

Contents

| | | |
|----------|--|----|
| 1 | Introduction | 1 |
| 1.1 | What is a Protocol? | 1 |
| 1.2 | Protocols as Processes | 3 |
| 1.3 | Techniques for Actual Protocols | 4 |
| 1.4 | Real Protocols | 4 |
| 1.5 | Reader's Guide | 5 |
| 2 | CSP Descriptions and Proof Rules | 7 |
| 2.1 | Processes and Process Synchronisation | 8 |
| 2.1.1 | Process Expressions | 9 |
| 2.1.2 | Process Algebra | 13 |
| 2.1.3 | Process Expressions for Process Networks | 20 |
| 2.2 | Channel History Semantics | 26 |
| 2.2.1 | Transitions and Traces | 26 |
| 2.2.2 | Inference Rules for Specifications Based on Traces | 29 |
| 2.3 | Failure Semantics | 35 |
| 3 | Protocols and Services | 45 |
| 3.1 | Providing a Service | 48 |
| 3.1.1 | Proving the Protocol Correct | 50 |
| 3.1.2 | Structuring your Proof | 54 |
| 3.2 | Service Features | 55 |
| 3.2.1 | Sequence Preservation | 56 |
| 3.2.2 | Data Unit Synchronisation | 56 |
| 3.2.3 | Flow Control | 56 |
| 3.2.4 | Freedom from Error | 57 |
| 3.2.5 | Service Reset | 58 |
| 3.2.6 | Connection Establishment and Release | 58 |
| 3.2.7 | Change of Mode | 60 |
| 3.2.8 | Information about Peer Change of State | 62 |
| 3.2.9 | Expedited Data | 63 |

| | | |
|----------|---|------------|
| 3.2.10 | Security | 63 |
| 3.3 | OSI and Other Layered Architectures | 64 |
| 3.3.1 | The Internet and Other Layered Architectures | 66 |
| 4 | Basic Protocol Mechanisms | 71 |
| 4.1 | Sequence Control and Error Control | 73 |
| 4.1.1 | Corruption Control | 73 |
| 4.1.2 | Simple ACK/NACK protocols | 76 |
| 4.1.3 | Simple Polling Protocols | 77 |
| 4.1.4 | ACK/NACK Protocols with Timeout | 78 |
| 4.1.5 | The Alternating Bit Protocol | 80 |
| 4.1.6 | The Case of the Floating Corpses | 82 |
| 4.2 | Flow Control | 87 |
| 4.2.1 | Fixed Window Protocols | 88 |
| 4.2.2 | Protocols with Receive Window Size 1 | 89 |
| 4.2.3 | Protocols with Receive Window Size Greater than 1 | 92 |
| 4.2.4 | Dynamic Window Systems and the Concept of Credit | 93 |
| 4.3 | Indication of Change of Peer State | 94 |
| 4.3.1 | Two-way Exchanges | 94 |
| 4.3.2 | Atomic Two-way Exchanges | 96 |
| 4.3.3 | Exchanges in the Presence of Errors | 97 |
| 4.4 | Change of Service Mode | 100 |
| 4.4.1 | Connection-mode and Connectionless-mode | 100 |
| 4.4.2 | Point-to-point and Multi-peer | 101 |
| 4.4.3 | Simplex and Duplex | 101 |
| 4.5 | Multiplexing and Splitting | 102 |
| 4.5.1 | Multiplexing | 102 |
| 4.5.2 | Splitting | 110 |
| 4.6 | Segmentation and Reassembly | 112 |
| 4.7 | Prioritisation | 116 |
| 5 | Multi-peer Consensus | 121 |
| 5.1 | Reliable Broadcasts | 122 |
| 5.2 | Election | 126 |
| 5.3 | Commitment | 129 |
| 5.4 | Byzantine Agreement | 135 |
| 5.4.1 | Using unsigned messages | 136 |
| 5.4.2 | Using signed messages | 138 |
| 5.4.3 | Other forms of Byzantine agreement | 140 |
| 5.5 | Clock Synchronisation | 141 |
| 5.5.1 | Logical Clocks | 142 |
| 5.5.2 | Real time clocks | 144 |
| 5.5.3 | Byzantine Clock Synchronisation | 146 |
| 5.6 | Finding the Global State | 148 |

| | | |
|----------|---|-----|
| 6 | Security | 155 |
| 6.1 | Cryptographic Methods | 155 |
| 6.1.1 | Encipherment | 156 |
| 6.1.2 | Secret Key Cryptosystems | 157 |
| 6.1.3 | Public Key Cryptosystems | 160 |
| 6.2 | Integrity | 164 |
| 6.3 | Digital Signatures | 167 |
| 6.4 | Entity Authentication | 170 |
| 6.4.1 | Authentication with Secret Key Cryptosystems | 171 |
| 6.4.2 | Authentication with Public Key Cryptosystems | 173 |
| 6.4.3 | Proofs of Authentication Protocols | 175 |
| 6.4.4 | Certification Authorities | 181 |
| 6.5 | Key Exchange | 184 |
| 6.6 | Non-cryptographic Methods | 186 |
| 7 | Naming, Addressing and Routing | 191 |
| 7.1 | General Principles of Naming and Addressing | 191 |
| 7.1.1 | Naming Strategies in the Upper Layers of the System | 194 |
| 7.1.2 | Directories and Servers | 197 |
| 7.1.3 | Distributed Directories | 199 |
| 7.1.4 | Internet Naming and the Internet DNS | 203 |
| 7.2 | Addressing Structures | 207 |
| 7.2.1 | OSI Addressing | 209 |
| 7.2.2 | Internet addressing | 210 |
| 7.2.3 | MOTIS/MHS Addressing | 214 |
| 7.3 | Routing | 215 |
| 7.3.1 | Flooding | 216 |
| 7.3.2 | Static Routing | 217 |
| 7.3.3 | Tree Routing | 218 |
| 7.3.4 | Centralised Adaptive Routing | 219 |
| 7.3.5 | Isolated Adaptive Routing | 221 |
| 7.3.6 | Distributed Adaptive Routing | 223 |
| 7.3.7 | Exploratory Routing | 226 |
| 7.4 | Congestion | 229 |
| 7.4.1 | Discarding | 231 |
| 7.4.2 | Limiting the Number of PDUs | 232 |
| 7.4.3 | Timeout-based control | 232 |
| 7.4.4 | Explicit feedback | 235 |
| 7.4.5 | Deadlock | 236 |
| 8 | Protocol Encoding | 241 |
| 8.1 | Simple Binary Encoding | 242 |
| 8.2 | TLV Encoding | 244 |
| 8.3 | ASN.1 Encoding | 246 |
| 8.3.1 | ASN.1 Types | 246 |

| | | |
|-----------|--|------------|
| 8.3.2 | ASN.1 Values | 248 |
| 8.3.3 | ASN.1 Encoding Rules | 248 |
| 8.4 | ASCII encodings | 251 |
| 8.4.1 | MIME encoding | 252 |
| 8.4.2 | S/MIME encoding | 255 |
| 8.4.3 | XML encoding | 257 |
| 8.4.4 | XML types | 263 |
| 8.4.5 | XML Security | 269 |
| 9 | Protocols in the OSI Lower Layers | 275 |
| 9.1 | Data Link Layer | 276 |
| 9.1.1 | Connection-mode | 276 |
| 9.1.2 | Connectionless-mode | 278 |
| 9.2 | Network Layer | 280 |
| 9.2.1 | Connection-mode | 280 |
| 9.2.2 | Connectionless-mode | 281 |
| 9.2.3 | Network Layer Security | 282 |
| 9.3 | Transport Layer | 284 |
| 9.3.1 | Connection-mode | 284 |
| 9.3.2 | Connectionless-mode | 288 |
| 10 | Application Support Protocols | 291 |
| 10.1 | Session Layer | 291 |
| 10.2 | Presentation Layer | 295 |
| 10.3 | Application Layer | 297 |
| 10.4 | Basic Application Service Elements | 298 |
| 10.4.1 | Association Control | 298 |
| 10.4.2 | Remote Operations | 299 |
| 10.5 | Commitment, Concurrency and Recovery | 301 |
| 10.6 | Client-server Systems | 303 |
| 10.6.1 | Remote Procedure Call | 304 |
| 10.6.2 | Binding | 307 |
| 10.6.3 | Asynchronous RPC | 307 |
| 10.6.4 | Object Services and Middleware | 309 |
| 10.6.5 | SOAP | 311 |
| 10.7 | Security Middleware | 316 |
| 11 | Application Protocols | 321 |
| 11.1 | File Transfer | 322 |
| 11.1.1 | ISO File Transfer and Management | 322 |
| 11.1.2 | Internet FTP | 326 |
| 11.1.3 | Network File System | 328 |
| 11.2 | Distributed Transaction Processing | 329 |
| 11.3 | Message Handling | 332 |
| 11.3.1 | The MOTIS Message Transfer Sub-layer | 333 |

| | | |
|----------|--|------------|
| 11.3.2 | The MOTIS Interpersonal Messaging Service | 335 |
| 11.3.3 | Internet Mail Protocols | 337 |
| 11.4 | Hypertext and the World Wide Web | 340 |
| 11.4.1 | Uniform Resource Identifiers | 340 |
| 11.4.2 | Hypertext Transfer Protocols | 342 |
| 11.4.3 | Web Caching | 346 |
| 11.4.4 | HTTP Authentication | 350 |
| 11.4.5 | Stateful HTTP and Cookies | 352 |
| 11.4.6 | Secure HTTP | 354 |
| 11.5 | Web Services | 356 |
| 11.5.1 | Web Service Description Language | 358 |
| 11.5.2 | Publication and Discovery of Web services | 361 |
| 11.5.3 | Web Service Architectures | 363 |
| A | Notation | 367 |
| A.1 | Data Types and Variables | 367 |
| A.2 | Data Values and Expressions | 367 |
| A.3 | Processes and Process Expressions | 368 |
| A.4 | Traces, Failures and Transitions | 369 |
| A.5 | Inference Rules for Process Specifications | 369 |
| A.6 | Security | 369 |
| B | Standardisation of Protocols | 371 |
| B.1 | Standards Organisations | 371 |
| B.2 | Standards Documents | 372 |
| B.2.1 | ISO standards | 372 |
| B.2.2 | ITU-T recommendations | 373 |
| B.2.3 | Internet standards | 374 |
| | References | 377 |
| | Index | 389 |