the research under my supervision and devoid of any plagiarism to the best of my knowledge. Certified further, that to the best of my knowledge, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or diploma was conferred on an earlier occasion on this or any other scholar.

Signature of the Supervisor

(Dr. S. RAVI)

Supervisor

ABSTRACT

Time slot communication involves a group of nodes communicating in specific time slots with intrinsic topology control schemes to maintain the network capacity for adhoc and sensor networks with guaranteed metrics. Research in this area has attracted a lot of attention so as to reduce the traffic and ensure reliable transmission in the network. A set of communication links between nodes use explicitly or implicitly optimal routing mechanisms in a wireless adhoc/sensor network. Desirable metrics include “controllable” parameters such as transmission power, directional antennas and multi-channel communications. In this work, the power consumption of nodes is minimized by topology control, where each node, instead of using its maximal transmission power, sets its power to a certain level so that an effective network topology can be formed to satisfy a certain constraint. The research work forms a dynamic topology and typically functions that can send data packets with or without checksum and with or without connection oriented technique. Basically, topology control aims to sustain this data propagation topology and enhance the network connectivity to provide reliable QoS (Quality of Service) and prolong the network lifetime. Especially, the most basic requirement of a network is that it be connected i.e. check for link state is done in this work.

Broadcasting is a basic operation in wireless ad hoc networks with many applications including route discovery. In broadcasting, a node (called the source node) disseminates a message to all reachable nodes in the network. A straightforward method of achieving this is through flooding in which each node retransmits every message that it receives for the first time. A network with all the nodes in the communication range of each other requires only one transmission to deliver a message to all the nodes in the network.

Dependability of the nodes in a group network is very important for its successful applications in the engineering area. Conventionally, when a node has a failure, it (i.e. data from that node) it needs to be identified and then discard it from the existing network and then reorganize with faultless nodes to continue with the normal operation. This should be done without a tradeoff with the functional coverage of the networks. In this research, a novel self-healing algorithm is implemented and tested such that the faulty node itself opts out of the network, thereby avoiding the need for an extra logical or physical layer module to perform the detection.

The generic framework for intrusion detection and collisionless data transmission in time slot mode of communication scheme is cooperative based. In this work, this is supplemented by performing two popular encryption schemes namely Data Encryption standard (DES) and advanced encryption standard (AES) following an existing first layer security model for identifying the trusted nodes. Thus, the initial layer tracks the node details and identifies all legitimate hosts accessing the data server and subsequently performs intrusion detection. The encryption and the time slot communication is implemented easily in Linux based hardware with the code written in python and uses open source tools. This eliminates the need for licensed software and other vendor related problems. Additionally, an energy-friendly scheme is proposed to draw smoother and lower current for minimizing battery charge consumption so as to suit for hard real-time applications. Conventional reported works are more suited for soft real-time applications only and are observed to be less energy friendly. The studied metrics include (but not limited to) latency, throughput, number of collisions among the broadcasting nodes, queuing model study, effect of variable arrival and departure rates of packets, etc. along with comparison studies.

Keywords: Slotted time communication, Network security, AES Encryption scheme, DES encryption scheme, BlowFish encryption scheme, Link state algorithm, Schedulers, Queuing models: Input and virtual output queuing.

ACKNOWLEDGEMENT

I like to express my sincere thanks to Revered **Mr. A. C. Shanmugam**, founder and Mr. **A. C. S. Arun Kumar**, President Dr. M. G. R Educational and Research Institute, University, Chennai-95, for creating a conducive environment and providing obligatory infrastructure for development and implementation of this work.

I express my thanks to **Dr. K. Meer Mustafa Hussain**, Vice Chancellor, Dr. M. G. R. Educational and Research Institute, University, Chennai -95, for his enthusiastic support and insightful ideas for this work to flourish.

I express my thanks to **Dr. A. Thirunavukkarasu**, Dean (Research), Dr. M. G. R. Educational and Research Institute, University, Chennai -95, for his enthusiastic support and insightful ideas for this work to flourish.

I express my sincere thanks to **Dr. Uma Rajaram** Dean (E & T), Dr. M. G. R. Educational and Research Institute, University, Chennai -95, for the amicable support provided to carry out this work.

I extend my genuine thanks with gratitude to my guide **Dr. S. Ravi**, Professor and Head of the department, Electronics and Communication Engineering, Dr. M. G. R. Educational and Research Institute, University, Chennai -95, for his subtle and considerate approach in shaping, guiding and directing me towards effective culmination of this work.

S. ARUL

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	Abstract	iv
	List of Tables	xii
	List of Figures	xiii
	List of Abbreviations	xviii
1	INTRODUCTION	1
	1.1 Objectives of Research	2
	1.2 Benefits of the Research Work	2
	1.3 Problem Statement and Proposed Solution	3
	1.4 Methodologies for Secure Data Transmission	
	Schedule	4
	1.5 Proposed Metrics	5
	1.6 Hardware Implementation for Time Slot	
	Communication	5
	1.7 Chapter wise Thesis Organization	7
2	LITERATURE SURVEY	9
	2.1 Reported Works on DES, AES and Blowfish	9
	2.2 Reported Work on Dynamic Information	
	Flow Tracking	16
	2.3 Reported Works on Time Slot Communication	25
	2.4 Inference from Literature Review	28

	DYNAMIC INFORMATION FLOW	
	TRACKING AND ENCRYPTION SCHEMES	29
3.1	Architecture for Intrusion Detection	31
3.2	E-Mote to Server Interface	32
3.3	Advanced Encryption Standard (AES)	33
3.3.1	Rijindael S-Box	33
3.3.2	Rijindael S-Box Inverted	33
3.3.3	Rijindael Reconversion	34
3.3.4	Rijindeal Key Expansion	34
3.3.5	Key Schedule Core	34
3.3.6	Add Round Key	34
3.3.7	Crete Round Key	34
3.3.8	Galois's-Multiplication	34
3.3.9	Rijindael AES Creation Round	35
3.3.9.1	Shift Rows Using Transposition Step	35
3.3.10	Galois Multiplication of 1 Column of 4x4 Matrix	36
3.4	Mode of Operation	36
3.4.1	Decryption	37
3.4.2	Append – PKCS7	37
3.4.3	Strip – PKCS7	37
3.5	Introduction to Data Encryption Standard (DES)	37
3.5.1	'Python' Implementation Of DES	37
3.5.1.1	Pydes: Class Initialization	37
3.6	Sharing of Base Class	38
3.7	Encryption/Decryption	39
3.8	Blowfish	39
3.8.1	Encryption Algorithm	39
3.8.2	Decryption Algorithm	40
3.8.3	Defining the Feistel Network	40

3.9	Energy Friendly Transmission	40
3.10	Encoding for Self Heal Data Transmission	43
3.11	Encrypted And Decrypted Module Output	45
3.12	Implementation of Energy Friendly Transmission With Comparison Results	47
4	TIME SLOT COMMUNICATION MODELS AND METRICS	54
4.1	Memory Access Peak Rate	54
4.2	Throughput and Packet loss	55
4.2.1	Packet Loss	55
4.2.2	Throughput	56
4.3	Inference	57
4.3.1	Improvement in Throughput	58
4.3.2	Improvement in Packet Loss Rate	59
4.4	Multicast Communication with Fanout Splitting	59
4.4.1	Packet Loss	59
4.4.2	Average Throughput	60
4.5	Throughput for TSC with FIFO Queue per Input Port	60
4.6	Realtime Implementation of TSC	62
4.6.1	Scheduling Algorithm for Input Queued Switches	62
4.6.2	Scheduling Algorithm for Input Queued Switches (Maximal and Approximates the Maximum Weight Matching)	63
4.6.3	Scheduler for Slotted Input Queued Switch With Virtual Output Queueing	64
4.6.3.1	Cell-Mode Scheduler	64
4.6.3.2	Packet-Mode Scheduler	65
4.7	Scheduler for Multicast	66

4.7.1	Total Number of Queues	66
4.7.2	Multicast Scheduler to Maximize Throughput	67
4.8	Slotted Time Algorithm	68
4.9	Optimal Waiting Time among Stations	69
4.10	Hardware Implementation Results	70
4.10.1	Description of Test Results	70
4.11	Time Slot Communication Implementation with Network Emulator	78
4.12	Chapter Conclusion	81
5	NODE DETECTION AND COLLISIONLESS TSC IN HARDWARE	82
5.1	Advanced Encryption Standard	83
5.2	Slotted Time Communication and Collisionless Data Transfer	84
5.3	Algorithm for Time Slot Communication	86
5.3.1	Collision Free Slotted Time Modulation	88
5.3.2	PSEUDO Code for Time Slot Communication	90
5.3.2.1	Communication Establishment	90
5.3.2.2	Collision Check in Time Slot Modulation	91
5.3.2.3	Station Beep Detection and Time Slot Trigger	91
5.3.2.4	Node Sending Data to Station in the Allotted Time Slot	92
5.4	Analysis of Packet-Switching Network	93
5.5	Mean Value of Retransmission Attempts	95
5.6	Hardware Implementation of TSC	96
5.7	Communication in MAC Layer	98

5.7.1	Communication in Upper Layer [i.e. Above MAC Layer]	98
5.8	Jitter Effects In TSC	101
6	RESULTS AND DISCUSSION	103
6.1	System Performance for Adaptive Arrival Rates	103
6.2	Performance in Slotted Time Multiple Arrivals	108
6.2.1	Average Arrival Rate for Self Similar Data Traffic	108
6.3	Hardware Implementation Results	117
6.4	Hardware Implementation of Security Model (Encrypted Data)	120
6.5	Hardware Implementation Results for Variable File Size, 25% Fixed Delay And 50% Fixed Packet Length	122
6.6	Scheduler Implementation Results	123
6.7	Energy Friendly Transmission Implementation Results	125
7	SUMMARY AND CONCLUSION	127
7.1	Summary of the Research work	127
7.1.1	Topology Control	127
7.1.2	Dependability	127
7.1.3	Intrusion Detection	127
7.1.4	Energy Friendly Transmission	128
7.1.5	Metrics Studied	128
7.1.6	Link State Ability	128
7.1.7	Hardware Implementation	129
7.1.8	Conclusion	129
	REFERENCES	130
	LIST OF PUBLICATIONS	

LIST OF TABLES

TABLE NO.	TABLE TITLE	PAGE NO.
3.1	Details of the optional pad character	38
3.2	Slots Allocation for node transmission	40
4.1	Average number of lost cells $NE[Y]$	57
4.2	Maximum throughput for 1Gbps ports switch	57
5.1	Identification of node address	97
5.2	Data Structure in MAC layer for node 1	98
5.3	Data Structure in MAC layer for node 2	98
5.4	Data Structure in upper layer for Node 1	99
5.5	Data Structure in upper layer for Node 2	99
5.6	Comparison between cross-layer design approaches based on the direction of information	100
6.1	Scheduler implementation status from plot 6.33	124
6.2	Energy Details (Random distribution) at each node in a given time slot	126

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
3.1	Probability of error Vs Percentage Message	29
3.2	Server Vs percentage message flow	30
3.3	Secured resources Vs the percentage nodes revealing their IP address during use	30
3.4	Architecture of E-mote system	31
3.5	Frame work proposed in this research for compromises in distributed networks	32
3.6	E-mote to server interface	33
3.7	Rijindael AES creation Round	35
3.8	Shift rows using Transposition	36
3.9	Galois Multiplication	36
3.10	High and Low energy nodes	41
3.11	Node 1 Energy Distribution	41
3.12	Node 2 Energy Distribution	42
3.13	Node 3 Energy Distribution	42
3.14	Sender to Receiver process as Sequential diagram	43
3.15	Data transmission sequence in self healing encoded packets	44
3.16	Data encoding process as Flow chart	45
3.17	Encrypted data transfer among trusted nodes	46
3.18	Encrypted data transfer among untrusted nodes	46
3.19	Energy Friendly Transmission for Node 1	48
3.20	Non- Energy Friendly Transmission for Node 1	49
3.21	Energy Friendly Transmission for Node 2	50
3.22	Non- Energy Friendly Transmission for Node 2	51

3.23	Energy Friendly Transmission for Node 3	52
3.24	Non- Energy Friendly Transmission for Node 3	53
4.1	File size (KB) Vs throughput (bytes/sec); Delay =600ms, Packet length =64 bytes	71
4.2	File size (Kilo bytes) Vs packets sent; Delay = 600ms, Packet length =64 bytes	72
4.3	File size (Kilo bytes) Vs packets received (bytes); Delay = 600ms, Packet length = 64 bytes	72
4.4	File size (Kilo bytes) Vs transfer time (seconds); Delay = 600ms, Packet length = 64 bytes	73
4.5	File size (Kilo bytes) Vs throughput (bytes/seconds); Delay=300ms, Packet length = 64 bytes	74
4.6	File size (Kilo bytes) Vs packets sent(bytes); Delay =300ms, Packet length =64 bytes	74
4.7	File size (Kilo bytes) Vs packets received (bytes) Delay = 300ms, Packet length= 64 bytes	75
4.8	File size (Kilo bytes) Vs transfer time(seconds); Delay = 300ms, Packet length= 64 bytes	75
4.9	Transfer delay (ms) Vs packets lost (bytes); File size = 104KB , Packet length = 64 bytes	76
4.10	Transfer delay (ms) Vs throughput (bytes/sec); File size = 104KB , packet length = 64 bytes	77
4.11	Assigned Node IP Address	78
4.12	Node 10 selected for Slot 1	79
4.13	Node 1 selected for Slot 5	79
4.14	Messages displayed in Specific Time Slot node	80
4.15	Node 6 selected for Slot 2	80
5.1	Hostname tracking based intrusion detection	82
5.2	General Description of AES Encryption Algorithm	84

5.3	Data Transmission between nodes in Time Slot Communication	85
5.4	Hardware set up for TSC	85
5.5	Control window mechanisms to prevent directional hidden terminal problem	89
5.6	Possible cross layer interaction between layers from down to top	100
5.7	Possible cross layer interaction between layers from top to down	100
5.8	Jitter effects and its variations with metric	102
6.1	Time Vs Buffer contents for the 50 percentage of arrival rate	103
6.2	Time Vs Input contents for the 50 percentage of arrival rate	104
6.3	Time Vs Output contents for the 50 percentage of arrival rate	104
6.4	Time Vs Buffer contents for the 95 percentage of arrival rate	105
6.5	Time Vs Output contents for the 95 percentage of arrival rate	105
6.6	Time Vs Input contents for the 95 percentage of arrival rate	106
6.7	Time Vs input contents for the 99 percentage of arrival rate	106
6.8	Time Vs output contents for the 99 percentage of arrival rate	107
6.9	Time Vs Buffer contents for the 99 percentage of arrival rate	108
6.10	Average values of input, output and waiting time for case (i) to case (iii)	108

6.11	Variable arrival, departure and waiting rates	109
6.12	Variable arrival, departure and waiting rates	109
6.13	Variable arrival, departure and waiting rates	109
6.14	Time slot Vs arrival of packet at node A for arrival rate for Brownian process	110
6.15	Time slot Vs arrival of packet at node B for arrival rate for Brownian process	111
6.16	Time slot Vs arrival of packet at node C for arrival rate for Brownian process	112
6.17	Arrival plot for node A, B and C	113
6.18	Arrival plot for node A, B and C	113
6.19	Arrival plot for node A, B and C	113
6.20	Time slot Vs arrival of packet at node A	114
6.21	Time slot Vs arrival of packet at node B	115
6.22	Time slot Vs arrival of packets at node C	116
6.23	Station and Node 2 communication setup	117
6.24	Node 2 sending data to Station	118
6.25	Station successfully receiving data from Node-3	118
6.26	Station successfully receiving data from Node-4	119
6.27	AES encrypted data with collision less STC implemented in hardware	120
6.28	Blowfish encryption performed in two hardware nodes	121
6.29	Transfer of data from node 1 (receiver) to node 2 (source)	121
6.30	Node 2 is the source and node -1 is the receiver	122
6.31	File size =69 KB; Delay= 150 ms and packet length=32 bytes	122
6.32	File size =104KB; Delay= 150 ms and packet length=32 bytes	123

6.33	Realtime implementation results of priority based scheduler	124
6.34	Plot illustrating the self opting out of node with lesser energy	125
6.35	Plot illustrating the self opting out of node with lesser energy (in continued iteration check)	126

LIST OF ABBREVIATIONS

AES	:	Advance Encryption standard
ARP	:	Address resolution protocol
BMMB	:	Basic Multi-Message Broadcast
BSMA	:	Broadcast Support Medium Access
CBC	:	Cipher Block Chain
CFB	:	Cipher Feedback
CM	:	Control Memory
DES	:	Data Encryption Standard
DSSS	:	Direct Sequence Spread Spectrum
ICMP	:	Internet Control Message Protocol
MAC	:	Media Access Control
MMB	:	Multi message Broadcast
NAK	;	No Acknowledgement
OFB	:	Output Feedback
QoS	:	Quality of Service
SM	:	Switch Memory
TSC	:	Time Slot Communication
TST	:	Time Slot Tracking