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 collsionless 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

LIST OF TABLES

LIST OF FIGURES

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