

The Management of Data, Events, and Information Presentation for Network Management

by

Masum Z. Hasan

A thesis

presented to the University of Waterloo

in fulfilment of the

thesis requirement for the degree of

Doctor of Philosophy

in

Computer Science

Waterloo, Ontario, Canada, 1996

©Masum Z. Hasan 1996

I hereby declare that I am the sole author of this thesis.

I authorize the University of Waterloo to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the University of Waterloo to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

The University of Waterloo requires the signatures of all persons using or photocopying this thesis. Please sign below, and give address and date.

Abstract

The purpose of a network management (NM) system is to monitor and control a network. Monitoring and control functions entail dealing with large volumes of data, events, and the presentation of relevant information on a management station. In this thesis we focus on data and events management and information presentation issues of an NM system. Existing NM systems either use traditional database systems which are not well suited for an NM system or they lack intelligent event and information presentation management frameworks. None of the systems provides a unified framework for managing data, events and information presentation tasks on an NM station.

We believe that the complexities of network management can be reduced substantially by exploiting, enhancing and combining the features of new generation database systems such as *active temporal* and *database visualization systems*. In this thesis we show that an active database system where active behaviors are specified as *Event-Condition-Action (ECA) rules* is a suitable framework for NM data and events management. The **Hy**⁺ *database visualization system* with its sophisticated abstraction and visualization capabilities is well-suited to meet the requirements of NM information presentation. We also show that by viewing the network as a *conceptual global database* the network management functions can be specified as *declarative database manipulation operations* and *Event-Condition-Action (ECA) rules*.

But the facilities provided by existing active database systems are not enough for an NM system. A number of existing active temporal database systems provide support for a *composite event specification language (CESL)* (used in the E part of an ECA rule) that allows one to relate events in the temporal dimension. But these languages lack features that otherwise are required by certain applications.

We propose a CESL called CEDAR that extends the power of existing languages. CEDAR allows a user to specify various event management functionalities in the NM domain, which are difficult or impossible to specify in existing languages. An implementation model of the language operators using Colored Petri Nets is proposed. We also propose a model of a *network management database system* that incorporates CEDAR into an active database system, and various features required by an NM system. The resulting system (the **Hy**⁺-CEDAR system) is integrated with the **Hy**⁺ database visualization system.

Acknowledgements

During the past few years I have had the pleasure and good fortune to meet and work with many talented and supportive individuals.

First I would like to thank my office mates and colleagues, Mariano Consens, Manny Noik, and Dimitra Vista for their friendship, and help.

I am indebted to my advisor at the University of Waterloo, Prof. William Cowan for his support and encouragement. Thanks Bill so much.

I owe much to Prof. Alberto Mendelzon, my co-advisor at the University of Toronto, who always backed me, both financially and morally, and allowed me unlimited freedom to explore and to grow, and for that I will remain eternally grateful to him.

In addition to Alberto and Bill, I would like to thank the other members of my thesis committee: Prof. Mike Bauer, Prof. Edward P.F. Chan, Prof. Ji-Ye Mao, and Prof. Michael D. McCool.

My warmest thanks to my brothers Shaheen, Miku, and Mamun and my sister Asma who always wanted to see their brother rise and shine.

Finally, my dear parents. I could not have come to this point without their constant encouragement from childhood. "Pursue your studies, no matter what, until you achieve the highest possible degree" is my father's motto for us. Yes, I did it. Thanks Abba and Amma for everything (dad and mom in Bengali), this thesis is dedicated to you.

Contents

1	Introduction	1
1.1	Thesis Overview	8
2	Network Management Systems	11
2.1	The OSI Reference Model	11
2.2	Network Management	14
2.2.1	Functional Management	16
2.3	NM Data and Events	17
2.4	DTNM information presentation	22
2.5	Existing NMDB systems	24
2.5.1	Commercial Systems	25
2.5.2	Yemini et. al.'s System	25
2.5.3	MANDATE System	27
2.5.4	DECmcc System	28
2.5.5	X.500 based System	28
2.5.6	Event Correlation Systems	28
2.6	Discussion	29

2.6.1	Proposal for a Network Management Database System	31
3	Active and Temporal Databases	33
3.1	Active Databases	34
3.1.1	Events in ECA rules	35
3.2	Temporal Databases	38
3.3	Active temporal Databases	42
3.4	Composite Event Specification Languages	45
3.4.1	ODE	45
3.4.2	SAMOS	48
3.4.3	Snoop	49
3.4.4	EPL	50
3.4.5	Limitations of the Languages	53
3.5	Temporal Logic	58
3.6	Discussion	60
4	CEDAR, The Event Specification Language	62
4.1	Events in CEDAR	65
4.1.1	Chronon	66
4.1.2	Intervals	66
4.2	Definition of CEDAR	67
4.2.1	Syntax and Semantics	67
4.2.2	Interval operator	71
4.2.3	Additional Operators	71

4.2.4	Event Attributes	72
4.2.5	Constraining Events through Attributes	73
4.2.6	Event Expressions with Attributes	74
4.2.7	Parameter Context	74
5	Operational Semantics of CEDAR using Colored Petri Nets	76
5.1	Colored Petri Net	76
5.1.1	Behavior of CPN	78
5.1.2	Properties - Liveness, Boundedness	80
5.1.3	CPN of the Operators	82
5.1.4	Attribute Constraints in CPN	94
5.1.5	Parameter Context in CPN	96
5.1.6	Mapping CEDAR Expressions to CPNs	97
5.1.7	Implementation	98
6	A Network Management Database System	101
6.1	The DB2 Active Database System	102
6.2	Mapping CEDAR Expressions to DB2 Triggers	105
6.3	The Hy ⁺ System	107
6.4	Network Management Database	114
6.4.1	CEDAR Rules	115
6.4.2	Defining Events in the NMDB	116
6.4.3	Polling or sampling	118
6.4.4	NM by Delegation	119

6.5	The architecture	121
7	Case Study	128
7.1	Visualizing the Network Database	129
7.2	A Fault Management Scenario	134
7.2.1	Defining and Observing Problem Symptoms	135
7.2.2	Diagnosing a Fault	139
7.3	Example Event Expressions	143
7.4	Example ECA Specifications	148
7.5	Event Correlation using Hy+	149
8	Conclusion	154
8.1	Limitations and Future Work	156
	Bibliography	159
A	Portion of TCP/IP MIB	170
B	Implementation of CEDAR	175
B.1	Composite Event Detector	175
B.2	Sample Run of CEDAR System	180

List of Figures

1.1	TCP links superimposed on the physical topology map.	6
1.2	Thesis Overview	10
2.1	The ISO/OSI Reference Model	12
2.2	Communication between nodes in a network	13
2.3	Manager-Agent Network Management Model	16
2.4	Global Network Management Database	19
2.5	Example causal relationship between alarm events	21
3.1	A simple Architectural View of Execution of ECA rules	35
3.2	Example: Discount rate cut composite event	37
3.3	Example: Sampling of stock sell events	44
3.4	FSM for $sequence(E_1, E_2)$	47
3.5	Illustration of Event Detection	51
3.6	Examples for Parameter Contexts	52
3.7	Parallel entities contributing to global history	55
3.8	Comparison of language features	61

4.1	Specification of Hysteresis Mechanism	63
4.2	“Persistence” of sampled event	64
4.3	Example Composite Event Expression with Aggregation	65
4.4	Example event history of E_1 and E_2	71
5.1	CPN for $E_1 \ominus E_2$	82
5.2	CPN for E_1 fby E_2	84
5.3	CPN for E_1 conc E_2	85
5.4	CPN for E_1 in $[I]$	86
5.5	CPN for E_1 in_end $[I]$	87
5.6	CPN for E_1 not_in $[I]$	88
5.7	CPN for $E_1 \square [I]$	89
5.8	CPN for first (E_1) in_end $[I]$	90
5.9	CPN for last (E_1) in_end $[I]$	91
5.10	CPN for nth (E_1)	91
5.11	CPN for E_1 fs E_2	92
5.12	The default CPN for $E_1 \oplus E_2$	93
5.13	CPN for $[E_1, 10 \textit{ minute}]$	94
5.14	CTPN for $[E_1, 10 \textit{ minute}]$	95
5.15	CPN for max ($E_1.a$) fs E_2	96
5.16	CPN for count and avg	97
5.17	CPN for \oplus and fby operators in Chronicle context	99
5.18	Parse tree for $E = ((E_1 \oplus E_2) \textbf{fby} (E_3 \ominus E_4)) \textbf{in} [E_5, E_6]$	100
6.1	Mapping CEDAR expressions to DB2 Triggers	108

6.2	Visualizing tuples.	109
6.3	Visualizing a Hygraph.	109
6.4	Browsing the example database.	110
6.5	Example GraphLog queries and result.	112
6.6	Request for NM data	115
6.7	Translation of data-pattern statement	123
6.8	Example translation of data-pattern event statement	124
6.9	NM by Delegation	125
6.10	A conceptual architecture of an NM system	126
6.11	An example distributed architecture of an NM system	127
7.1	Defining subnets over the physical network topology.	129
7.2	Defining and displaying the logical network layer map.	132
7.3	History trace of MIB objects for boomer.	133
7.4	Traffic information displayed against the topology map.	137
7.5	Defining an alert for possible problem symptoms.	138
7.6	Highlighting congested gateways in the logical map.	140
7.7	TCP links superimposed on the physical topology map.	142
7.8	Specification of Hysteresis Mechanism	146
7.9	“Persistence” of sampled event	147
7.10	Diagrammatic View of the rule sequences	151
7.11	Queries to form causality graph.	152
7.12	Event correlation group hygraphs.	153
B.1	CEDAR expression mapping process	175