

TABLE OF CONTENTS

CERTIFICATE	II
APPROVAL SHEET	II
CANDIDATE’S DECLARATION	III
CERTIFICATE	III
ACKNOWLEDGMENTS	IV
ABSTRACT	V
TABLE OF CONTENTS	VII
LIST OF FIGURES	IX
LIST OF TABLES	XI
ACRONYMS	XII
1. INTRODUCTION	1
1.1 MULTIPATH TCP (MPTCP)	3
1.2 SECURITY ISSUES WITH MPTCP	7
1.2.1 ADD_ADDR ATTACK	7
1.2.2 DENIAL OF SERVICE (DOS) ATTACK	8
1.2.3 OTHER ATTACK	8
1.3 MOTIVATION FOR THIS WORK	9
1.4 PROBLEM STATEMENT AND OBJECTIVES	9
1.4.1 PROBLEM STATEMENT	9
1.4.2 OBJECTIVES	10
1.5 RESEARCH CONTRIBUTIONS	10
1.6 THE OVERALL STRUCTURE OF THE THESIS	10
2. BACKGROUND STUDY	12
2.1 MULTIPATH TCP (MPTCP)	12
2.1.1 MPTCP CONNECTION INITIATION	16
2.1.2 JOINING A NEW SUB-FLOW TO THE ONGOING CONNECTION	19
2.1.3 ADVERTISEMENT OF THE NEW ADDRESS TO ANOTHER HOST	22
2.1.4 REMOVING THE IP ADDRESS	24
2.1.5 DATA SEQUENCE SIGNAL (DSS)	25
2.1.6 THE ABRUPT CONNECTION RELEASE (MPTCP FAST CLOSE)	25
2.1.7 CHANGE IN MPTCP SUB-FLOW PRIORITY	26
2.2 CRYPTOGRAPHY AND NETWORK SECURITY	26
2.2.1 CRYPTOGRAPHY, SECURITY ATTACKS & SECURITY GOALS	26
2.2.2 ELLIPTIC CURVE CRYPTOGRAPHY (ECC)	32

2.2.3	IDENTITY-BASED ENCRYPTION (IBE)	35
3.	LITERATURE REVIEW	38
3.1	REVIEW OF MAJOR SECURITY ISSUES WITH MPTCP	39
3.1.1	ADD_ADDR ATTACK	39
3.1.2	DOS ATTACK ON MP_JOIN	40
3.1.3	SYN FLOODING ATTACK	41
3.1.4	EAVESDROPPER IN THE INITIAL HANDSHAKE	41
3.1.5	CROSS-PATH INFERENCE AND TRAFFIC DIVERSION ATTACK.....	42
3.1.6	DATA SEQUENCE SIGNAL MANIPULATION	42
3.2	REVIEW OF EXISTING SECURITY SOLUTIONS FOR MPTCP	44
3.2.1	ENCRYPTION-BASED SOLUTIONS.....	46
3.2.2	HASHING-BASED SOLUTIONS	47
3.2.3	OPPORTUNISTIC SECURITY SOLUTIONS	49
3.2.4	MPTCPSEC	49
3.2.5	ADD_ADDR2.....	50
3.2.6	OTHER SOLUTIONS	51
4.	PROPOSED SYSTEM ARCHITECTURE AND METHODOLOGY	56
4.1	SECURE KEY EXCHANGE MODEL FOR MPTCP (SKEXMTCP) USING IDENTITY-BASED ENCRYPTION	56
4.1.1	PRIVATE KEY GENERATION (SKG_SKEXMTCP).....	57
4.1.2	MPTCP SESSION KEY EXCHANGE USING KEY PAIR (MPC_SKEXMTCP)	59
4.2	SECURE COMMUNICATION BETWEEN PKG AND COMMUNICATING HOSTS ...	61
5.	EXPERIMENTS AND RESULT ANALYSIS.....	63
5.1	RESULTS AND DISCUSSION OF SESSION HIJACKING BY MAN-IN-THE-MIDDLE ATTACK AND EAVESDROPPER IN INITIAL HANDSHAKE	63
5.2	RESULTS AND DISCUSSION OF PROPOSED SECURE KEY EXCHANGE MODEL FOR MPTCP (SKEXMTCP) USING IDENTITY-BASED ENCRYPTION	70
5.2.1	IMPLEMENTATION SETUP.....	70
5.2.2	SECURITY AND PERFORMANCE EVALUATION	72
6.	CONCLUSION AND ROAD-MAP	78
6.1	CONCLUSION.....	78
6.2	ROAD MAP FOR FUTURE WORK	79
7.	PUBLICATIONS.....	80
8.	REFERENCES	81