Reviewing the Battle at the Alamo

Grace C. Mak-Cheng
Kenneth Doris
Grumman Corporation
Great River, New York

Robert Perry
Norm Lawler
Concurrent Computer Corporation

ABSTRACT

The creation of the synthetic, virtual battlefield at the 14th I/ITSEC in San Antonio demonstrated the feasibility of the use of the non proprietary Distributed Interactive Simulation (DIS) protocols for the interoperability of dissimilar simulations. Although a major milestone has been reached in the demonstration of the ability of dissimilar simulators to communicate with the DIS protocol, true interoperability has yet to be determined. The actual interoperability of the players cannot be assessed until a thorough review the individual player's action and response has been made.

During the demonstration, a data logger developed by Concurrent Computer Corporation was used to collect all message traffic on the DIS network. Grumman, in conjunction with Concurrent, has begun a post mission review of the data collected. This paper will describe the findings of this review. A comparison of how the actual network traffic compared with the predicted assumptions, and how the use of the next order dead reckoning algorithms may impact the network traffic will be made. Discrepancies as a result of differences in the terrain database and interpretations of the rules of engagement will be pointed out. This paper will also include the "lessons learned" from this review process.

ABOUT THE AUTHORS

Grace Mak-Cheng is an Engineering Specialist in Grumman's Combat Systems organization. She is currently responsible for an Independent Research and Development project involving real-time networking of distributed simulation. She actively participates on the Standards for the *Interoperability of Defense Simulations*. Ms. Mak-Cheng is the principal investigator for Grumman's development of a DIS Network Interface Unit. During the 14th I/ITSEC, this unit was used to network Grumman's Flight Instrument Trainer to the DIS network for the DIS Demonstration. She holds a Masters in Computer Science from New York Institute of Technology and a Bachelor of Electrical Engineering from New York Polytechnic Institute of Technology.

Kenneth Doris is a Technical Advisor in Grumman's Combat Systems organization. He is currently directing several research projects, including one devoted to DIS investigation. He is an active member of both the Communications Architecture and the Emissions subgroups of DIS. Last fall Mr. Doris lead the Grumman team at the 14th I/ITSEC DIS demonstration held in San Antonio. He holds a Bachelor of Electrical Engineering from Rensselaer Polytechnic Institute and has twenty-five years experience in Simulation and C^{3}I, specializing in computer architecture and software engineering

Robert Perry is a member of Concurrent Computers' Professional Services group. He works on a consulting basis for Concurrent Computer Corporation customers, as well as in-house special projects. During the 14th I/ITSEC, he authored a DIS monitor which recorded and graphically displayed all network activity. Mr. Perry holds a Bachelor of Electrical Engineering from George

Washington University and has eighteen years experience in the simulation and computer sciences.

Norm Lawler is a member of Concurrent Computers' Engineering division. He is a project manager responsible for a number of Internal Research and Development projects involving distributed computing technology, specifically client/server application development for real-time environments. He actively participates on the Standards for the Interoperability of Defense Standards. Mr. Lawler holds a Bachelor of Science from University of Western Australia and has eleven years experience in networked applications development.

Reviewing the Battle at the Alamo

Grace C. Mak-Cheng
Kenneth Doris
Grumman Corporation
Great River, New York

Robert Perry
Norm Lawler
Concurrent Computer Corporation

INTRODUCTION

The concept for the real time demonstration of the Distributed Interactive Simulation (DIS) Standard at the 14th Interservice/Industry Systems Education Conference (I/ITSEC), which was held in San Antonio, Texas November 2-5, 1992 was conceived only eight months prior to the demonstration. Although the extent of what DIS can support is broad, the scope of the demonstration was restricted by the limited preparation time. During the eight month period, the twenty-eight organizations which participated in the demonstration worked together to define the scope of the demonstration.

The I/ITSEC demonstration was an integrated display of two standardization efforts: the DIS standard protocol data units (PDU) and communications architecture, and Project 2851, the standard for common visual data bases. The Institute for Simulation and Training (IST) at the University of Central Florida coordinated the testing and integration efforts. The pre-demonstration testing included testing of the communication protocols, DIS PDU's, terrain orientation, appearance and interactivity. Although participants were required to pass the test administered by IST before participation in the demonstration, as this paper will point out, it was possible to pass the test and not be DIS compliant.

For the demonstration, Concurrent Computer Corporation developed a network monitor which logged all the messages which were sent on the DIS network. This paper will discuss the development and implementation of the network monitor. This paper will also describe the analysis of the data collected during the demonstration. The findings of these analyzes may aid in the further development of the DIS compliant test bed, the development of future data loggers and network monitors and development of a better understanding of the DIS standards.

I/ITSEC DIS Demonstration Ground Rules

The I/ITSEC demonstration was a joint application of manned and unmanned simulated vehicles. A few of the I/ITSEC demonstration participants "listened" to the network and used the information as input to their radar simulations or displayed a "window" into the simulated battlefield environment.

DIS Network

The participants decided to make the DIS network public. This meant that anyone could play on the network as long as he or she did not interfere with any other player on the network. The participants used IP broadcast directed to UDP port 3000 (decimal) for legitimate DIS traffic. Any non-DIS messages put on the network during the demonstration were to be sent point-to-point if possible, and if not possible, by multicast. Each company was assigned 10 unique UDP port numbers for non-DIS traffic.

DIS PDU's & Dead Reckoning

The DIS standard used in the I/ITSEC DIS demonstration was Version 1.0 dated May 8, 1991. Only a subset of the PDU's listed in the DIS standard was used for the demonstration. These PDU's were the Entity State, Fire,

Detonation, and Collision PDU's. Though the Collision PDU was part of the exercises, air entities were exempted from collision tests.

With the Entity State PDU, a relative time stamp was used as a result of the absence of a global network timing mechanism. Articulation parameters were only used on some of the ground based vehicles. Of the 64 bits in the articulation parameter, the first 32 bits were used to indicate the turret azimuth and gun elevation. The remaining 32 bits were padded with zeros.

With the Detonation PDU, no articulated parameters were present in the PDU since no damage models were used in the DIS demonstration. Damage assessment models were excluded to reduce the complexity of the exercise.

The dead reckoning model used was the first degree model. The threshold parameters for issuance of new Entity State PDU's were three degrees and one cubic meter.

Terrain Database

The delivery of the terrain data base was the responsibility of the Project 2851 team. Vendors took the common database formats and converted the data into a form suitable for their computer image generators. The data base was distributed to participants in SSDB (Standard Simulator Data Base) interchange format (SIF). The data base selected for the I/ITSEC demonstration was a 100x100 km area which included portions of Fort Hunter Liggett, CA. Although there were some known discontinuities in culture and terrain, the tight schedule made freezing the data base necessary. A high resolution area of 10 km N/S and 30 km E/W was specified as the area containing all ground vehicle activity. Participants were advised to convert the high detail area as faithfully as possible. The error threshold requested by participants was set to 1.0 meters.

Testing

The IST's test plan defined the interoperability requirements for participation in the DIS I/ITSEC interoperability demonstration. The level of interoperability defined was for demonstration only and did not constitute conformance with the DIS standard for other applications. However, the test plan can be considered as a subset of a full test implementation. Details of the test plan, test procedure and test results have been published by IST (Ref. 1).

Development of the DIS Monitor

The monitor was developed on a Concurrent Computer model 7100 computer. This machine included three Motorola 68040 processors, 32 Mbytes of memory, a graphics display system (GA-5000), and integral Ethernet and SCSI controllers. This hardware was driven by Concurrent's Real Time UNIX operating system (RTU), X-Windows, and the DIS monitor application.

The goal of the DIS monitor was to provide a real-time visual display of network traffic on a per player basis as well as log all network activity to disk for later review. The demands of this goal required that the application utilize the real time extensions to UNIX that RTU provides. This includes priority scheduling, CPU dedication, and very efficient inter-process communication mechanisms. The monitor application was based on four co-operating (UNIX) processes: a net reader, a statistician, a disk writer, and the display system. Each of these processes attached to a shared memory area and coordinated all data access through locked counters and asynchronous traps.

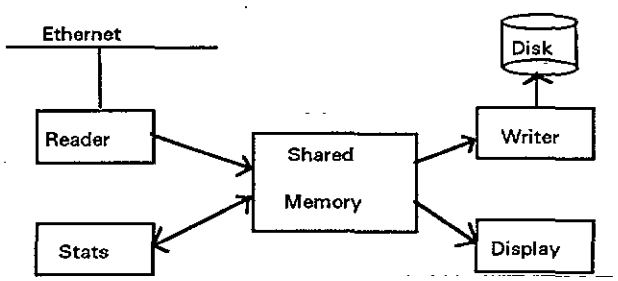

Figure 1 Concurrent Computer Corporation Network Monitor

Net Reader - This process used the Data Link Programming Interface (DLPI) available in UNIX. DLPI allows an application to bypass all network protocol software thereby providing the most efficient access to the net while still

maintaining hardware independence. In addition DLPI passes the "raw" Ethernet frame to the application. Each frame includes hardware source and destination addresses. These addresses proved very useful in identifying players during an exercise and in simulating all players during a replay operation. The net reader issues reads on the net and when data is available, it time stamps the packet, and loops waiting for the next read completion.

Statistician - This process reviews data provided by the Net Reader and decodes each packet according to type on both a player and net basis. This process runs until it has processed all the new data provided by the Net Reader; at which time it suspends execution.

Disk Writer - This process logs all packet data and associated time stamps to disk. Similar to the Statistician, this process continues to execute as long as new data is available.

Display - This X-Windows based program graphically displays the output of the Statistician process using custom bar chart and strip chart Widgets. There are two screens in the monitor. One shows overall network activity while the other indicates the type of activity by the specified player.

As the packets are read from the net, each is time stamped using the internal gettimeofday() UNIX system call. For analysis, this stamping procedure is very important as there was no synchronized time base across the network. It is assumed that by using DPLI, real-time priorities, and the pre-emptive kernel of RTU, any delay associated with packet transmissions and reception within the host machine is constant. One "problem" discovered during the analysis regarded the interpretation of the recorded time stamp. The time recorded is based on GMT while the standard UNIX routine that interprets this time takes into the account the time zone of the machine doing the analysis.

POST MISSION REVIEW

The post mission review involved examining two issues: (1) Network Traffic, and (2) Entity Interactions. Analysis of the network traffic involved examining the number of packets which was issued by each entity and the network bandwidth consumption of these packets. A second order dead reckoning algorithm was applied to the Entity State PDUs issued by each entity to determine the effect of this higher order algorithm on the network traffic. Since only four DIS PDUs were used at the demonstration, the entity interaction analysis was limited to examining the Fire/Detonation event sequences and the Collision detection.

ACTUAL NETWORK TRAFFIC

Network Packet Analysis

During the 14th I/ITSEC demonstration, Concurrent Computer Corporation made a number of logs of the network traffic, which included some test sessions as well as the plenary session. The following analysis is based on the data log of the second plenary session which was recorded on Tuesday, November 3, 1992, for one hour starting at 5:30 p.m. This period of time was chosen since it represents a pattern of network traffic usage under a "controlled" DIS scenario and is not distorted by DIS testing and debugging activities.

Two key aspects of networking which affect DIS are the processing load imposed on each host on the network by DIS traffic, and the consumption of the available network bandwidth. The load on each host system is directly related to the number of network packets which have to be processed, where each packet imposes an interrupt and processing overhead before the DIS data can be made available to the simulation application. The bandwidth issue is related to the amount of data transmitted over the network, typically in terms of bits per second (bps).

Out of the total of 150,000 network packets logged during the analysis period, 96,334 were DIS PDUs and 53,666 were non-DIS packets. Figures 2 and 3 show a further breakdown of the DIS PDUs and the non-DIS packets:

	Entity State	Fire	Detonation	Collision
No. of PDUs	96,213	61	56	4

Figure 2 DIS PDU Types

	ARP	ICMP	TCP	OTHER UDP
No. of Packets	5025	48,364	149	128

Figure 3 Non-DIS PDU Types

As expected, Entity State PDUs make up the bulk of the DIS traffic. As all of the DIS PDUs were UDP broadcast packets, every host should have received and processed all 96,334 PDUs. Averaged over the one hour analysis period, this represents a per host load of only 27 PDUs/second. A more detailed analysis showed that the worst case sustained load occurred over an 18 second interval during which the average load was 112 PDUs/second, with a peak of 139 PDUs/second. During this interval 28 entities contributed to the network traffic, six Anti-Armor Maverick guided missiles produced 78% of the total Entity State PDUs during this time.

A total of 98 simulation entities was recorded over this one hour period. The breakdown of the number of PDUs issued by each entity type is shown in Figure 4.

The large number of non-DIS packets, particularly the ICMP (Internet Control Message Protocol) and to a lesser extent the ARP (Address Resolution Protocol) message, was unexpected. The ICMP packets were almost totally of Type 3, Code 1 ("host unreachable"), all from the same source, indicating that the probable cause was one particular host on the network used a non-conformant IP protocol suite. This host sent ICMP error messages as a result of receiving a datagram defined to an IP broadcast address. (See Section 3.2.2 of RFC 1122 - Requirements for Internet Hosts -- Communications Layers).

Interestingly, there was a period of approximately 27 minutes during the middle of the one hour analysis period when almost no ICMP messages were logged, indicating that the problematic host was either powered down or disconnected from the network at this time. Since every ICMP message was directed to a specific host, this should not have imposed any extra unnecessary processing load on the other hosts on the network.

Network Bandwidth Analysis

The 150,000 network packets (DIS and non-DIS) transmitted during the one hour analysis period resulted in 21.4 Mb of data being sent over the network. This gives an average bandwidth usage of only 0.0475 Mbps over the one hour period. The peak bandwidth consumption for this one hour demonstration only reached 0.15 Mbps, thus using only 1.5% of the available 10 Mbps bandwidth capacity of the Ethernet. Moreover, the 1.5% bandwidth usage was a result of at least one ICMP packet being transmitted by the errant host discussed earlier. Further analysis showed that only 16 simulation entities contributed to the peak loading.

Figure 5 shows the rates (per minute) at which DIS and non-DIS packets were transmitted over the network. The peak for both types of traffic during the second minute is the point of peak bandwidth usage, while the DIS PDU peak in minute 28 was the point of maximum DIS PDU load for the hosts on the network. This graph shows the close correlation between the DIS broadcast PDUs and the ICMP messages discussed earlier.

The total number of DIS-related and non-DIS-related bytes (summing the complete Ethernet frame sizes contained in the packets) transmitted over the network came to 17.75 Mb and 3.65 Mb respectively.

Dead Reckoning Algorithm Analysis

For the I/ITSEC demonstration, the first degree dead reckoning model was used. Since the fields in the Entity State PDU which would allow for higher orders of dead reckoning (i.e., the acceleration and angular velocities) were in most cases not filled in by the participants, a detailed analysis of the use of other dead reckoning algorithms was not possible.

KIND/ DOMAIN	NUMBER IN EXERCISE	ENTITY STATE PDU	FIRE PDU	DETONATION PDU	COLLISION PDU	% OF BANDWIDTH
PLATFORM/ LAND	52	15739	6	6	2	16
PLATFORM/ AIR	16	71065	31	27	0	75
PLATFORM/ SURFACE	4	2237	23	23	2	2
MUNITION/ ANTI-AIR	14	4294	0	0	0	4
MUNITION/ A-ARMOR	6	1935	0	0	0	2
MUNITION/ A-SHIP	5	924	0	0	0	1
LIFEFORM/ LAND	1	19	0	0	0	0
TOTAL	98	96,213	61	56	4	

Figure 4 DIS PDU Breakdown

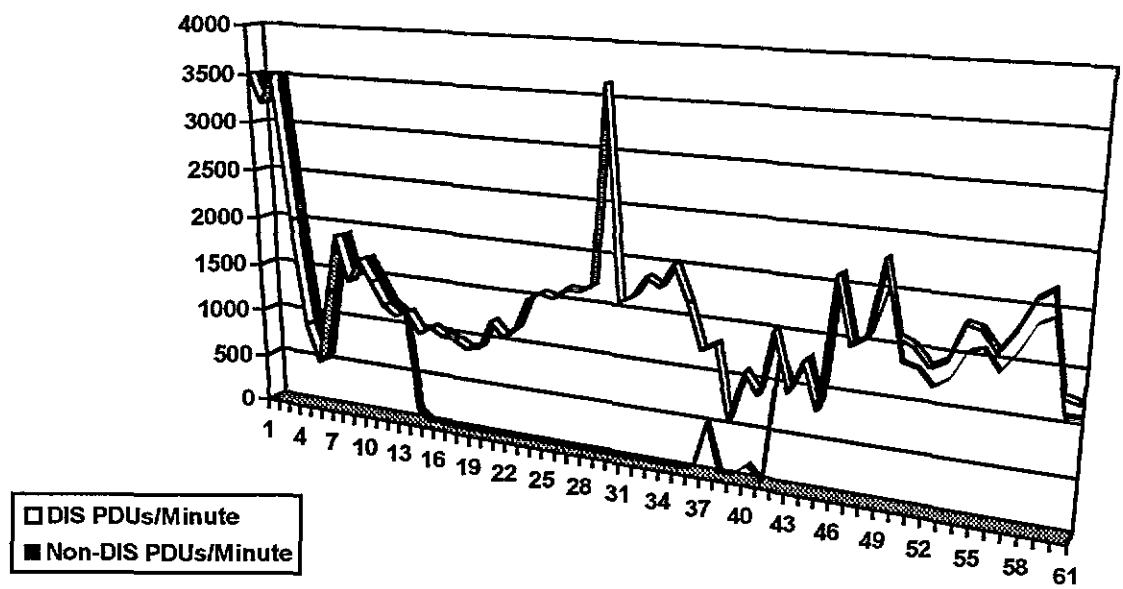

Figure 5 Network Bandwidth Analysis

I/ITSEC EXERCISE TRAFFIC ESTIMATES

% ENTITIES AT HIGH RATE		0%	20%	40%	60%	80%	100%
% ENTITIES AT LOW RATE		100%	80%	60%	40%	20%	0%
# of TANKS	52 →	17,638	51,551	85,463	119,375	153,288	187,200
# of AIRCRAFT	16 →	4,608	41,216	77,824	114,432	151,040	187,648
# of SHIPS	4 →	1,152	2,240	3,328	4,416	5,504	6,592
# of TACTICAL VOICE LINKS	0 →	0	0	0	0	0	0
# of TACTICAL DATA LINKS	0 →	0	0	0	0	0	0
TOTAL TRAFFIC BITS/SEC	→	23,398	95,007	166,615	238,223	309,832	381,440
PDU/SEC	→	14	62	109	156	203	250

However, it was possible to analyze the effects of a second degree dead reckoning model with the recorded data by calculating the entity's acceleration from two frames of velocity data. A new position was calculated with the acceleration and velocity terms. Using the recorded data as the "truth" for the entity's position, a comparison was made to determine if an Entity State PDU needed to be issued as a result of exceeding the threshold limits of one cubic meter.

The results of this analysis showed that the use of a second degree of dead reckoning resulted in a saving of 1634 Entity State PDUs. The uses of a second degree dead reckoning algorithm resulted in no savings of Entity State PDUs for entities which were land platforms (i.e., tanks); however, a saving of as much as 17% was seen with some of the air platforms. With the entities which were munitions, little savings were seen (i.e., only a saving varying from one to five Entity State PDUs).

Predicted Network Traffic

The predicted network traffic is based on a network bandwidth analysis program which was written by Grumman (see Ref. 2). Figure 6 shows the predicted network traffic for the given number of entities which were recorded during the plenary session. The observed average rate of 27 PDUs/sec matches well with a predicted rate of about 10% activity while the peak observed rate of 139 PDUs/sec would match about 50% activity. The predicted traffic in bits/sec of approximately 200K bits/sec , however , is somewhat high in comparison to the observed peak of 150K bits/sec.

Discrepancies in entity interactions

This portion of the analysis is still ongoing. One observation that can be made is that not every Fire PDU was followed by a corresponding Detonation PDU (61 vs. 56). The next step will be to look in detail at the time difference between the issuance of the Fire PDUs and the associated Detonation PDUs, and to examine whether the intended targets match in both.

Lessons Learned

The data logs included a header which contained the exact time in seconds, from January 1, 1970, GMT, in which the data logging began and when it finished. Each logged Ethernet frame was similarly time stamped. Unfortunately, the relevant timezone and daylight saving information (w.r.t the machine recording the data) were not logged which made it extremely difficult to match up data logs with known events which occurred at the specific times during the I/ITSEC demonstration (e.g., the start of the plenary sessions).

Suggestions

If the data logs are large, then a general requirement is to provide a way to analyze specific sections of a data log, and wall clock times are the most obvious means of identifying significant points in the log. If the analysis is to be carried out on systems other than the machine which recorded the data, then the timezone and daylight saving information must be recorded somewhere in the data log.

At the time of the I/ITSEC demonstration, no analysis tools had been implemented. While Concurrent Computer Corporation also had a Network Monitor displaying real-time the network traffic loads, it was not obvious at the time that ICMP messages were being transmitted over the network at such significant rates. It was only during later when analyzed over a reasonable time frame that *ICMP messages were seen as significant and* likely to cause a potential network problem. The lesson to learn here, is that analysis tools should be an integral part of any data logger and it should be possible to use the tools even during the data recording session to obtain a more complete view of network traffic patterns and be able to pinpoint network problems earlier.

References

[1] I/ITSEC DIS Interoperability Demonstration Test Procedures and Results; Institute for Simulation and Training, University of Central Florida; Feb. 16, 1993.

[2] Computer Architecture for Distributed Interactive Simulation (CADIS); *Military-Standard (Draft)*; Institute for Simulation and Training, University of Central Florida; June 28, 1993.

[3] RFC 1122 -- Requirements for Internet Hosts -- Communication Layer.