VIRTUAL NETWORK REPRESENTATIONS OF INFORMATION WARFARE BATTLESPACE

Kenneth Y. Jo
John T. Dockery
Defense Information Systems Agency
Arlington, VA 22204

ABSTRACT

Virtual network methodologies are applied to information warfare (IW) simulation in which objects and agents behave with special relationships. Decision makers operate in a virtual battlespace, which is in essence an information cyberspace in which IW attacks damage assessments, countermeasure efforts, and repairs are interrelated through virtual networks. The virtual network representation is used to model not only communications networks but also socio-technical networks with dynamic, hyperactive characteristics. Different virtual network representations are realized to characterize various behaviors and to help generate associated performance measures. Communications network attacks will constitute a major source of IW activities that will be analyzed. Virtual networks are used to represent object behaviors with appropriate levels of abstraction depending on IW scenarios and problem domains.

1. INTRODUCTION

Virtual network techniques are applied to information warfare (IW) object-oriented simulation to provide a suitable framework for object communication and collaboration. The virtual networks will not only interrelate objects for their collaboration during simulation but also provide communications means if information needs to be transferred during object interactions. Conventional analysis of communication networks focuses on the local properties of the physical systems involved. Going beyond the scope of conventional analysis, this paper extends the role of virtual networks to the total simulation of object behaviors in modern information warfare operations.

The Defense Information Systems Agency (DISA) essentially has a defensive interest in IW through its role as the lead agency in the Department of Defense (DOD) for maintaining the communications infrastructure for government information assurance and security operations. In order to defend its networks, DISA will baseline the information carrying properties of the communications networks it designs. Next, DISA will detect network anomalies that indicate the presence of IW, diagnose the type of the IW attack and methods (e.g., jamming of communications channels or information insertion via a virus), diagnose the seriousness of the attack relative to a network's ability to support operational decisions, and remediate the IW attack through the design/selection and implementation of countermeasures. To aid the implementation of such tasks, IW simulation models are being developed by DISA.

Modern C4I operations cover all aspects of IW operations. Virtual networks can demonstrate where particular network topologies are used to correlate with particular communications and decision processes in command and control environments. In IW simulations, broker objects initiate and dictate IW activities so that their agents and other involved objects will be brought into the domain. Virtual networks will then provide a framework in which objects collaborate among themselves and information needs to be transported. A virtual network transforms objects into a new problem domain but preserves their inherent system and functional characteristics.

Information flows resulting from IW activities give rise to virtual network response times, also called response surface times, as they pass through physical network media and entities. These virtual connections will be linking all objects during IW simulation. It has been known to be difficult to diagnose IW attacks on even moderately sized battlefield networks. Even definitions of normal behavior play multiple roles in diagnosis. They set conditions for triggering diagnostic processes, establish bounds for the construction of explanatory hypotheses, and provide criteria for determining the value of evidence. Significant uncertainty in any of these areas provides an opportunity for an adversary to exercise control over both operational users by managing their perception of information flows, steering them towards interpretations of the network situation that are ultimately disadvantageous. Thus, complex battlefield networks provide an ideal environment for an adversary to exercise reflexive control over its opponent.

The DISA IW model is federated with joint exercise models through a runtime infrastructure for collaborative simulation. The model will run in the federated environment as defined by the High Level Architecture (HLA) and as mandated.
by the Joint Technical Architecture (JTA) (cf. [6] and [7]). The rationale for using such architecture frameworks is to access other simulation models with different functional and mission applications and to save computation runtime and modeling resources. The IW model will be specifically used to assess the effectiveness of present and future IW doctrine, operations, scenarios, and strategies. Another objective of the model is to train the users in assessing the impact of IW attacks on the information infrastructure particularly on networks and databases. The model will also teach the users how to counter various IW attacks and minimize damages.

2. IW SIMULATION MODEL VIA VIRTUAL NETWORK

All activities in IW simulation will be modeled by opening up specific virtual networks. These virtual networks can be communications networks, socio-technical networks, and C2 networks. The domain of each virtual network will vary depending on the objects, perception, or problem domain. True system or network states as well as perceived states can be visualized by displaying respective virtual networks.

Objects and agents can initiate events which will be queued and scheduled for target server objects within the hierarchy of virtual network domains. High level interactions or mechanisms involving end user objects are appropriate for high-level, coarse analysis. Lower level interactions will cover detailed local object activities without being directly related to the ongoing high-level missions and activities. Virtual network representations relate these high and lower level interactions with appropriate mappings and also assist in computing performance measures by exploiting structured, redimensioned problem domains. Figure 2 shows an example which illustrates the interrelationships of network objects and agents during an IW simulation and defines several virtual network domains.

The names and properties of IW objects can be transformed from an object structure into a virtual network structure by changing from an n-dimensional space to another n-dimensional space:

\[ y = R(x) \]  (1)

where \( R \) is a mapping which transforms entities into entities with other identities and a new set of attributes. Semantic, syntactic, and programmatic relationships of semiotic types are considered to define mapping between logical domains of different virtual networks. In addition, the q-analysis techniques (see [1] and [2]) are used to convert an object network into an abstracted virtual network representing the command and intelligence structure suitable for analysis by simulation. The q-analysis, which has been shown to be isomorphic to graph theory, and its associated metrics will also be applied to the detection and evaluation of the effects of IW.

The network intrusion detector (NID) is a suite of software tools employed by DISA that help detect, analyze, and gather evidence of intrusive behavior occurring on premises networks. The NID operates within a security domain, a collection of hosts to be protected. The domain can be either a subset of a network or the entire network to which NID is directly connected. The NID also complements a firewall system by providing a sniffer capability to monitor network traffic, and to determine if firewall filters are functioning properly. The network can exercise several types of control actions to remediate the damage caused by IW attackers. Such actions can be admission, routing, flow control, and allocations of bandwidth.

Every layer of the ISO protocol stack will contribute to network security. In the physical layer, protection against wire tapping can be installed. In the data link layer, link encryption can be added. In the network layer firewalls can be installed. At the transport layer, there exist elements of electronic warfare, destruction of nodes, and manipulation of the electronic data. In the transport layer, an entire connection can be encrypted end to end, that is, process to process. To handle issues such as authentication and nonrepudiation, the solutions must be present in the application layer. The IW simulation layer is one of the applications. The simulation architecture is being constructed within the HLA framework in which all simulation functions and object interactions are processed. Such a simulation architecture will be constructed by adapting the top three higher layers of the ISO. Here, the hierarchy has added the simulation layers since IW could conceivably capture the sensory equipment and replace it with a simulation.

During network operation, the user can damage networks and objects within each network as desired. A set of objects such as IW attackers will be created during simulation while other objects necessary can be optionally generated. The IW model also provides a hierarchy of information-related attributes such as bits and bytes, characters, symbols, data information, perception, experience, wisdom, significance, etc. Since decision makers in general operate on "significant information," it is suggested that one can affect a vast swath of events if the significance criteria is changed. Actually, it is not necessary to change the basic information, only the weighting needs to be changed. As the quality of information changes, various virtual networks such as social networks, C2 networks, and communications networks will be introduced whenever appropriate. Figure 3 illustrates that different objects and agents will perceive different virtual networks.

![Figure 2. Interrelationships of IW Network Objects and Agents via Virtual Networks](image-url)
Figure 3. Virtual Networks Perceived by Different Objects.

The DISA IW model generates simulation results as output whenever the system state changes or upon request by the user. The virtual network model constantly updates its variables and parameters to provide the network characteristics as desired. The user will view current network workloads, delays, quantity and damage status at routers, brokers, muggers, missionaries, investigators, repairs, and network. In addition, the user will compare the true state with the state perceived by each object under simulation, and the course of actions resulting from such different sets of information will be analyzed.

3. OBJECT-ORIENTED IW NETWORK MODEL

The DISA IW model is supported by an agent-based architecture with diagnostic approaches. Virtual networks can link and interrelate various independent agents in operation at any given time. Each virtual network is comprised of a number of links that represent the relationships among objects and/or agents in the problem domain. Some of these links are of a communications nature. Links without any data communications are said to be "null" to distinguish them from conventional communications links. They can be hyperactive but may not carry any data traffic at times and can be created and destroyed as objects interact (see [4]). Both null and communications virtual links are considered. Null communications links will be used when an object sends a message to itself or others just to invoke an activity or send a wake-up call. The response time for null communications can be instantaneous.

When communications objects or agents are involved during simulation, virtual networks representing deployed communications networks will be brought in along with their inherent system characteristics that can be effective for the current activities. The main advantage of using virtual networks for IW simulation is that end-to-end connections are made among all objects rendering all complex details transparent. In addition, the response time that is state dependent can be effectively generated by examining only the virtual networks that are affected by current activities. Overall average response times will often be used as response surface times to aggregate the background traffic and domain-specific traffic. Detailed empirical statistics can also be used to attain more accuracy of the system performance.

Agents interact with other agents within locally restricted neighborhoods but within a virtual network domain. A regular C2 agent may employ different neighborhoods for different interactive functions. For example, an IW monitoring agent may define its attention neighborhood in terms of designated functions in the population of operations agents while it may employ neighborhoods defined over information flows when tracking a located information anomaly. Investigative agents (IAs) interact locally to generate an IW defense strategy. A broker object may act as the security for the router, being an inoculation or natural immunity against the IW attacker. The broker object also simulates the security or firewall protecting the router object. Muggers will delay an investigation or repair process. The role of a missionary object is to misdirect the investigation and/or repair process, enabling the IW attacker to cover fingerprint trails. An object model diagram specifies system structure by identifying object classes and their multiplicities, relationships and roles, and subclass relationships. An example of the object relationship diagram for the IW model is illustrated by Figure 4.

During IW simulation, the virtual network approach will keep track of simulation domain traffic and background traffic. For each node and link traffic volume will be produced. For each ongoing IW activity, it will compute the corresponding traffic flows, primary or secondary, for the assigned virtual path. The routing algorithm will then determine the best path using routing metrics. The selected path will be constrained by the network topology which will be changed dynamically. For each virtual path, it will compute or estimate the end-to-end response time through analysis, simulation, or empirical results. When the activity is completed, traffic flow in the virtual path will be released. At any given simulation time, the model will keep track of all ongoing activities in the main IW simulation domain.

Figure 4. High-level Object Interaction Diagram for IW
During IW simulations, objects will use a statechart, (i.e., state-transition diagram) to describe modal behaviors that can be different under various circumstances or in different modes. Thus, states can be viewed as abstract situations in an object’s life cycle or as temporary object invariants. Objects use statecharts to describe modal behaviors that can be different under different circumstances or modes (cf. [5]). Moreover, the model will generate delays and percentage errors as a function of the quantity and types of IO attackers. Real and ghost nodes will be generated, and different IW attack scenarios in varying intensity will be tested.

4. COMMUNICATIONS OBJECT SIMULATION

Methods for Virtual Networks

Procedures to handle information flows that are interchanged in the object-oriented IW simulation model are presented next. Virtual network consideration is key to this innovative concept. Moreover, simulation and analysis are mixed to produce accurate performance attributes using minimum possible run time. The virtual network consideration also conforms to modern asynchronous transfer mode (ATM) network technology. Virtual networks like ATM seek to combine the grains from intelligent multiplexing features of connectionless switching with guaranteed performance features provided by connection-oriented switching.

To model communications networks during IW simulation, network addresses have to be defined first via a Domain Name System (DNS). To map an entity name into a communication entity, DNS uses a library to transform the entity name into a network name. The communications model will then provide a capability to route demanded messages between objects or entities via communications media. Messages containing orders or reports are transmitted from a source node to a destination node. Virtual connections between those end nodes are established through links along the assigned paths.

Let $y_i^m(t)$ be the total demanded traffic rate of type $m$ from node $i$ to node $j$ at time $t$ and let $y_{ij}^m(t)$ be the total demanded traffic rate at time $t$ from node $i$ to node $j$, summing over $m$ from 1 to $M$. Let $y_{ij}(t)$ be 1 if a path from $i$ to $j$ uses link $a$ at time $t$ and 0 otherwise. The total information flow of type $m$ at node $a$ at time $t$, is given by

$$y_a(t) = \sum_{i,j} y_{ij}^m(t) \delta_{ij}(t)$$

(2)

Procedures to allocate demanded information workloads for a given virtual network and to compute performance attributes are next given.

a. Assign a network address to each communications entity depending on its network domain, function, and hardware type. The resultant network hierarchy can be much different from that of the IW main object model. Nodes belonging to different domains may have to be introduced to complete all virtual connections.

b. Links, either logical or physical, will be established between all node pairs representing different entities. For each link, its type, capacity, information flow level, and governing network/routing protocols will be specified.

c. Between the pair of end nodes for the current communications session, data will be flowing along the selected path until the session is finished. A virtual or dedicated path from the source to the destination node will be established (cf. Figure 5) to transport a given workload. For each node pair, incremental flows will be allocated according to their types or priorities while all demanded sessions are processed. For each demanded, incremental flow assignment, a routing algorithm decides the best path according to given routing metrics. The end-to-end response time can be computed either by analysis, simulation, or empirical results. Traffic in updating, managing, distributing messages and protocol overhead will also be considered.

d. For the demanded session for which a path cannot be assigned due to non-availability of bandwidth or resources, the session will be marked for subsequent attempts or will be discarded. If discarded, the blocking might have occurred somewhere in the network. The blocking probabilities can be dependent on the current network state.

e. Suitable bandwidth will be allocated to the current communications session. Depending on its type and applications, such allocation can be dedicated or arbitrarily set by the network manager. During the communications session, the allocated bandwidth will be used along the selected path from source to destination node. When the session is completed, the path will be freed up for subsequent use by other communications sessions.

f. Link and node utilization of the entire network will be continually updated as time progresses. The performance measures such as delays are direct consequences of the traffic flow levels at each node or link. The end-to-end communications delay is the sum of all components of nodes and links along a selected path. The reason that flows from source to destination nodes are incrementally assigned is to characterize realistic practices and to maximize the throughput. Overflows (i.e., unmet demands) will be identified if the network produces such results.

Let $R_k$ be the number of alternate virtual paths available in the routing matrix for traffic from source $i$ to destination $j$. Define $M_{ij}(k)$ to be the number of virtual links for the $k$th virtual path available from node $i$ to node $j$. If probabilistic routing is used, assign to path $k$, out of $R_k$ paths, for type $m$ traffic, probability $p_{ij}(k)$. Given $p_{ij}(k)$ and demanded traffic rate at source nodes, the input traffic rate into the $s$th link of path $k$, $\lambda_s$, can be determined by solving simple traffic flow equations. Let $P^m_s$ denote the mean delay at link $s$ for type $m$ traffic. Then the end-to-end response time from node $i$ to node $j$ for type $m$ traffic is

$$T^m = \sum_{k=1}^{R_k} p_{ij}(k) \sum_{s=1}^{M_{ij}(k)} (D^m_s + \alpha_s)$$

(3)

where $\alpha_s$ is the sum of node processing times, transmission delays, and propagation delays. Now, the traffic weighted average delay for type $m$ traffic, given the total aggregated traffic load $\Gamma^m$, is computed as

$$\Gamma^m = \sum_{i,j} \frac{\lambda_i}{\Gamma^m}$$

(4)
reliability of path (ij) for type m traffic, in networks. Among M different types, type 1 messages are handled by the IW virtual network. Acknowledgment messages will also be handled by the IW virtual network. In virtual networks, the grade of service will be measured in terms of the cell loss probability or information overflows for problems that are complex and numerically intractable. Virtual networks are key to the representation of object behaviors with appropriate levels of abstraction depending on IW scenarios and problem domains. Analytical approaches were introduced to aid simulation processes in representing network behaviors.

Virtual network representations were applied to characterize various behaviors and to generate associated performance measures for problems that are complex and numerically intractable. Virtual networks are key to the representation of object behaviors with appropriate levels of abstraction depending on IW scenarios and problem domains. Analytical approaches were introduced to aid simulation processes in representing network behaviors.

REFERENCES