MASTER COPY KEEP THIS COPY FOR REPRODUCTION PURPOSES

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Oct 21, 1994	Final 1 Apr 91 - 30 Jul 94

4. TITLE AND SUBTITLE
Formal Design of Communication Protocols Using Estelle

5. FUNDING NUMBERS
DAAL03-91-G-0086

6. AUTHOR(S)
Paul D. Amer, Professor

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
CIS Dept
Univ of Delaware
Newark, DE 19716-2586

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
ARO 28506.7-EL

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

In 1989, Estelle was approved as one of two ISO International Standard Formal Description Techniques(FDT) for the formal specification of computer communication protocols. Based on communicating extended finite state machines (CEFSM), Estelle has a formal, mathematical, implementation-independent semantics. It is an expressive, well-defined, well-structured language that is capable of specifying distributed, concurrent information processing systems in a complete, consistent, concise and unambiguous manner.

Over the past 3 years with the support of ARO and US Army CECOM, the PI has derived a number of results in the areas: Extensions and enhancements of Estelle; Protocol Visualization, and Automatic Test Case Generation. These results described herein.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Protocol engineering; Estelle; Networking; Formal specification;, Visualization;	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev 2-89)
Prescribed by ANSI Std Z39-18
298-102

19950203 386

Title: Formal Design of Communication Protocols Using Estelle

Type of Report: Final

Author: Paul D. Amer, Professor

Date: October 20, 1994

US Army Research Office

Contract No.: 28506-EL / DAAL03-91-G-0086

Institution: Department of Computer and Information Science
University of Delaware
Newark, DE 19716

1 Problems Studied and Results

In 1989, Estelle was approved as one of two ISO International Standard Formal Description Techniques(FDT) for the specification of computer communication protocols [3, 8]. Based on communicating extended finite state machines (CEFSM), Estelle has a formal, mathematical, implementation-independent semantics. It is an expressive, well-defined, well-structured language that is capable of specifying distributed, concurrent information processing systems in a complete, consistent, concise and unambiguous manner.

Based on a model of communicating extended finite state machines (EFSM), Estelle has been successfully demonstrated for specifying many existing and proposed ISO protocols and services. Estelle has been demonstrated as a successful FDT for specifying existing and proposed ISO protocols and services: gateways, network [7], transport, session [12], presentation [11], FTAM [17] and virtual terminal. As part of the formal specification process, the principal investigator (PI) discovered and corrected several inconsistencies (i.e., errors) in the draft standard of vtp.

Over the past 3 years with the support of ARO and US Army CECOM, the PI has derived a number of results (see Figure that follows) in the areas: Extensions and enhancements of Estelle; Protocol Visualization, and Automatic Test Case Generation. These results have based on the Estelle language, now an international standard language for formally specifying communication services and protocols.

In particular GROPE, a system that allows the Graphical Representation Of Protocols in Estelle, has been developed [1]. GROPE pictorially represents a protocol's architecture and EFSM behaviors, and animates the firing of transitions, the exchange of interactions between modules, the changing of machine states, and a host of other *visible* protocol features.

Normally after several years work, a protocol's specification reaches a stable stage of standardization. However, even though a protocol specification is standardized and assumed correct, it also must be assured that different implementations based on the same standard specification can interoperate successfully.

We have used our GROPE visualization as a means for better understanding specifications and their test sequences. This work on Protocol Test Case Visualization (PTCV) was published in [9] as an area of protocol engineering. PTCV's primary goal is to facilitate the human intuitive understanding of protocol test cases and the specifications from which they are derived. In an ideal world, protocols will be formally specified and automatically verified. These proven-correct specifications will be used to automatically derive test cases whose correctness also will be automatically verified and whose fault coverage will be accurately and precisely quantified.

The reality, however, is that today's state-of-the-art is far from this utopian scenario. The reality is that there exists today a significant dependence on human expert understanding and intuition to engineer specifications and to decide on the goodness or relevance of each test case used for testing implementations. Until this imprecise approach is formalized, PTCV is meant to maximize that expert's understanding and intuition by visualizing test cases through graphics and animation.

PTCV has combined two of the PI's active research areas: automatic test case generation and protocol visualization. In test generation, several efforts are in progress to automatically generate tests from a formal specification written in Estelle [4, 6, 10, 14, 5, 16, 15].

- P. Amer, C. Chassot, T. Connolly, M. Diaz, P. Conrad. "Partial order transport service for multimedia and other applications," *IEEE/ACM Trans on Networking*, 10/94
- M. Diaz, A. Lozes, C. Chassot, P. Amer. "Partial order connections: a new concept for high speed and multimedia services and protocols," *Annals of Telecommunications, 49(5-6)*, 5/94, 270-281
- P. Kalyanasundarum, P.D. Amer. "Protocol Test Case Visualization," *6th International Workshop on Protocol Test Systems (IWPTS)*, Pau, France, 9/93
- P.D. Amer, C. Chassot, T.J. Connolly, M. Diaz. "Partial order transport service for multimedia applications: Unreliable service," *Proc INET '93, 3rd International Networking Conf*, San Francisco, 8/93, BFA1-10
- P.D. Amer, C. Chassot, T. Connolly, M. Diaz. "Partial order transport service for multimedia applications: Reliable service," *Proc 2nd Conf on High Performance Distributed Computing*, Spokane, 7/93, 272-280
- P.D. Amer, D.H. New. "Protocol visualization in Estelle," *Computer Networks and ISDN Systems, 25(7)*, 2/93, 741-760
- S.C. Chamberlain, P.D. Amer. "Formal specification of real-time constraints in Estelle," *Reseaux et Informatique Repartie, 2(2)*, 1992, 113-134
- P.D. Amer, W. Chun. "Improvements on UIO sequence generation and partial UIO sequences," in *Protocol Specification, Testing, and Verification, XII*, (Orlando), J. Linn, U. Uyar (eds), North-Holland, Amsterdam, 1992, 245-260
- S.C. Chamberlain, P.D. Amer. "Estelle enhancements to support the specification of distributed systems," *Proc Computer Networks '91*, Wroclaw, Poland, 6/91

Figure 1: Publications Supported, in part, by Contract DAAL03-91-G-0086.

The advantages of automatic test generation are evident: faster definition of test cases, more quantifiable fault coverage, etc. Additionally, environments exist for visualizing formal specifications [13]. In particular, our PTCV environment interacts with GROPE [2], a visualization system that animates Estelle specifications for better and faster understanding of a protocol's design and eventual implementation.

A protocol engineer with a good knowledge of a protocol machine can deduce the functionality of a test and understand which part of the protocol machine is being tested with each given test. This allows the engineer to focus on deciding which tests are important or unimportant vis-a-vis protocol test coverage. This will have significant importance when these test cases have to be applied to an implementation. A user can concentrate on the important problem at hand: to identify a good set of tests that need to be run to achieve the required degree of confidence in a protocol machine. Being able to physically visualize a test case on a workstation monitor will outperform mentally picturing a test case written in TTCN.

PTCV also helps in validating tests and/or specifications. PTCV can be used to: (a) visualize tests that have been automatically generated from a given specification or (b) visualize tests generated manually (perhaps by someone else).

In case (a), visualization helps validate the automatic test generation process itself. Here tests are generated from a formal specification. Then a user sees tests applied to that specification. If a test fails, the user knows that something is wrong with the generated test since theoretically all tests correctly generated from a given specification when applied to the same specification should succeed. In case (b), PTCV helps validate empirically both the specification and the tests; it uses the tests to validate the specification and the specification to validate the tests. When a user sees a test fail, the user knows that either the independently generated test case is faulty or the specification has a problem.

Work at Delaware has resulted in a prototype system (also known as the PTCV tool) that visualizes a very limited set of protocol tests [9]. The PTCV tool inputs an Estelle specification (MUT) and test cases in TOF generated from that Estelle specification to derive the architecture for PTCV. The derivation process resulted in an Estelle specification that represents the architecture with the MUT embedded in it. The fixed part of the tester architecture is independent of the module whose test cases are being visualized and hence has to be generated only once. The dynamic part of the tester architecture is dependent on the module being tested and has to be generated at least once for each MUT.

The derivation of the PTCV architecture dealt with the following issues:

- Extracting interface information contained in the module header definition of the module whose test cases are being visualized.
- Converting test cases from a specified test notation (TOF) into an extended finite state machine and then generating Estelle code.
- Evaluating constraints that restrict the range of values that can be used in certain interaction fields. These constraints are specified during the test generation process. Constraint evaluation concerns itself with analyzing a list of given constraints and deriving a set of restrictive constraints that can be used by the test and which satisfies all given constraints. This set of restrictive constraints are then applied during test visualization. For example, given two constraints: one specifying that a sequence

number field must have a value greater or equal to 0 and the other specifying that the field must have a value less than 7, constraint evaluation will result in a constraint that allows a range of 0-6 for the sequence number field; a value in this range is used during test visualization.

- Combining the static part of the architecture and the generated dynamic part to derive an Estelle specification that represents the PTCV architecture with the module being tested as an integral part.

The architecture (Estelle specification) generated by the PTCV Tool can then be used to visualize the test cases (contained within the specification) using GROPE.

Overall, the generous support of ARO during this three year period has significantly assisted the Principal Investigator and his team of graduate students to create and further the knowledge in the subarea of protocol engineering entitled "Protocol Visualization."

2 Participating Scientific Personnel

Darren New, PhD Thsis: "Protocol Visualization in Estelle," 1991

Woojik Chun, PhD Thesis: "Test case generation for protocols specified in Estelle," 1992.

Pramod Kalyanasundarum, MS Thesis: "Protocol Test Case Visualization," 1992 (currently working on his PhD in Network Management)

Mark Carroll, MS Student (currently working on his PhD in Compilers for Parallel Computers)

Phill Conrad, Phd (in progress)

Rahmi Marasli, Phd (in progress)

Greg Burch, Phd (in progress)

References

[1] P. Amer and D.H. New. Protocal visualization in Estelle. *Computer Networks and ISDN Systems*, 25(7), 741–760, Feb 1993.

[2] P. D. Amer and D. H. New. Protocol visualization in Estelle. *Computer Networks and ISDN Systems*, 25(7), 741–760, Feb 1993.

[3] S. Budkowski and P. Dembinski. An intro to Estelle: A specification language for distributed systems. *Computer Networks and ISDN Systems*, 14(1), 3–23, 1987.

[4] W. Chun and P.D. Amer. Test case generation for protocols specified in Estelle. In J. Quemada, J. Manas, and E. Vazquez, eds, *Formal Description Techniques III*, 191–206, Amsterdam, 1991. North Holland.

[5] W.Y.L. Chan, S.T. Vuong, and M.R. Ito. An Improved Protocol Test Generation Procedure Based on UIO's. *SIGCOMM '89 Symposium: Communication Architecture and Protocols in Computer Comm. Review*, 19(4), 283–294, Sept 1989.

[6] J.P. Favreau and R.J. Linn Jr. Automated generation of test scenario skeletons from protocol specifications written in Estelle. In B. Sarikaya and G.v. Bochmann, eds, *Protocol Specification, Testing, and Verification VI*, Amsterdam, 1987. North-Holland.

[7] Information Processing Systems — Open System Interconnection. *Protocol for providing the connectionless-mode network service (Internet Protocol) Addendum 2: Estelle formal description, proposed draft 8473/PDAD2.*

[8] Information Processing Systems — Open System Interconnection. *ISO International Standard 9074: Estelle — a formal description technique based on an extended state transition model.*

[9] P. Kalyanasundaram and P.D. Amer. Protocol test case visualization. In O. Rafiq, ed, *6th International Workshop on Protocol Test Systems*, (accepted), Amsterdam, (to appear). North Holland.

[10] D.Y. Lee and J.Y. Lee. A well-defined Estelle specification for automatic test generation. *IEEE Trans on Computers*, C–40(4), 526–542, Apr 1991.

[11] A. Lombardo. On the Estelle Specification of OSI Protocols. In *Proc. Computer Networking Symposium*, 3–11, Wash, DC, Nov 1986.

[12] P. Mondain-Monval. ISO Session Service and Protocol Descriptions in Estelle. In Diaz, Ansart, Courtiat, Azema, and Chari, eds, *The Formal Description Technique Estelle*. North-Holland, Amsterdam, 1989.

[13] D. H. New. *Protocol Visualization.* PhD thesis, University of Delaware, 1991.

[14] M. Phalippou and R. Groz. Evaluation of an empirical approach for computer-aided test case generation. In *Proc. 3rd International Workshop on Protocol Test Systems*, Wash, DC, Oct 1990.

[15] K. Sabnani and A. Dahbura. A protocol test generation procedure. *Computer Networks and ISDN Systems*, 15(4), 285–297, Sept 1988.

[16] B. Sarikaya, S. Eswara, and V. Koukoulidis. A formal specification based test generation tool. Tech report, Elec. & Comp. Eng., Concordia University, Canada, 1988.

[17] G. T'Hooft. Formal description techniques: Communication tools for data communication specialists: Formal specification and implementation of a file transfer protocol. *Computer Networks and ISDN Systems*, 14(1), 311–321, 1987.