

Obsah

1	Model distribuovaného systému	7
1.1	Základní pojmy	7
1.1.1	Paralelní a distribuovaný algoritmus	7
1.1.2	Co by mělo být distribuováno a proč?	7
1.1.3	Proces a model distribuovaného výpočtu	8
1.1.4	Kooperace a synchronizace procesů	9
1.2	Procesové modely	9
1.2.1	Modely s předáváním zpráv	9
1.2.2	Jiné modely paralelních a distribuovaných systémů	9
1.3	Model s předáváním zpráv	10
1.3.1	Spoje	10
1.3.2	Odolnost proti poruchám	11
1.3.3	Požadavky kladené na síť	11
1.4	Stupeň rozdělení algoritmu	12
1.4.1	Asymetrie	12
1.4.2	Textová symetrie	12
1.4.3	Slabá symetrie	12
1.4.4	Silná symetrie	12
1.5	Techniky návrhu distribuovaného algoritmu	12
1.5.1	Difuzní zpracování	12
1.5.2	Obíhající příznak oprávnění	13
1.5.3	Časová razítka	13
1.5.4	Řízení v distribuovaných algoritmech	13
1.6	Paralelní procesy	14
1.6.1	Model	14
1.6.2	Deterministický systém procesů	14
1.6.3	Vzájemně neinterferující systémy	15
1.6.4	Maximálně paralelní systémy	15
1.7	Složitost distribuovaných algoritmů	16
1.8	Synchronizační úlohy	16
1.9	Dokazování správnosti distribuovaných algoritmů	17
1.9.1	Formální dokazování	17
1.9.2	Odvozování algoritmů	18
1.9.3	Specifikace	18
1.10	Některé typické distribuované algoritmy	18
1.10.1	Synchronizační algoritmy	18
1.10.2	Souběh (rendezvous)	21
1.10.3	Síťové algoritmy	21
2	Síťové algoritmy	23
2.1	Studované struktury	23
2.2	Kořenový strom – paralelní prohledávání	23
2.2.1	Paralelní prohledávání sítě	23
2.2.2	Princip implementace: vlna	24
2.2.3	Algoritmus průchodu stromu se zpětnou vazbou	24
2.2.4	Konstrukce stromu nejkratších cest	26
2.2.5	Algoritmus průchodu s řízením přenosu	28
2.3	Kořenový strom – sekvenčním prohledáváním	29
2.3.1	Sekvenční prohledávání sítě	29
2.3.2	Princip implementace: obíhající příznak	29
2.3.3	Algoritmus s lokální synchronizací	30
2.3.4	Algoritmus s řídicí informací v příznaku	31
2.4	Konstrukce kostry	33
2.5	Konstrukce virtuálního kruhu	33
2.5.1	Problém	33
2.5.2	Princip: konstrukce založená na sekvenčním prohledávání	33

2.5.3	Algoritmus	34
2.5.4	Složitost	34
3	Synchronizátory	35
3.1	Synchronizátory	35
3.1.1	Různé formy synchronizace procesů	35
3.1.2	Synchronizace	35
3.2	Pojem vlny a synchronizace posloupností vln	35
3.2.1	Úvodní příklad	35
3.2.2	Vlnové algoritmy	38
3.3	Synchronizace logickými pulsy	41
3.3.1	Koncepce synchronizátoru	41
3.3.2	Princip implementace	43
3.3.3	Příklady implementace	43
3.4	Synchronizace fázemi	47
3.4.1	Úvod	47
3.4.2	Jednoduchý příklad: výpočet optimálního směrování	48
4	Směrování v počítačových sítích	50
4.1	Úvod	50
4.1.1	Hlavní kritéria směrování	50
4.1.2	Přehled směrování v praxi	51
4.2	Síťové algoritmy a směrování nejkratší cestou	51
4.2.1	Neorientované grafy	51
4.2.2	Minimální kostra	51
4.2.3	Algoritmy nejkratších cest	52
4.2.4	Distribuovaný asynchronní Bellman – Fordův algoritmus	54
4.2.5	Adaptivní směrování založené na nejkratších cestách	55
4.3	Šíření směrovacích informací - ošetření poruch linek	56
4.3.1	Záplava – algoritmus sítě ARPANET	57
4.3.2	Záplava bez periodické aktualizace	57
4.3.3	Všesměrové vysílání topologických informací bez pořadových čísel	58
5	Synchronizace procesů v počítačových sítích	60
5.1	Vzájemné vyloučení procesů, kritické sekce	60
5.1.1	Triviální řešení vzájemného vyloučení	60
5.1.2	Algoritmus Ricarta a Agrawaly	61
5.2	Volba jednoho z n procesů	62
5.2.1	Changův a Robertsův algoritmus	63
5.2.2	Hirschbergův a Sinclairův algoritmus	64
5.2.3	Další volební algoritmy	65
5.3	Správa distribuovaných dat	65
5.3.1	Konzistence duplikovaných dat	65
5.3.2	Detekce vzájemné nekonzistentnosti	65
5.3.3	Udržování vzájemné konzistence	66
5.3.4	Inicializace nového uzlu	66
5.4	Dohoda v podmínkách neurčitosti	66
6	Detekce ukončení a uváznutí v distribuovaném systému	68
6.1	Uváznutí	68
6.1.1	Uváznutí – detekce a zotavení	68
6.1.2	Uváznutí při přidělování prostředků	68
6.1.3	Uváznutí při výměně zpráv	69
6.1.4	Uváznutí při přidělování prostředků – apriorní metody	69
6.1.5	Uváznutí při přidělování prostředků – aposteriorní metody	70
6.1.6	Algoritmus CMH (Chandy, Misra, Haas) – uváznutí při výměně zpráv	70
6.2	Detekce ukončení procesu	71
6.2.1	Algoritmus Dijkstra, Scholtena – difuzní zpracování	72
6.2.2	Ukončení na kruhu (Dijkstra, Feijen, van Gasteren)	73
7	Úvod do počítačových sítí	75
7.1	Co to je počítačová síť	75

7.2	Použití počítačových sítí	76
7.2.1	Cíle a důvody	76
7.2.2	Aplikace sítí	77
7.3	Struktura sítě	78
7.4	Architektury sítí	79
7.4.1	Hierarchie protokolů	79
7.4.2	Problémy návrhu vrstev	82
7.5	Referenční model OSI	82
7.5.1	Fyzická vrstva	83
7.5.2	Vrstva spojů	83
7.5.3	Síťová vrstva	84
7.5.4	Transportní vrstva	84
7.5.5	Relační vrstva	85
7.5.6	Prezentační vrstva	85
7.5.7	Aplikační vrstva	85
7.6	Služby	85
7.6.1	Terminologie OSI	85
7.6.2	Spojované a nespojované služby	86
7.6.3	Primitivní operace pro implementaci služeb	87
7.6.4	Vztah služeb a protokolů	87
7.7	Ostatní modely síťových architektur	87
7.7.1	Model IEEE	87
7.7.2	Model TCP/IP	88
7.8	Příklady sítí	88
7.8.1	Veřejné sítě	88
7.8.2	ARPANET	90
7.8.3	BITNET	90
7.8.4	USENET	90
7.8.5	SNA	91
7.9	Propojovací síť	93
8	ISDN a B-ISDN	95
8.1	Co to je ISDN	95
8.2	Služby ISDN	95
8.3	Vývoj ISDN	95
8.4	Architektura ISDN	96
8.5	Číslicová místní ústředna	97
8.6	Rozhraní ISDN	97
8.7	Řízení ISDN – SS #7	99
8.8	Perspektivy ISDN	100
8.9	Cíl návrhu B-ISDN	100
8.10	Přepojování komunikačních cest v B-ISDN	102
8.11	Přenosové režimy	102
8.12	Technické řešení B-ISDN	103
8.12.1	Fyzická vrstva B-ISDN	103
8.12.2	Vrstva ATM	104
8.12.3	Adaptační vrstva	104
9	Aplikační služby pro tvorbu distribuovaných systémů	107
9.1	Prostředí distribuovaných aplikací	107
9.2	Virtuální terminál	107
9.2.1	Virtuální terminál telnet	107
9.3	Distribuované uživatelské rozhraní	108
9.3.1	Otevření relace ve vzdáleném uzlu, služba rlogin	108
9.3.2	Vzdálené zadávání příkazů řídicího jazyka, služba rsh (remote shell)	108
9.3.3	Služba rcmd (remote command)	109
9.3.4	Vzdálené spouštění procesů, služba rexec (remote exec)	109
9.4	Systémy ovládání souborů v distribuovaných systémech	109
9.4.1	Možnosti řešení	109
9.4.2	ISO služba FTAM	110

9.4.3	Služba ftp (File Transfer Protocol)	110
9.4.4	Služba tftp (Trivial File Transfer Protocol)	111
9.4.5	Služba rcp (remote copy)	111
9.4.6	Služba archivace souborů	111
9.5	Elektronická pošta	111
9.5.1	E-mail, ISO norma X.400	112
9.5.2	Elektronická pošta síť INTERNET	114
9.5.3	Distribuovaný adresář, ISO norma X.500	114
10	Bezpečnost distribuovaných systémů	115
10.1	Bezpečnostní zásady	115
10.1.1	Implementace bezpečnostních zásad	115
10.2	Jak se vytváří bezpečný systém?	116
10.3	Fáze specifikace – stanovení bezpečnostních zásad	116
10.4	Fáze specifikace – stanovení bezpečnostního modelu	116
10.5	Fáze implementace – služby pro implementaci modelu	117
10.5.1	Prokazování totožnosti.	117
10.5.2	Prověřování zplnomocnění	118
10.6	Implementace služeb komunikační bezpečnosti	118
10.6.1	Symetrický bezpečný kanál	118
10.6.2	Asymetrický bezpečný kanál	118
10.6.3	Podpisování	118
10.6.4	Prokazování totožnosti.	119
10.6.5	Delegování a odebrání přístupových práv.	120
10.7	Co činí Unix bezpečným?	121
10.8	Kryptografie	121
10.8.1	Úvod ke kryptografii	121
10.8.2	Kryptografické metody s utajováním klíčů (symetrické kanály)	122
10.8.3	Kryptografické metody se zveřejněním kódovacího klíče – asymetrický kanál	124
10.8.4	Autentizace zpráv (ověřování pravosti)	125
10.8.5	Podpisování zpráv	126
11	Prezentace dat pro přenos počítačovou sítí	131
11.1	Úvod	131
11.2	Vnější typová reprezentace	132
11.2.1	Zápis abstraktní syntaxí, ASN	132
11.2.2	Norma firmy Xerox – Courier	133
11.3	Doporučení CCITT X.409	133
11.3.1	Transformace reprezentací	134
11.4	Kompresce zpráv v počítačové síti	135
11.4.1	Teoretický základ komprese dat	135
11.4.2	Kompresce konečné množiny zpráv	136
11.4.3	Kompresce nekonečné množiny zpráv	136
11.4.4	Huffmanovo kódování	136
11.4.5	Aritmetické kódování	136
11.4.6	Kontextově závislé kódování	137
11.4.7	LZW kódování (slovníková komprese)	137
12	Vlastnosti programovacích jazyků pro tvorbu distribuovaných aplikací	139
12.1	Úvod	139
12.2	Přehled vybraných programovacích jazyků	140
12.2.1	Modula	140
12.2.2	Ada	140
12.2.3	DP - distribuované procesy	142
12.2.4	CSP - komunikující sekvencí procesy	143
12.2.5	Tak tedy jaký jazyk?	144
12.3	Podrobný rozbor potřebných vlastností programovacích jazyků	144
12.3.1	Komponenty	144
12.3.2	Spojení mezi komponentami	147
12.3.3	Sémantika komunikačních operací	149

12.3.4	Jednosměrná komunikace	150
12.3.5	Obousměrná komunikace	152
13	Kooperace mezi procesy, model klient – server	153
13.1	Úvod	153
13.2	Volání vzdálených procedur	156
13.2.1	Předávání parametrů	157
13.2.2	Identifikace a lokalizace serverů	157
13.2.3	Protokol RPC komunikace klient – server	158
13.3	Sémantiky volání vzdálených procedur	159
13.4	Implementace serveru	160
13.4.1	Současnost požadavků na obsluhu	160
13.4.2	Sírotci	161
13.5	Vztah RPC a komunikačního podsystemu	162
13.6	Struktura programů klienta a serveru v systému Unix 4.3 BSD	162
14	Internetworking	165
14.1	Introduction	165
14.2	Methods of internetworking	165
14.3	Homogeneous internet (physical level interconnection)	166
14.4	Heterogeneous internet	167
14.4.1	Network connection on the data link level	168
14.4.2	Network level connection	170
14.4.3	Higher level network connection	173
14.5	Examples of distributed application services in the internet	174
14.5.1	Internet name system	174
14.5.2	Distributed directory, X.500	175
15	SÍŤOVÉ PROSTŘEDÍ Unix –DARPA/BSD (TCP/IP), ISO, NFS	180
15.1	Standardní komunikační prostředky	180
15.2	Síť uucp	180
15.2.1	Pohled programátora na zadávání požadavků na přenos	181
15.3	Počítačová síť Unix TCP/IP (DARPA/Berkeley Services)	181
15.3.1	Všeobecný popis sítě TCP/IP	181
15.3.2	Základní služby pro zasílání zpráv zabezpečené transportní vrstvou TCP/IP	182
15.4	Transport dat podle normy ISO v operačním systému Unix (System V)	183
15.4.1	Typy služeb transportního rozhraní ISO v systému Unix System V	183
15.4.2	Služby pro nespojovanou komunikaci	184
15.5	Proč dva typy služeb transportu dat?	184
15.6	Filozofie transportního rozhraní – příklad služeb typu BSD	184
15.7	Síťové prostředí NFS	186
15.7.1	Distribuovaný systém ovládání souborů NFS	187
15.7.2	Vzdálené provádění příkazů v rámci NFS	187
15.7.3	Volání vzdálených procedur	187
15.7.4	Autentizace, prokázání totožnosti	187