COMMUNICATION ARCHITECTURE ISSUES FOR DISTRIBUTED INTERACTIVE SIMULATION (DIS)

Amy Vanzant-Hodge
Dr. Bruce McDonald
Institute for Simulation and Training (IST)
Orlando, Florida 32826
and
Karen Danisas
Simulation, Training and Instrumentation Command (STRICOM)
Orlando, Florida 32826

ABSTRACT

The Standards for the Interoperability of Defense Simulations, also known as the Distributed Interactive Simulation (DIS) standards, have been under development since 1989 and currently define a set of protocol data units (PDUs) by which dissimilar simulators and simulations can communicate in a networked environment. A series of workshops have provided the forum for industry, government, and academia to develop these standards. The Communication Architecture / Security Subgroup (CASS) of these workshops is responsible for defining the communication architecture to be used for networking dissimilar systems together. This paper will present issues that have been brought to the surface by CASS in the process of defining the communication architecture for DIS.

The government mandate for the use of Government Open Systems Interconnection Profile (GOSIP) for all communication architectures has driven the DIS requirements. The concept of distributed simulations requiring interaction has led to the definition of **service requirements** which must be met by the communication architecture. Two of these, **real-time** and **multicast**, are not provided for by GOSIP at this time. Another issue is the need for **reliable** communications within the real-time multicast setting. These issues lead to the question of what type of performance can be expected and is needed to accomplish some level of fidelity for applications within DIS. Other issues include (1) the incorporation of security into DIS and (2) the connection of existing devices to DIS compliant networks. As these issues are examined, the objective of interoperability among systems leads to the use of existing standards, where available. This paper will address the role of communication architecture in DIS, service and security requirements, requirements for interfacing dissimilar systems, the use of existing standards, and the overall CASS approach for defining communication architecture for DIS.

ABOUT THE AUTHORS

Amy Vanzant-Hodge received a BS and MS in Computer Science from the University of Central Florida in 1983 and 1989 respectively. She has several years of application software experience before joining IST in 1990. At IST, Amy has participated in such projects as Intelligent Simulated Forces, Networking and Communication Technology Laboratory, Vehicle Integrated Defense System, and is currently the liaison for the Communication Architecture/Security Subgroup for the Interoperability Standards project.

Dr. Bruce McDonald received his Ph.D. degree in Industrial Engineering from Texas A & M University in 1973. He is currently the Program Manager for the development of standards for the interoperability of defense simulations at IST. He is the chairman of the DIS Steering Committee, which leads the standardization efforts. Dr. McDonald has 22 years of experience in research and systems analysis on training systems and operational equipment.

Karen Danisas received her masters degree in Industrial Engineering from the University of Central Florida in 1990. She is currently the Project Engineer for DIS Standards Development programs at the Army's Simulation Training and Instrumentation Command (STRICOM), Orlando, Florida. She has worked in the simulation and training community for 7 years.

COMMUNICATION ARCHITECTURE ISSUES FOR DISTRIBUTED INTERACTIVE SIMULATION (DIS)

Amy Vanzant-Hodge
Dr. Bruce McDonald
Institute for Simulation and Training (IST)
Orlando, Florida 32826
and
Karen Danisas
Simulation, Training and Instrumentation Command (STRICOM)
Orlando, Florida 32826

INTRODUCTION

Imagine yourself sitting in a tank simulator that is effectively moving across a simulated terrain based on the visual representation of the terrain displayed on the viewscreen. As you turn the turret, you see other simulated tanks moving along the terrain beside you. The order comes in that your platoon should proceed to location Alpha. As you move your tank toward location Alpha, the other tanks also move and keep their formation around you. The unique feature about this scenario is that the other tank simulators and the people guiding those simulators are each located in different cities than you. You are able to train in a joint exercise and interact with other trainees without having to travel to a distant location. You and the others are participating in a Distributed Interactive Simulation (DIS) exercise.

What Is DIS

The scenario described above has been demonstrated in the Simulator Networking (SIMNET) project funded by the Defense Advanced Research Projects Agency (DARPA). DIS is an expansion and standardization of the concepts proved in SIMNET. DIS will encompass simulatrs, stimulators, real devices, support devices, and will eventually support thousands of entities interacting in exercises where the participants are globally dispersed.

The Standards for the Interoperability of Networked Defense Simulations, also known as the Distributed Interactive Simulation (DIS) standards, have been under development since 1989 and currently define a set of protocol data units (PDUs) by which dissimilar simulators and simulations can communicate in a networked environment. These PDUs define the information passed between the systems participating in a DIS exercise. A series of workshops provide a forum for industry, government, and academia to develop these standards. The basic DIS concepts [2] are:

- No central computer for event scheduling or conflict resolution.
- Autonomous simulation nodes are responsible for maintaining the state of one or more simulation entities.
- There is a standard protocol for communicating "ground truth" data.
- Receiving nodes are responsible for determining what is perceived.
- Simulation nodes communicate only changes in their state.
- Dead reckoning is used to reduce communications processing.

What type of communications technology will support such an effort and does that technology exist today?

Role of Communications Architecture In DIS

The communications architecture is a blueprint for defining the communications mechanisms and requirements to be used for DIS. The Communication Architecture / Security Subgroup (CASS) of the standards workshops is responsible for defining this communication architecture. In order to guarantee communications in a world wide domain, using standards for defining the communications architecture is necessary. However, with the variety of network standards currently available, the selection of a specific set of standards is not an easy choice. Also, in those areas where standards do not currently exist, the DIS community must promulgate certain technologies to be standardized to meet the DIS communication architecture needs. As a starting point, the CASS decided that the communications architecture should comply with the Government Open Systems Interconnection Profile (GOSIP).

OSI Reference Model and GOSIP

The communications architecture can be likened to the human body in that it contains many unique pieces that must work together for the body to function. Like the body, the communications architecture has a "spine" that acts as the common support for the architecture structure. This spine is the set of communication protocols that allow information to be transmitted from one system to another. GOSIP defines one type of spine.

GOSIP is based on the International Organization for Standards (ISO) Open System Interconnection (OSI) protocols. The ISO Reference Model (ISORM)[3] defines a seven layered approach (a stack) where each layer provides different communications services. In a full OSI stack, there would be protocols for each layer of the stack. Partial stacks are also implemented. Because GOSIP has been mandated by Congress to be used in government data communications, the DIS community supports the evolution of a DIS GOSIP compliant communication architecture.

Many of the issues presented in this paper are directly related to the use of the ISORM and the OSI standard as well as other standards. This paper attempts to discuss some of the issues revolving around the selection of and the use of these standards and technologies for the DIS communication architecture.

SERVICE REQUIREMENTS

Before any problem can be solved, it must first be defined. Defining the services that must be provided by the communication architecture is the first step toward developing the communication architecture. This list of services, or service requirements, evolved over a period of three years through the discussions at the DIS standards workshops by the CASS. This subgroup is responsible for providing the development of the DIS standard for communication architecture. Below is the list of the communication service requirements for DIS as defined by the CASS:

- Unicast
- Multicast
- Broadcast
- Real Time Operating Speeds
- Non-Real Time
- Small Packets
- Bulk Transfer
- Reliable
- Unreliable
- Low Interpacket Dispersion for Voice/Video
- Multicast Management
- Authentication /Access Control
- Non-Blocking Interface
- Flow Control
- Low Latency Packet Delivery
- Security
- Flexible Entity Naming and Addressing
- High Throughput

These requirements evolved from discussions of how to provide the type of communications services that would facilitate the various DIS applications envisioned. As with anything in a dynamic state, these requirements will change as technology changes and as the DIS community's needs change.

Needed Requirements versus Desired Requirements

When viewing the above service requirements, the initial question of "can all of those requirements be met" comes to mind. The level or degree that the requirement is met must also be considered. Realistically, all of the above requirements cannot be met today because all of the necessary technology does not yet exist. The requirements must then be viewed in terms of those that are needed for DIS applications to run today and those requirements that are desired for future applications of DIS.

PDU Requirements

In an attempt to answer the above question, the Communication Architecture for DIS (CADIS)[1] preliminary draft standard takes the approach that each DIS PDU requires certain services to make its communication practical. The document categorizes the ten current standardized PDUs into communication classes based on the desired and needed service requirements. The service requirements analyzed were a subset of those listed above, which include real-time, broadcast, multicast, unicast, reliable and best effort.

Real-time. A real-time service is one which satisfies timing constraints imposed by the service user. The timing constraints are user specific and should be such that the user will not be adversely affected by delays within the constraints. DIS requires that tightly coupled data be processed within 100ms and loosly coupled data be completed within 300ms, therefore the DIS real-time threshold is 100ms.

One of the issues regarding this threshold is whether it is attainable using the existing technology of physical media, protocols, operating systems, applications and their interfaces to the network, and security mechanisms. Each of these items demands some amount of time. The delay that occurs when this time is used is called latency. The real-time thresholds stated above only indicate a total latency that is acceptable, not how much each of the items above is allowed. In the CADIS document, latency was categorized so that different parts of the network had bounds on the time it could use. These bounds are shown in Figure 1. It shall be noted that these bounds are not finalized, but represent a starting place for initial DIS applications.

Multicast, Broadcast, and Unicast. Multicast is a transmission mode in which a single message is sent to multiple network destinations, i.e. one to many. Broadcast, a mode in which a single message is sent to all destinations, is the current method of delivering messages for SIMNET and upcoming DIS procurements. Unicast is a mode for point-to-point communications, such as messages used for simulation management to bring a new system into a DIS exercise.

It is envisioned that future DIS applications will have thousands of entities sending PDUs, and using broadcast mode for all PDUs could overrun the available bandwidth on the network. Multicast mode would allow the PDUs to be sent to only those entities designated in a multicast address group and thereby reduce traffic for the rest of the network.

Multicast protocols do exist today, such as STreams-II, eXpress Transfer Protocol (XTP) by Protocol Engines, and Internet Protocol (IP) Multicast. However, each of these is limited in the multicast services that they provide and therefore do not meet all of DIS needs. STreams-II, which is currently used for SIMNET applications, is the closest to meeting DIS requirements but has not been standardized. Multicast is one requirement that cannot be met today by using a GOSIP compliant stack since GOSIP currently contains no multicast protocols.

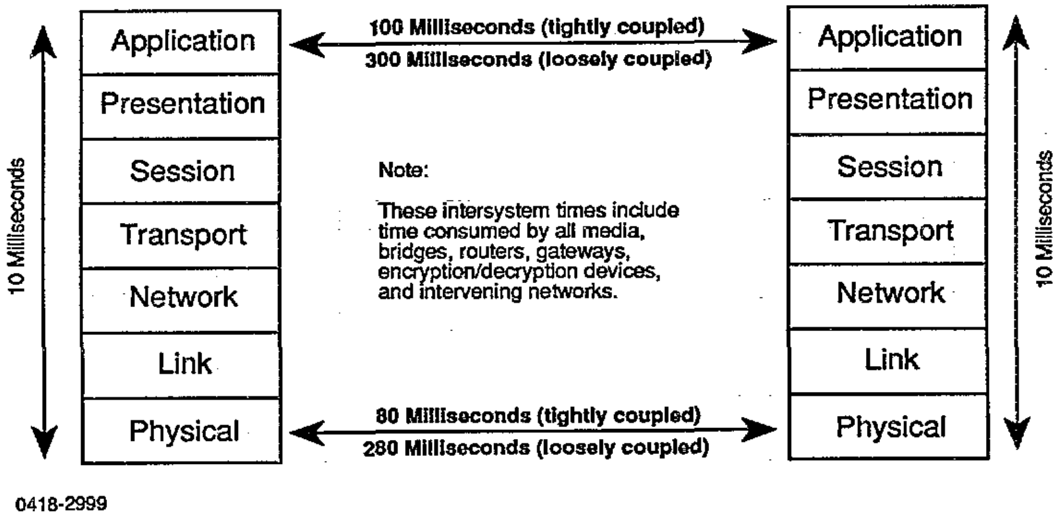
Application
Presentation
Session
Transport
Network
Link
Physical
10 Milliseconds
100 Milliseconds (tightly coupled)
300 Milliseconds (loosely coupled)
80 Milliseconds (tightly coupled)
280 Milliseconds (loosely coupled)
Note:
These intersystem times include time consumed by all media, bridges, routers, gateways, encryption/decryption devices, and intervening networks.
0418-2999

Figure 1. Standard Latency Values

Reliability versus Best Effort. A reliable communication service is one in which the number and type of errors that the user finds in the data is acceptable for the application. Reliable communication may require specific mechanisms in order to achieve the user's requirements, i.e. error detection and correction of PDU errors such as bit errors, duplicated PDUs, missing PDUs, or out-of-sequence PDUs.

The communication architecture desired for DIS must be generally reliable, with a low bit error rate and minimal discarding of messages as a means of flow or congestion control. Requirements such as flow and congestion control are largely dependent on network design and the protocols chosen. "Low loss," not "no loss", communication support is sufficient for the real time transfer of data throughout the system. Similarly, in-order packet delivery is desirable to avoid anomalous behavior in the DIS entities. Currently, no protocol exists that provides real time service, and is totally reliable. Therefore, protocols are sought that provide the "best effort" in a balance between these two requirements.

Information Types

Communication between DIS entities will occur via PDUs, as stated earlier. The network that is used to transport the PDUs will also transport other types of information. This information may be bulk video packets, voice packets, terrain databases, entity models, and simulation management information.

When a DIS exercise begins, those entities participating in the exercise must be coordinated. This is the responsibility of the simulation management PDUs. Initializing a system may require sending models of the entities that are participating in the exercise, sending the terrain database to be used for the exercise, and sending time synchronizing information. The databases and entity models should be transported in the form of bulk data. If another DIS exercise is occurring at the same time, would the bulk transfer of a terrain database interrupt or delay PDUs from the other exercise? Transporting video information is a similar situation.

When "voice" data messages are introduced to the mix of traffic, another dimension of performance becomes important. To be able to collect together and replay continuous voice messages, the inter-message dispersion in time of the individual parts can not be degraded too much. Current experience in this area suggests that an initial target for effective communication of continuous speech is inter-message dispersion of less than 50 milliseconds. (The estimated range for this parameter is actually thought to be between 20 and 50 milliseconds. More work is needed to refine this requirement.) Because this is less than the defined real-time threshold stated above for the PDUs, a conflict in priorities for different data types may occur. Investigations of multiple data types for DIS need to be performed.

SECURITY

The issue of security for DIS applications is not simple. DIS has the potential to be international in scope, and should support multi-level and multinational data. This will require security issues to be addressed up front, starting with the security needs of the United States military, who will be the initial primary users of DIS. Each branch of the military has different security needs in terms of the information that will be put onto the network for DIS exercises. How to accommodate all of these needs is the crux for implementing security into the DIS substructure of the communication architecture.

Requirements and Applications

The ten PDUs that are standardized today are nonclassified and very general in the types of data they represent. For a simulator to send these across the network initially poses no problem. The difficulty comes when the movements or actions of the entities represented are sensitive, thus creating the need for a secure exercise. This **confidentiality requirement** can be met through the use of encryption devices and security protocols.

The potential for running concurrent exercises of differing levels of security is one of the most difficult issues to address. Implementation of MultiLevel Security (MLS) will depend upon the availability of MLS systems that have been approved for use in DIS.

Authentication of DIS participants is another security issue that must be resolved. For any secure exercise, it will be necessary to verify that all participants are who they say they are. Identification of entities may occur at various levels; the network host computer, the user level, and the individual process. Encryption is one method used to provide authentication through the use of issued encryption keys. A centralized key management facility for DIS will be needed to provide these keys.

Data Integrity is the need to insure that the data transmitted during DIS exercises is not corrupted, deliberately or by accident. Error handling mechanisms, such as checksum, are used to verify the detection and correction of corrupted data as it passes through the network. Cryptography implementations can also provide integrity verification.

A critical facility to have for any secure system, including networks, is an **audit facility.** The audit facility maintains logs of security-relevant events in tamper-proof, restricted access locations. Typical examples of logged events include attempted logins and access to critical data. For DIS, each secure exercise should have an audit trail of who participated, for how long, and through data logging, what they contributed to the exercise.

The last security issue to be discussed here is that of **physical security.** This type of security is outside the scope of the communication architecture, however, components of the network as well as security devices must be physically secure to accommodate secure DIS exercises. Also included is the validation of personnel who will have access to this equipment. These security measures must follow the requirements of national security publications and direction from the National Security Agency (NSA). Secure DIS exercises must therefore be setup and adhere to these requirements.

DISSIMILAR SYSTEMS

Dissimilar Systems are defined as those devices which do not currently use or implement DIS PDUs. These may be simulators which communicate via a different protocol, i.e. the SIMNET simulators, or ones which were never intended to be used in an interactive networked environment. In order to allow these devices to participate in a DIS exercise, some conversion hardware and/or software must be created to allow the device to interface with DIS entities.

Defining The Interface

For obvious reasons, creating the interface between the dissimilar systems and DIS will be completed on a case per case basis since most systems were developed independently. From a communications architecture point of view, the standard for communication architecture can define the interface that the system can use for conversion and connection to a DIS network. While the DIS side of the interface will be the same for all systems, the system side will be particular to that system.

Application Gateways

An application gateway is a device that will provide the dissimilar system with a connection/protocol conversion to DIS. Attempts have been made to create generic application gateways so that changing a few parameters would provide for the conversion. With the multitude of devices that now need to participate in DIS exercises, a generic approach is desired. However, due to the independent development of these systems, a generic approach is unlikely except in a few cases. The Strawman DIS Architecture Description Document created by Loral [4] contains a high level approach for creating and integrating dissimilar systems through the use of a Cell Adaptor Unit (CAU). This may be the best approach to use for connecting dissimilar systems.

USE OF EXISTING STANDARDS

The most important goal for the DIS communication architecture is to achieve interoperability on a world wide scale. To accomplish this, the communication architecture must use standards in all possible cases to meet the service requirements outlined previously.

Existing Standards

In the process of deciding which standards to use, all existing standards must be judged against the requirements. Those standards that meet the requirements will be considered for specification. Future applications of DIS must also be part of this consideration.

One set of protocols being considered is the suite of protocols specified by GOSIP. These protocols are standardized, have several implementations, and are currently being used by government and industry. The OSI protocol suite has also been supported by the European community for many years.

Another set of protocols under consideration is the *Internet* protocols. These protocols have been in use on the Internet for several years, are available from many vendors and are used world wide.

Where Requirements Are Not Met

For current DIS applications, the number of entities participating in an exercise will be in the hundreds and communication occurs mostly over local area networks (LANs). Industry reports conclude that the current implementations of OSI protocols are *not fast enough to meet the real-time requirements* of DIS over local area networks.

Another area in which requirements are not met is multicasting, as shown in section 2.2.2. The DIS community will need to advance multicast protocols or changes to existing protocols through the standards bodies (ISO, American National Standards Institute (ANSI), and CCITT) so that DIS applications will be provided with the services required for large number entity exercises.

NIST Security Protocols

The Secure Data Network System (SDNS)[5] architecture was developed through a project sponsored by the National Security Agency as a basis for standardization of security services in the OSI architecture. This specification is published as a standard by the National Institute of Standard and Technology. These standards cover the three areas: security protocols, key management, and access control. The security protocols, Security Protocol 3 (SP3) and Security Protocol 4 (SP4) are defined to be used in layers 3 and 4 of the OSI stack. These protocols are heavily dependent on cryptographic management and access control service. These standard protocols and security mechanisms will eventually be included in the communications architecture for DIS when security for DIS has been more defined.

6. CASS APPROACH FOR COMMUNICATION ARCHITECTURE

The CASS has proposed a phased approach for *the implementation of a DIS GOSIP compliant* communication architecture. The interim architecture is based on the UDP/IP protocol, chosen based on product availability and interoperability of various vendors' versions. A migration from UDP/IP protocols to the OSI protocols will occur as they are standardized, tested and developed. This approach, designed to be accomplished in three phases, is described in more detail in the CADIS document [1].

CONCLUSIONS

The issues presented in this paper were those that have been discussed at the DIS standards workshops, specifically in the Communication / Architecture Security Subgroup (CASS) meetings. The CASS is working to resolve these issues by specifying standards to be used for communication architecture whenever possible. The progression toward GOSIP is one indication of this. As the standard evolves and technology evolves, these issues will be resolved, and interim solutions found. Because of the present dynamic nature of DIS and technology in general, new issues for communication architecture as related to DIS will continually surface. This is just the beginning.

ACKNOWLEDGEMENTS

This paper has been supported by the U.S. Army's Simulation Training and Instrumentation Command (STRICOM) under contract N61339-91-C-0091.

REFERENCES

[1] Communication Architecture for DIS (CADIS), Draft Standard, March 1992.

[2] Distributed Interactive Simulation Operational Concept, IST, February 1992.

[3] International Standard. Information processing systems - Open Systems Interconnection - Basic Reference Model. ISO, October 1984, ISO 7498-1984 (E)

[4] Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols, US Dept. of Commerce, February 1990, NISTIR 90-4250.

[5] Strawman Distributed Interactive Simulation Architecture Description Document, Volume I, Summary Description, Loral Systems Company, ADST Program Office, March 31 1992.