(ESTELLE '98 Workshop, Paris, November 1998)

USING ESTELLE TO EVOLVE MIL-STD 188-220

Paul D. Amer   Adarshpal S. Sethi   Mariusz A. Fecko
University of Delaware
Newark, DE 19716

Theodore Dzik   Raymond Menell
US Army CECOM
Fort Monmouth, NJ 07703

M. Ümit Uyar
City College of the City University of NY
New York, NY 10031

Michael McMahon
ARINC, Inc.
Shrewsbury, NJ 07702

ABSTRACT

For the past four years, the University of Delaware's Protocol Engineering Lab has been assisting in the US Army's development of MIL-STD 188-220. Initially UD formally specified the Data Link and Intranet layers of 188-220 in Estelle. These Estelle specifications resulted in more than fifty changes/improvements to the 188-220 document. Most importantly, these Estelle specifications are now an official part of the 188-220B standard. During the past two, UD has researched the difficult practical problem of generating test cases automatically from these Estelle specifications. Test cases are of important benefit to the CECOM in its development of a 188-220 conformance test facility. UD has delivered to CECOM two sets of tests for 188-220's Data Link Layer Class A service; further tests are being generated.

I. Introduction

In May 1994, the University of Delaware's (UD) Protocol Engineering Lab began its involvement with the US Army in using Estelle [5], [8], [11], [12], [13] to formally specify MIL-STD 188-220. An initial small contract with ARL in Aberdeen, MD, supported both simulation and specification of the May 1993 188-220 version [4], [9]. The formal specification research effort received the attention of the Communications-Electronics Command (CECOM) Software Engineering Center in Ft. Monmouth, NJ, which leads the effort to evolve 188-220 to meet the Army's requirements, through the Joint Combat Net Radio (CNR) Working Group.

The English specification of 188-220 changed significantly during 1993-95 and, as a result, a new version entitled 188-220A was published in July 1995 (see Figure 1). Beginning June 1995, CECOM sponsored UD initially for the formal specification of 188-220A's revised Data Link Layer services and, later in 1996, for the Intranet Layer service.

This work supported, in part, by the US Army Research Office Scientific Services Program administered by Battelle (DAAL03-91-C-0034), by the US Army Research Office (DAAL03-91-G-0086), and through collaborative participation in the Advanced Telecommunications and Info Distribution Research Program (ATIRP) under the Federated Laboratory Program, Cooperative Agreement DAAL01-96-2-0002.

Dr. Uyar, a research professor with CCNY, is presently Visiting Associate Professor at UD.

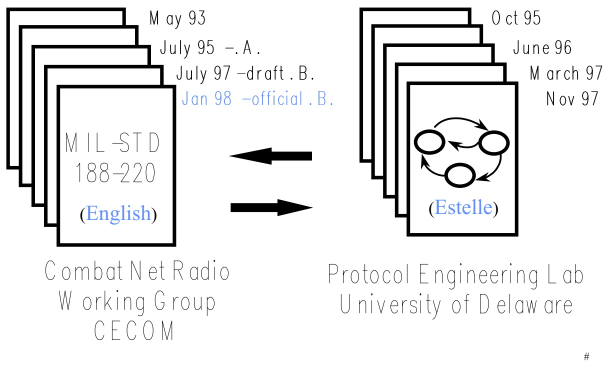

Fig. 1. History of MIL-STD 188-220 Development

The English language version of 188-220A continued its significant progress during 1995-1997 in part thanks to UD's parallel efforts to develop and maintain equivalent Estelle formal specifications. At least fifty changes to the English specification of 188-220A resulted from UD's efforts using Estelle to formally specify the standard [2]. These changes and others resulted in the most recent version 188-220B. This draft underwent a Joint services review; the CNR WG resolved a number of issues that arose during the review; and the official 188-220B was approved in January 1998 [1]. While the English text of 188-220B takes precedence in case of disagreement with the Estelle specifications, *UD's Estelle specifications are an official part of the MIL-STD.* 188-220B may well represent the first (?), only (?) major national or international standard officially including an Estelle specification.

Upon the creation of the US Army's ATIRP Telecommunication and Information Distribution Consortium in January 1996, UD's Protocol Engineering Lab began research collaboration with CCNY. Together efforts were expanded to automatically generate test cases from the Estelle specifications. This ATIRP-sponsored research directly supported CECOM's efforts to evolve 188-220 for its battlefield digitization mission. Generating tests from simple formal specifications (ie., pure finite state machine (FSM)) has been extensively studied in the literature. But the inherent complexity of 188-220B is far beyond specifying with pure FSMs, hence the need to use a more powerful specification language such as Estelle, ISO 9074. Unfortunately, generating tests from Estelle specifications presents difficult theoretical and practical problems. With ATIRP sponsorship, UD has and continues to investigate these problems with the practical motivation of applying the results towards 188-220B test case generation.

Test cases are important to CECOM's mission to develop interoperable C^4I systems. These tests support a testing capability that can assure conformance and interoperability of 188-220B implementations. Based on several research results [7], [14], [15], UD was able to generate an initial set of tests for 188-220B's Data Link layer. The delivery of these automatically generated tests to CECOM occurred in August 1997 and January 1998. This was a major milestone of the ATIRP consortium demonstrating how *research* support of Estelle test case generation resulted in tests that can assist CECOM's mission and the Army.

The initial tests that were delivered were for one component of 188-220B's Data Link layer. UD is continuing to study Estelle-based test case generation and to apply its results to the entire set of Data Link layer services.

This paper provides the reader with a better understanding of the ongoing protocol engineering activity at UD to evolve of 188-220. *It is assumed that the reader is already familiar with Estelle.* The paper is organized as follows. Section II overviews 188-220 and its primary function with the Army plans for the digital battlefield. Section III describes in greater detail the tests that have been delivered to CECOM as a result of UD's Estelle test case generation research.

II. MIL-STD 188-220

The Protocol Engineering Lab researchers at UD used Estelle to specify parts of the 188-220 protocol suite. This suite was developed to meet the requirements for horizontal integration, seamless internet communications and increased mobility using combat network radios [6]. This protocol, a critical piece of the new Joint-Army Technical Architecture, is now mandated for CNR communications. It is being implemented in U.S. Army, Navy and Marine Corps systems, and has been demonstrated initially during the Army's Task Force XXI (TFXXI) Advanced Warfighting Experiment in March 1997. 188-220 is now receiving allied/international attention, while portions of its protocol architecture have been promulgated in the Internet Engineering Task Force. Expected outcomes from its use are expected to be seamless connectivity of C^4I systems, horizontally integrated information networks, and joint interoperable C^4I systems for the warfighter.

188-220 was originally developed in May 1993 as a joint forces' standard to exchange Variable Message Format messages between fire support Digital Message Transfer Devices (DMTDs) and automated C^4I systems.

Version 188-220B, whose architecture is depicted in Figure 2, describes the protocols needed to exchange messages using CNR as the transmission media. These protocols include the physical, data link and part of the network layer of the OSI model. The protocols apply to the interface between host systems and radio systems. Hosts usually, but not always, include communications processors or modems that implement these lower layer protocols. The unshaded portions of Figure 2 indicate those protocols and extensions that were developed specifically for use with CNR.

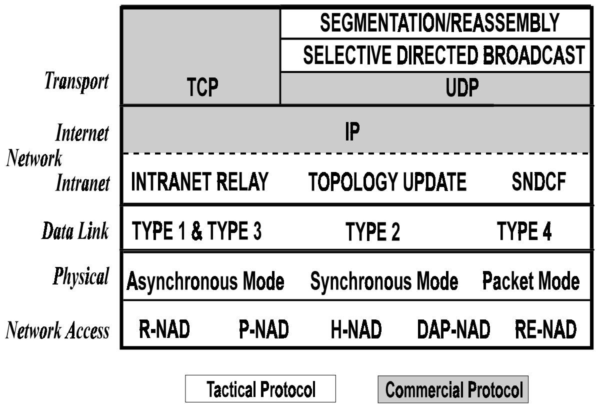

Fig. 2. MIL-STD 188-220B Protocol Architecture

The new Joint-Army Technical Architecture drives the development of Army tactical C^4I systems implementing these standards. Army systems must build to these blueprints to achieve interoperability and seamless communications for Task Force XXI Modernization.

The Joint CNR Working Group is officially chartered under the DoD Data Communications Protocol Standards Information Transfer Management Panel (IXMP). The purpose of the WG was to initially develop the protocols, and then address, resolve and document the solutions to standards-related technical issues, that is, (1) to fix any incomplete, incorrect or unsuitable aspects of the standards; (2) support a rapid development process (for implementers); and (3) document the resulting solutions and standards changes, precluding each developer from choosing different (possibly proprietary or non-interoperable) approaches.

The WG serves as a forum for focusing government and industry resources on resolving these issues. This teamwork approach resulted in quick changes to the standard and timely progression of the protocol's implementation for TFXXI. WG participants have included representatives from the DoD services/agencies, industry and academia.

III. Results: Test Case Generation

CECOM's Digital Integration Laboratory (DIL) is responsible for certifying that all systems that participated in Task Force XXI were interoperable. To perform this responsibility and future testing/certification for systems communicating over CNR, the DIL requires automated 188-220B protocol test tools. The CECOM Software Engineering Center is developing a Conformance Tester that automatically evaluates a 188-220B implementation identifying where it differs from the standard. This information can be used as a first step in the DIL's certification process, or to objectively categorize a 188-220B implementation to guide future implementations and standard evolution. The Conformance Tester capability will be used for the Army and the Army's joint requirements for years to come.

In support of this task, UD's Protocol Engineering Lab is developing test scripts to be used by the 188-220B Conformance Tester. The test scripts (a.k.a. test cases) specify a logical sequence of test steps that are performed by a Conformance Tester to individually test the Data Link Layer (Classes A,B,C) and Intranet Layer.

The test scripts are input to the Conformance Tester which in turn stimulates an Implementation Under Test (IUT), and assesses responses to determine if the IUT correctly implements the protocols. Since it is impossible to exhaustively test an implementation in practice, a good set of test scripts should at least check those events that affect state/transition, boundary conditions, and stress points. The test scripts themselves should be structured as independent modular components to facilitate modifying and adding to the scripts in response to 188-220's continuing evolution.

As shown in Figure 3, the process that UD has taken in generating tests is an indirect one. It would be ideal to be able to generate tests directly from an Estelle specification. However with today's state-of-the-art testing knowledge, this is not yet possible. The Estelle language being more powerful than pure FSMs in its specifying capability results in EFSMs that up to now are too complex for direct test case generation. A second approach to solving

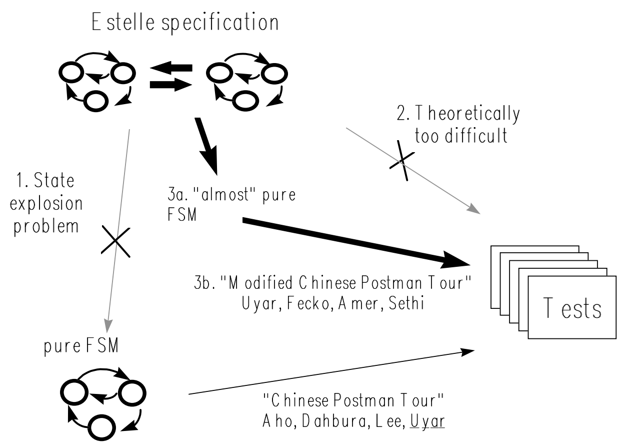

Fig. 3. Test Generation from Extended FSMs

the problem would be to *expand* Estelle's EFSMs thereby converting them to pure FSMs. This would be useful since methods exist for generating tests directly from pure FSMs (e.g., [3]). Unfortunately, converting even simple EFSMs can result in the state explosion problem, that is, the resultant FSM has so many states and/or transitions that either it takes too long to generate tests, or the number of tests generated is too large for practical use.

At UD, an intermediate approach has been investigated. An Estelle EFSM is partially expanded (hence resulting in some more states and transitions), but not expanded completely to a pure FSM. The EFSM is expanded partially just enough to generate a set of tests that is feasible and practical in size. Determining just what features to expand in the general case is the difficult aspect of this research.

Using some initial results, UD generated tests for the SAP component of 188-220B's Data Link Layer Class A service. The original EFSM specifying this functionality consists of 1 state and 15 transitions. Since the total number of possible test scenarios that would result after full expansion to a pure FSM is infeasibly large, the original EFSM was converted to three EFSMs, each somewhat closer to a pure FSM, but still containing some extensions. Each of the new EFSMs focused on a separate functionality of the Class A SAP service.

From the original EFSM with 1 state and 15 transitions, three expanded EFSMs were derived having 398, 303, and 112 states, and 799, 401, and 119 transitions, respectively. Using the expanded machines, UD's software generated three sets of tests: set I consists of general behavior tests of the the SAP component interacting with two destinations, set II tests datalink precedence, and set

III tests an IUT's behavior when interacting with up to sixteen destinations. The three sets involve 1732, 1428, and 145 inputs/expected-outputs, respectively. Each sequence of inputs/outputs exercises every transition in the corresponding expanded EFSM at least once. In August 1997, these tests were delivered to CECOM for use in its 188-220B testing facility.

The generated test sequences could be augmented to verify that the IUT is in the proper state after each input is processed. This step will at least double and likely even triple the test sequence length, hence making actual testing a longer process. UD is developing software to generate tests that include state verification using UIO sequences [10]. Current efforts at UD are on-going to generate tests for: the Station Component of the Data Link Layer Class A service, the other Class services (B,C) and the Intranet Layer.

REFERENCES

[1] *Military Standard - Interoperability Standard for Digital Message Device Subsystems (MIL-STD 188-220B)*, 1998.

[2] P. Amer, G. Burch, A. Sethi, D. Zhu, T. Dzik, R. Menell, and M. McMahon. Estelle specification of MIL-STD 188-220A datalink layer. In *Proc MILCOM '96*, McLean, VA, Oct 1996.

[3] A. Aho, A. Dahbura, D. Lee, and M. Uyar. An optimization technique for protocol conformance test generation based on UIO sequences and rural chinese postman tours. In S. Aggarwal and K. Sabnani, eds, *Protocol Specification, Testing, and Verification VIII*, 75–86, Amsterdam, 1988. North-Holland.

[4] R. Burch, P. Amer, and S. Chamberlain. Performance evaluation of MIL-STD 188-220A: Interoperability standard for digital message transfer device subsystems. In *Proc MILCOM '95*, San Diego, CA, Nov 1995.

[5] 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.

[6] T. Dzik and M. McMahon. MIL-STD 188-220A evolution: A model for technical architecture standards development. In *Proc MILCOM '97*, Monterey, CA, Nov 1997.

[7] M. Fecko, P. Amer, A. Sethi, M. Uyar, T. Dzik, R. Menell, and M. McMahon. Formal design and testing of MIL-STD 188-220A based on Estelle. In *Proc MILCOM '97*, Monterey, CA, Nov 1997.

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

[9] H. Li, P. Amer, and S. Chamberlain. Estelle specification of MIL-STD 188-220A: Interoperability standard for digital message transfer device subsystems. In *Proc MILCOM '95*, San Diego, CA, Nov 1995.

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

[11] R. Tenney. A tutorial introduction to Estelle. Tech Report 88–1, Univ of Mass, Boston, Jun 1988.

[12] R. Tenney. Tutorial on Estelle and early testing. Tech Report 97–4, Univ of Mass, Boston, 1997.

[13] K. Turner, ed. *Formal Description Techniques.* North-Holland, Amsterdam, 1989.

[14] M. Uyar, M. Fecko, A. Sethi, and P. Amer. Minimum-cost solutions for testing protocols with timers. In *Proc IEEE International Performance, Computing, and Communications Conf*, Phoenix, Feb 1998.

[15] U. Uyar, M. Fecko, A. Sethi, and P. Amer. Generation of realizable conformance tests under timing constraints. In *Proc MILCOM '98*, Boston, Oct 1998.