APPLICATION OF ARTIFICIAL INTELLIGENCE TO THE DOD DIRECTORY

David Gaon
Defense Information Systems Agency, Arlington, VA

Ruth E. Lang
John D. Lowrance
Philip R. Cohen
SRI International, Menlo Park, CA

ABSTRACT

The Department of Defense (DoD) is planning for the implementation of a DoD Directory capability based on CCITT Recommendations X.500-X.521, which define the Data Communication Networks Directory. The functional and operational requirements that define the DoD Directory will yield a system with a significant level of complexity. Problems and barriers which impede progress toward the envisioned DoD Directory service exist. This paper describes these problems and the artificial intelligence-based approach developed to solve and reduce them in order to achieve a usable, capable, secure, and manageable DoD Directory service.

1. INTRODUCTION

The Department of Defense (DoD) is planning for the implementation of a DoD Directory capability based on CCITT Recommendations X.500-X.521, which define the Data Communication Networks Directory [1]. The DoD Directory will be comprised of:

- The DoD information held by the Directory which is collectively known as the Directory Information Base (DIB). When the hierarchical structure of the data is important, the DIB will be referred to as the Directory Information Tree (DIT).
- A collection of Directory System Agent (DSA) application programs which provide access to the DIB.
- Directory User Agent (DUA) application programs which provide access to the Directory by DoD users.

The functional and operational requirements that define the DoD Directory [2] will yield a system with a significant level of complexity. Realizing this, the Defense Information Systems Agency (DISA) has identified the relevance of artificial intelligence (AI) technologies to solving problems and reducing barriers that impede progress toward the envisioned DoD Directory service. Four particular areas with known and/or with potential problems have been identified by DISA and form the basis of our research and this paper. They are characterized as follows.

User Interfaces. The DoD requires that a common user-friendly interface be available for DoD Directory operations. Significant challenges exist in devising DUA interfaces that can support the range of DoD users' skills, on the variety of hardware available, and using a diverse set of access capabilities and still meet the usability and performance requirements set by the DoD.

The amount and variety of information to be contained in the DoD Directory is expected to be large, and the organization of the DIT may not be obvious to users. Despite these factors, interfaces must not be cumbersome or confusing to use. Users need an interface that makes it easy to enter enough distinguishing details to find desired entries, assists them by detecting or correcting typographical and obvious errors, and guides the construction of queries and updates such that DoD Directory and network resources are efficiently used.

Directory Management. The management structure of the DoD Directory will be modeled after the network management capability of the Defense Communications System and will feature a hierarchy of management and control centers. DoD Directory management responsibilities will include configuration, fault, performance, security, and accounting management. Developing cost-effective, easy-to-use tools that assist managers in planning, embody management policies and procedures, and accommodate both local and DoD Directory-wide concerns will be a significant challenge. These tools must balance the need to expend both DoD Directory and network resources to perform monitoring or management functions and to satisfy user requests.

Distributed Operations. The DIB for the DoD Directory will be distributed across a collection of hierarchically organized DSAs. Effective contextual replication of data, knowledge references, and information regarding the set of operations supported by a DSA is key in minimizing costly distributed Directory operations that are employed to locate authoritative stores of information and provide a timely response to the user.

To support DoD query and replication performance requirements, a broad view of the capability and current capacity of the DoD Directory is needed. This information must be obtained with negligible resource impact on the DoD Directory. In addition, cache management strategies and algorithms based on expected and actual usage patterns are needed in order to optimize resources utilized to obtain data from remote DSAs.

Secure Operations. The DoD DIB will contain both classified (up to the SECRET level) and unclassified information. Although strong authentication mechanisms may provide a sufficient firewall for most attempts, spoofing, unauthorized methods of access or update, and aggregation of data are likely.

If the presence or absence of certain behaviors, including patterns of DoD Directory usage, are visible to uncleared users (e.g., withholding portions of request results), inferences about the presence or absence of classified information, or even its value, may be possible. In addition, although the DoD requires that local caches be managed in such a way as to protect the contents as is done in the DoD Directory, lack of control of the caching of certain types of data without the ability to apply collective access policies or restrictions may open the door to compromise.

Our goal for each of these areas has been to identify methods to mitigate or eliminate problems that will delay or prohibit the introduction of an effective DoD Directory service based on X.500. The rest of this paper presents a description of a candidate approach for the application of AI technologies to these four problem areas, and outlines a development strategy that can be used for the infusion of these technologies into an operational DoD Directory system.

2. CANDIDATE APPROACH FOR AI TECHNOLOGY APPLICATION

A recommended style of interaction for the DUA interface, and a functional model for posing question and modification requests that employs AI technologies is described here. The use of adjunct tools that are related but separate and distinct from both the DUA and DSA are suggested for enhancing the ability of DoD Directory managers and the capability of distributed and secure operation. Although the DSA would also benefit from the application of AI techniques, we have deferred making recommendations in this area because:

- New recommendations regarding data and knowledge replication are expected in the 1992 version of the standard. These additions along with other changes and improvements may present a significantly different set of distributed operation and management problems than those identified to date.
- Information generated by the user is knowledge and context rich whereas information exchanged between DUA and DSA and between DSAs is knowledge and context poor. By focusing the application of AI technologies at a level where knowledge and context information is most readily available (at the DUA), a notable impact on perceived end-user functionality can be made. This impact is expected to reveal additional insight into the need for AI technologies to improve overall DoD Directory functionality.

2.1 Style of Interaction

A multimodal user interface will allow users to employ whatever modalities[1] of interaction are supported by their computing equipment, which is expected to range from simple terminals to X-terminals, PCs, pen-based computers, and powerful workstations. Many will come equipped with a high-quality microphone and digital signal-processing capabilities. Users will employ query-by-reformulation problem-solving techniques to access information in the DoD Directory and will interact with it using direct manipulation interfaces that combine typed, handwritten, and/or spoken natural language. The user should employ a direct manipulation style of interaction whenever possible. When other modalities are more appropriate, they can be invoked.

The combination of direct manipulation with natural language will enable DoD Directory users to sidestep limitations of user interfaces based on direct manipulation techniques alone [3]. These limitations include the inability to effectively identify objects not on the screen, specify temporal relationships, identify and operate on large sets and subsets of entities, or use the context of interaction. English, or any other natural language, provides a set of finely honed descriptive tools such as the use of noun phrases for identifying objects, verb phrases for identifying events, and tenses for describing time periods.

2.2 Question/Modification Request Support

The functional model diagramed in Figure 1 would be used to support either an end-user or DoD Directory manager in performing question or modification requests. In this context, we differentiate questions and modification requests that are high-level expressions of the user's intent from low-level queries and updates that are abstract service requests for X.500 services. In the text below, references to processes, data items, and user input devices depicted in the diagram appear in italics. This facilitates correlating the diagram with the following paragraphs.

The user selects among a set of *templates* tailored to different prototypical questions and modifications so that each is well-suited to an individual's job role or security clearance level. The *templates* will be composed of attribute-value slots. Defaults for attributes and constraints on values will be used to guide user input. By employing defaults and constraints, slots will offer more functionality than a simple form or tabular presentation. As is typical of query-by-reformulation interfaces, a user will formulate questions and modification requests for access to or modification of DoD Directory information by selecting values to fill into a slot from a short menu.

A generalized *Parser/Interpreter* would map the slot and its filler information into an expression in the internal knowledge representation language—that is, it would generate the *slot interpretation.* The user who does not know precisely the value to enter or select, can enter (via *keyboard, mouse, microphone,* or *pen*) a simple or full English noun phrase. Phrases entered would be translated by the *Parser/Interpreter* into the knowledge representation language. The *Parser/Interpreter* would draw on a *grammar* of English, augmented by knowledge of typical ungrammatical ways that users enter information, and a *lexicon* tied to the slot and filler information as well as the *DoD Directory knowledge base* (composed of the *user model,* and *constraint, default, and security knowledge*) to analyze the user input. Synonyms for both attributes and values would be represented in the *lexicon,* and a means would be supplied for individual users to augment the standard *lexicon* with their own synonyms and acronyms.

Each interpreted slot would be input to the *Question/Modification Assembler,* which incrementally formulates questions and modification requests. The *Question/Modification Assembler* applies the *DoD Directory knowledge base* and updates the *template* accordingly to offer restrictive information. For example, if the user selected "7th Infantry Division (light)" from a menu as the organizational unit, the *Question/Modification Assembler* might enter "Ft. Ord, California" into the localityName field of the *template.* In addition, constraint checking could take place so that the user would be notified immediately of violations.

At some point, the *template* would be sufficiently complete that a question or modification request could be composed. If told to formulate a query, the *Question/Modification Assembler* would attempt to unify the slot expressions into a complete query with quantifiers and default information. If successful, it would create an *initial question/modification,* which would serve as input to the *Query/Update Planner.*

The *Query/Update Planner* will generate a plan of retrieval or update and execute it. Reactive planning procedures will be used as the basis for both the initial assembly and the plan generation. To handle unanticipated or more complex requests, generative planning techniques should be applied in place of the reactive planning techniques.

Before the plan is executed, the intent of the question or modification must be inferred from the *initial question/modification* generated based on a partially filled out *template.* To infer intent properly, information in the *DoD Directory knowledge base* must be considered. Procedures will be defined beforehand that correspond to different *templates* in various states of completeness. Each such procedure would outline the steps needed to determine the appropriate response. These steps would be sensitive to portions of the environmental knowledge—for example, the *user's model* might be used to determine how various *templates* should be interpreted. The *Query/Update Planner* would use this knowledge to determine

[1] In light of current industry marketing jargon, it is worth briefly distinguishing *multimedia* from *multimodal.* Whereas the term *media* is generally used to focus on the production, storage, and transmission of signals, the term *modality* is used here to concentrate on the syntactic, semantic, and pragmatic properties of those signals.

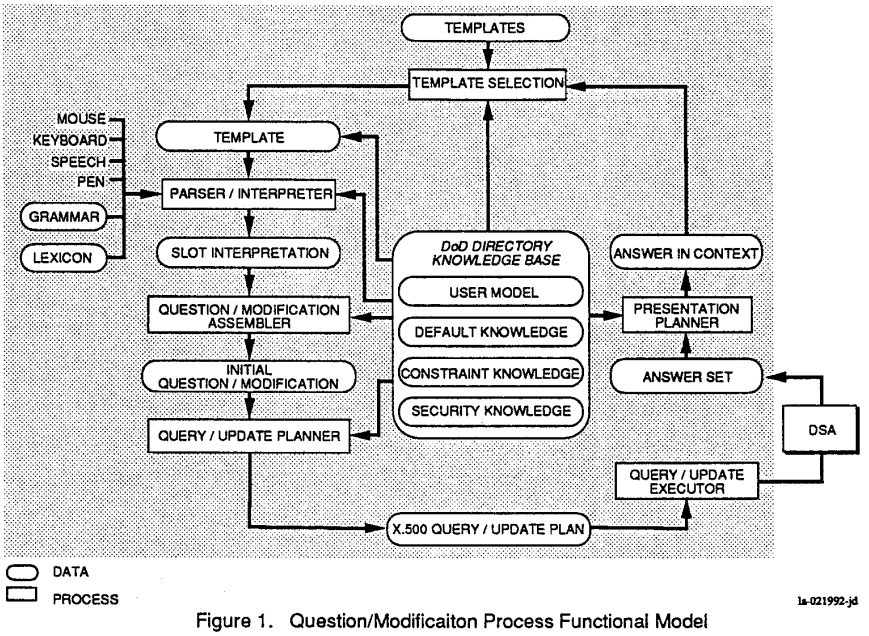

Figure 1. Question/Modificaiton Process Functional Model

the intended question or modification, and the fundamental subgoals that need to be achieved to effect an appropriate response (i.e., identify a general plan to execute among the set of predefined plans).

The Query/*Update Planner* will convert this general plan into a specific *X.500 query/update plan*. This is a compilation task where an abstract specification of a procedure is converted into a detailed sequence of lower-level operations that can be directly executed. The conversion will be based on a set of pre-specified procedures for reducing interrelated question and modification goals to sequences of X.500 protocol operations. The procedures will need to be sensitive to environmental conditions pertaining to the anticipated number of answers to each query so that the procedures can be optimally ordered to improve performance. In addition, information pertaining to the anticipated network load and the available resources for responding to information requests need to be taken into account to formulate an effective plan. Frequently used multi-step queries and updates can be captured as procedures for immediate application, obviating the need for planning based upon more primitive procedures. The successive application of these procedures at more and more detailed levels will result in the formation of an overall plan. The overall *X.500 query/update plan* will drive interaction between the *Query/Update Executor* and a *DSA*.

Once the *answer set* has been retrieved, the *Presentation Planner* will reason about how best to present that information to the user. One option would be to display a collection of forms, one for each entity returned. If the *Presentation Planner* determined, based on the user's preferences and display characteristics, that the returned information was too voluminous to display properly, a message to that effect would be printed. Other methods of presentation, such as tables, would be used when appropriate.

After receiving a set of answers, the user may wish to refine the query by entering new information into some of the slots. In addition, the user may be given the opportunity to ask a complete English question to restrict the retrieved answers further, which would allow the user to incorporate more than just attribute-value information, perhaps adding ternary and higher-order relationships. Just as is implicit with the further addition of refining information into *templates*, these follow-up questions will use the context of prior questions either by caching the answers to a previous question, or by unifying prior queries with the meaning of the current ones. Finally, the process of presenting the *answers in context* could also add information to the question *templates*.

2.3 Directory Management Support

Whenever a job requires the DoD Directory Manager to query or update the DIT, the same functional interaction as depicted in Figure 1 would be employed, but with templates, knowledge, and predefined plans specific to configuration, fault, performance security, and accounting management. In addition, two types of tools will be needed that are distinct from those supporting the question/modification request process. The first type are tools that would be used in advance of end-user access to the DoD Directory and would aid in the task of defining the DoD Directory structure, security policies, etc. An example tool that could be used to assist a DoD Directory Security Manager is described in the following paragraph. The second type are tools that would run continuously during DoD Directory operation to ensure effective distributed and secure operation of the DoD Directory, and provide a user interface for managers to analyze or solve problems as needed. Because monitoring and problem detection is primary and manager interaction is secondary for these tools, they will be further described in Section 2.4.

The templates referenced in Figure 1 will control access by restricting the types of question and modification requests that can be posed. For example, certain subdirectories, certain attributes, certain values of attributes, or certain aggregates may be prohibited. Such restrictions could be imposed user by user or group by group. A planning tool or reasoning tool would be used to analyze the set of allowable questions or predicates to ensure that sensitive or disallowed information could not be obtained through their repeated or successive use. This type of analysis would be performed in advance of DoD Directory use—

that is, when the templates are being defined—so that needed restrictions can be integrated into the templates themselves.

2.4 Distributed and Secure Operations Support

AI technologies can be used to enhance some of the more continuous and operational aspects of the DoD Directory. Processes that are separate from the DSA and DUA can be used to monitor and detect problems with distributed and secure operations. If anomalies are discovered, the process can alert the human user that a problem may exist, provide advise on how the problem may be corrected, or additionally take action to correct the problem without human intervention. Although separate, this capability could enhance the overall performance of DSAs and the DoD Directory as a whole. Two examples of these continuously operating adjunct tools are described here.

A tool that employs uncertain reasoning techniques may be used to continually assess potential performance and fault problems of the DoD Directory. Observable events such as the failure of a distributed operation or slow response from a remote DSA would be logged. A collection of these observable events would then be related to a potential set of problems. Because each performance problem can be probabilistically associated with some set of observable events, the observed events can serve as evidence of the problem [4]. Uncertain reasoning can be used on the set of observed events and arrive at a consensus that identifies the cause of the problem. Given this assessment of poor performance, both reactive and generative planning can be employed to determine an appropriate response to correct the problem(s). If the collection of diagnostic and repair procedures (i.e., procedural knowledge) can be defined and described as is done in an operator's manual for maintaining the DoD Directory, then the generative or reactive planning technologies can be used to apply this procedural knowledge automatically as appropriate.

An intrusion detection tool based on rule-based expert system technology could aid the task of detecting suspicious or undesired user activity [5]. Information about known DoD Directory vulnerabilities and about possible intrusion scenarios would be encoded in rules and used to determine whether a user's actions constituted an intrusion. Data collected at the highest system levels are the most useful for detecting suspicious events and inferring malicious or benign user intent. The rule-based expert system tool would be used to examine this data after the user's request is satisfied, and therefore would not impede end-user performance. Results of the analysis performed by this tool could subsequently be used by a DoD Directory Security Manager to conduct debriefing or investigative activities.

3. SUGGESTED DEVELOPMENT STRATEGY

As described in [2], the DoD Directory will be deployed to the DoD user community in two phases. An Initial Operating Capability (IOC) is planned for 1995 and the Final Operating Capability (FOC) is planned for 2000. The interface, functional model of the question/modification process, and adjunct support tools described in Section 2 can be implemented using more than one type of AI technology. This flexibility can be used to the advantage of the DoD user community to make DoD Directory capabilities based on AI technologies available at both IOC and FOC. Table 1 summarizes a two-phased approach for assimilating AI technologies into DoD Directory implementation. Those technologies listed under Phase 1 are those that can be applied directly to the candidate approach described in Section 2, and will make a significant impact on the capability of IOC or FOC fielded systems while not requiring excessive technology development investment to yield positive results. Phase 2 technologies hold promise for improving the capability of the DoD Directory at FOC, but will require an investment in research and development to ensure their applicability to the DoD Directory.

Table 1. Phases of Technology Deployment

Problem Area	AI Technology and Application	Phase 1	Phase 2
User Interfaces	Object-oriented knowledge bases for templates	X	
	Query-by-reformulation for results refinement	X	
	Typed natural language for filling in templates	X	X
	Spoken and handwritten natural language for filling in forms		X
	Reactive planning and control for presentation planning	X	X
	User modeling for customization		X
Directory Management	Reactive planning and control for distribution management, fault detection, and isolation correction	X	
	Uncertain reasoning for fault/performance detection, and fault isolation		X
	Reactive and generative planning for configuration management, and corrective action determination and automation		X
Distributed Operations	Reactive planning and control for filtering, simple query planning, and multistep query/update planning	X	X
	Generative planning for query/update planning, and distribution planning		X
Secure Operations	Rule-based expert systems for intrusion detection	X	
	Reactive planning for determining access control and restriction	X	
	Uncertain reasoning for intrusion detection, inference detection and correction, and access control and restriction		X

4. SUMMARY AND CONCLUSIONS

The style of interaction, functional model of the question/modification process, and use of adjunct tools to augment DUA and DSA functionality presented in Section 2 provides a unique approach to the problems associated withthe DoD Directory. The use of templates comprising slots accessed through multimodal interaction will not only provide an interface that is as easy to use as a simple form or tabular interface, but provides a higher level of abstraction for obtaining DoD Directory services that enables users to obtain information when they do not know what attributes and values to select. The use of this high-level abstraction in combination with observed information regarding the status of the DoD Directory will enable planning programs to generate an efficient query or update that conserves DoD Directory resources. In addition, the high-level information when combined with information regarding the context of the user's interaction can be used to uncover security violations more quickly and effectively.

Applying AI technologies to resolve the problems that affect offering a DoD Directory capability that meets DoD requirements is both valid and advisable. AI use should be considered as part of each phase of planning, designing, and developing the DoD Directory. Because AI-based technologies will directly impact the finalization of DoD Directory requirements, the development of an architecture, the design of the schema and DIT, the development of security policies, and so on, they must not be considered "add-on" capabilities to be substituted for non-AI-based technologies when a need or problem arises. Use of AI technologies to the exclusion of other technologies is not advocated, but their use in prudent combination with non-AI-based technologies is advised.

5. ACKNOWLEDGMENTS

Research at SRI International was supported by the Defense Information Systems Agency under contract DCA100-91-C-0032 [6]. Preparation of this paper was supported by SRI International. Contributions made by Teresa F. Lunt in the area of Directory security are gratefully acknowledged by the authors.

6. REFERENCES

1. "Data Communication Networks Directory, Recommendations X.500-X.521," The International Telegraph and Telephone Consultative Committee, November 1988.
2. Defense Information Systems Agency, "Concept for Integrated DoD Directory Services," Washington, D.C., November 27, 1991.
3. Cohen, P.R., "The Role of Natural Language in a Multimodal Interface," Proceedings of the Friend21 International Symposium on Next Generation Human Interfaces, Tokyo, Japan, November 1991.
4. Lowrance, J.D., T.D. Garvey, and T.M. Strat, "A Framework for Evidential-Reasoning Systems," in G. Shafer and J. Pearl, eds., *Readings in Uncertain Reasoning*, Morgan Kaufmann Publishers, Inc. San Mateo, CA, 1990, pp. 611-618.
5. Lunt, T.F., "An Intelligent System for Detecting Intruders," Proceedings of the Symposium: Computer Security, Threat and Counter-measures, Rome, Italy, November 1990.
6. Lang, R.E., J.D. Lowrance, P.R. Cohen, and T.F. Lurt, "A Study in the Application of Artificial Intelligence Technology to the DoD Directory," Draft Final Report, Project 2808, SRI International, Menlo Park, CA, February 1992.