

LIST OF FIGURES

Figure 1.1 TCP vs. MPTCP connection scenario [2].....	1
Figure 1.2 Use Cases of MPTCP	4
Figure 1.3 TCP vs. MPTCP in TCP/IP protocol stack	5
Figure 1.4 MPTCP connection establishment and addition of sub-flow [22]	6
Figure 2.1 (a) MPTCP connection Scenario (b) TCP connection scenario [27]	13
Figure 2.2 MPTCP header format.....	14
Figure 2.3 MPTCP connection process	16
Figure 2.4 Multipath Capable (MP_CAPABLE) Option	17
Figure 2.5 MPTCP 3-way handshake process for connection establishment.....	18
Figure 2.6 Wireshark Capture of MPTCP SYN Packet.....	18
Figure 2.7 MP_CAPABLE option in TCP SYN	18
Figure 2.8 MP_JOIN Option to initiate a new sub-flow over the existing connection	19
Figure 2.9 Join Connection (MP_JOIN) Option (for Initial SYN) [3]	20
Figure 2.10 Join Connection (MP_JOIN) Option (for Responding SYN/ACK) [3]	20
Figure 2.11 Join Connection (MP_JOIN) Option (for Third ACK) [3]	21
Figure 2.12 Wireshark Capture of MPTCP MP_JOIN packet	21
Figure 2.13 MP_JOIN option in MPTCP SYN	21
Figure 2.14 Advertisement of new address using ADD_ADDR packet	23
Figure 2.15 ADD_ADDR MPTCP header format.....	23
Figure 2.16 Wireshark Capture of ADD_ADDR packet	24
Figure 2.17 ADD_ADDR Option.....	24
Figure 2.18 Network Security Model	27
Figure 2.19 Private Key Encryption (Symmetric Key Encryption).....	31
Figure 2.20 Public Key Encryption (Asymmetric Key Encryption).....	32
Figure 2.21 Elliptic curve for $y^2 = x^3 + ax + b$, where $a=-4$ and $b=5$	33
Figure 2.22 Key Exchange using ECC [28].....	34
Figure 2.23 Identity-Based Encryption.....	37
Figure 3.1 Attack Classification	38
Figure 3.2 ADD_ADDR attack scenario [24] [27]	40
Figure 3.3 Elliptic Curve Cryptography-based solution [48]	47
Figure 3.4 Hash Chain-based initial handshake.....	47
Figure 3.5 ADD_ADDR2 Packet exchange	50

Figure 3.6 ADD_ADDR2 Option	51
Figure 3.7 Secure and lightweight solution based on packet confirmation [11]	52
Figure 3.8 Session Key Distribution using SDN [10].....	53
Figure 4.1 Key Generation with IBE	58
Figure 4.2 3-way handshake with the proposed scheme.....	60
Figure 4.3 Secure key exchange during a 3-way handshake using IBE	60
Figure 4.4 Key exchange scenario between Alice–PKG and Bob–PKG.....	62
Figure 5.1 Experiment setup for performing attacks	65
Figure 5.2 Real vs. illusion for Alice and Bob during the session hijacking attack [28]	65
Figure 5.3 Configuration of tap interfaces	66
Figure 5.4 Data lost analysis during different-sized file transfer with hijacking attack	66
Figure 5.5 Data lost analysis in % during file transfer of different format.....	67
Figure 5.6 Wireshark capture for Eavesdropper at initial handshake capturing keys in clear form in MPTCP version 0.....	67
Figure 5.7 Extracting keys captured during the initial handshake to perform ADD_ADDR attack by using python script for MPTCP version 0.....	68
Figure 5.8 Wireshark capture for Eavesdropper at initial handshake capturing keys in clear form in MPTCP version 1.....	69
Figure 5.9 Extracting keys captured during the initial handshake to perform ADD_ADDR attack by using python script for MPTCP version 1.....	69
Figure 5.10 Experimental setup for testing the proposed work	71
Figure 5.11 Setting up the private key generator (PKG) of IBE	71
Figure 5.12 Public Parameter and Security Parameter Generation of IBE	72
Figure 5.13 Request for master key and private key share to the PKG	72
Figure 5.14 Encryption step and combine the key share to generate private key for decryption	72
Figure 5.15 Comparison between times required for the key generation and encryption using ECC and IBE.....	74
Figure 5.16 Comparative study of bytes required in key exchange with various MPTCP options in security solutions.....	76