Virtual Machine Applicability to Dynamic Coalitions

Lauren B. Eisenberg Davis and David V. Heinbuch
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723
USA

Lauren.Davis@jhuapl.edu, David.Heinbuch@jhuapl.edu

ABSTRACT

The Johns Hopkins University Applied Physics Laboratory has investigated the suitability of virtual machine technology for use in dynamic coalition networks. The remote creation and teardown of dynamic coalition networks among partners with different degrees of trustworthiness is a very desirable capability and poses a difficult challenge to implement. There are many issues to be addressed in developing such a coalition capability, especially considering the high degree of security that is required. Configuring, distributing, and managing virtual machines from a central location may provide a secure means to quickly deploy, maintain, and take down private networks among coalition members.

JHU/APL has also investigated operational requirements that, together, encompass a variety of possible coalition network applications, such as networking among allied partners for military operations, dynamic collaboration of civilian partners, or coordinated large-scale system testing among multiple international organizations. For any particular application, only a subset of the requirements might apply.

This paper describes the system requirements for a Dynamic Coalition System, the applicability of virtual machine technology to the problem, and the additional technologies that would be necessary to fulfill the unmet requirements.

1.0 INTRODUCTION

Current and future reliance on coalitions and multi-national operations is complicated by the ability to share information electronically with coalition partners, many of whom are not members of traditional or long-standing alliances. The need to apply and deny access to some kind of coalition system in an ever-changing world situation is a challenge that must be met, addressing the need for availability of common information and tight security. The creation and termination of dynamic coalition networks among partners with different degrees of trustworthiness is a desirable capability and poses difficult challenges. Many issues need to be addressed in developing such a coalition capability, especially considering the high degree of security and integrity required. Configuring and managing virtual machines (VMs) from a central location may provide a secure means to quickly deploy, maintain, and destroy private networks among coalition members.

This paper discusses dynamic coalition networks, their security and how VM technology can address Dynamic Coalition (DC) implementation. The use of VM technology in securely creating Coalition Networks (CNs), and how such networks can be unfailingly shut down when no longer required, is explored.

Paper presented at the RTO IST Symposium on "Adaptive Defence in Unclassified Networks", held in Toulouse, France, 19 - 20 April 2004, and published in RTO-MP-IST-041.

2.0 OVERVIEW

This paper proposes a framework and outlines technical issues associated with forming and protecting CNs using VM technology. After a brief overview of VM technology, we describe the concept of a Dynamic Coalition System (DCS), consisting of a Coalition Management Server (CMS) and multiple CNs that may operate at different levels of trust. The DCS provides for DC creation, via a VM paradigm, that will:

- Secure communications between acknowledged members of a coalition whose membership can change dynamically.
- Deny access to non-members and former members.
- Support rapid setup, termination, and reconfiguration.

The paper describes the desired DCS capability, operational concepts, and general system and security requirements. The requirements combine concepts developed at The Johns Hopkins University Applied Physics Laboratory (JHU/APL) with constraints raised in the Department of Defense (DoD) Goal Security Architecture (DGSA) **[1]**, with respect to issues discussed in Joint Vision 2010 **[2]** and Joint Vision 2020 **[3]**. The validity of these concepts has been demonstrated in a system prototype; the prototype DCS will be described in another paper.

3.0 DEFINITIONS

The following terms and definitions will be used throughout this document.

Coalition	A group of separate entities that must coordinate efforts and communication to achieve shared goals; examples are (1) a group of countries all working toward a common goal or (2) a partnership of autonomous, diverse, geographically distant members.
Coalition Network	A subset of the coalition members, all at the same level of trust, all sharing one set of information. A coalition may require more than one CN. A system of CNs will support different levels of trust in a hierarchical fashion.
Information	May include analysis and conclusions drawn from pools of raw data.
Information Overlays	Automatic way to provide data or information to more than one CN. The information would reside only in one place, but could be accessed by members of multiple CNs. This can help with database synchronization.
Membership Revocation	Returning in total the state of a member to that prior to its membership.
Vulnerability	A security exposure or weakness in a system that can be exploited to undermine the integrity, availability, or confidentiality of the information or resources of the system.
Incident	An actual exploitation of a vulnerability.

4.0 ROLES

The DCS will allow for three roles within its framework:

- Coalition Management Server (CMS) – sets up and takes down CNs in response to authorized requests of network owners. The initial assumption is that NATO controls the CMS.
- Coalition Network Owner (CNO) – determines membership and policy for the CN; the CNO is normally, but not necessarily always, a coalition network member.
- Coalition Network Member (CNM) – participant in the CN.

Figure 1 illustrates a simple example of a DC network depicting CNs whose members are either of different trust levels or are supporting different missions. The example involves three coalition or alliance groupings associated with NATO:

- The lead NATO countries of the International Security Assistance Force (ISAF). The ISAF is the international peacekeeping mission in Afghanistan **[4]**, and was put under the command of the several NATO members at the time of its deployment in January 2002.
- The Northern Light NATO member participants. Northern Light 2003 is "a NATO live, joint and combined exercise [which took] place between 15 and 26 September 2003 in the Irish Sea, on the West Coast of Scotland and Brittany." **[5]**
- The Northern Light partner participants (non-NATO).

The CMS serves three CNs whose CNOs and CNMs are illustrated in Table 1. The countries enclosed in parentheses are members Northern Light, but are not depicted in Figure 1 due to space constraints. Note that Germany, the Netherlands, and the United Kingdom (UK) are participants in multiple CNs. UK is the CNO of both Northern Light CNs, and a CNM of the ISAF lead nations CN; the Netherlands and Germany are CNMs in both the Northern Light NATO member participant CN and the ISAF lead nations CN. The data shared is not necessarily at the same trust level for all CNs.

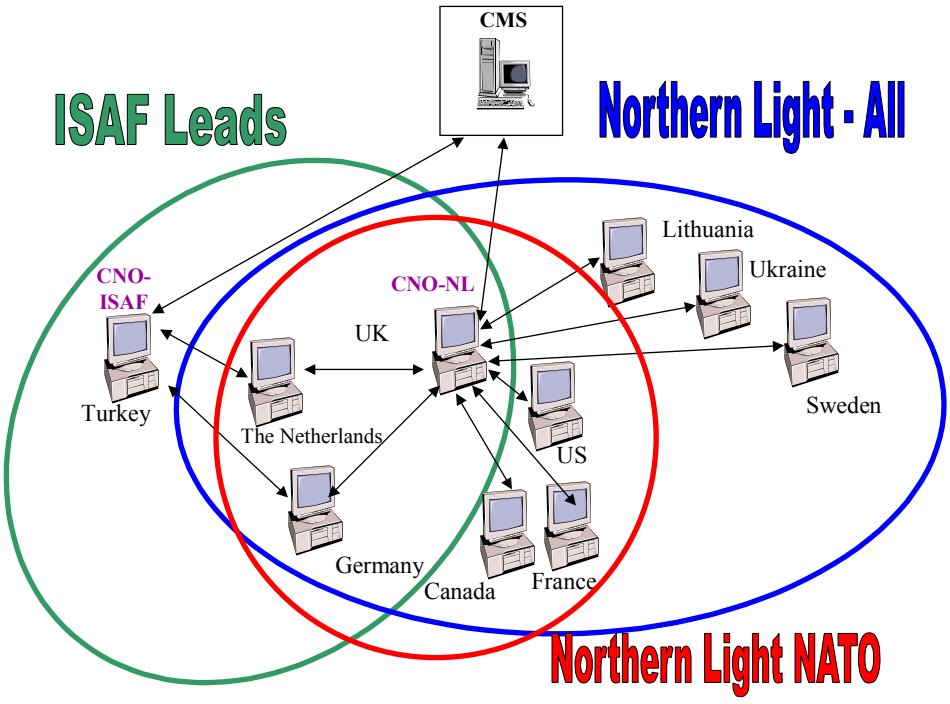

Figure 1 Example Coalition Network

Table 1 Coalition Network Example

Coalition Network	Description	CNO	CNM
CN#1	Lead NATO countries of the ISAF	Turkey	The Netherlands UK Germany
CN#2	Northern Light NATO member participants	UK	France US The Netherlands Germany Canada (Belgium) (Denmark) (Italy) (Norway) (Poland) (Spain)

Coalition Network	Description	CNO	CNM
CN#3	Northern Light NATO plus partner participants (non-NATO)	UK	Lithuania Ukraine Sweden France US The Netherlands Germany Canada (Belgium) (Denmark) (Italy) (Norway) (Poland) (Spain)

5.0 REQUIREMENTS

Before assessing the ability of VM technology to support DC networking, it is first necessary to determine all requirements that must be met to implement such a capability. DC networking is a high interest area that is being researched by a variety of organizations. Therefore, JHU/APL surveyed these efforts, as well as a variety of operational policy documents to determine a fairly comprehensive set of high-level technical requirements.

The following requirements were derived in part from paper reviews and research into other application types, including Defense Advanced Research Projects Agency (DARPA) DC projects and the DGSA. These requirements are for the full DCS, including aspects that may not be covered directly by VM technology, and fall into the following categories: Security Policy Creation, Initial Set Up and Termination, Coalition Network Membership Management, Effective Information Sharing, Data Separation, Data Protection, Communications Protection, Specialized Services Management, Interoperability Management, and Compromise Mitigation.

The requirements together encompass a variety of possible coalition network applications, such as networking among allied partners for military operations, dynamic collaboration of intelligence community partners, or coordinated large-scale system testing among multiple NATO members and task forces. For any particular application, only a subset of the requirements might apply.

Security policy creation requirements encompass combining security policies from each of the participants to form a cohesive policy, agreement on level of sensitivity, and control of the information shared between participants. Agreement on the level of sensitivity poses two interesting problems: labeling terminology, and the relative importance of the information to the different nations involved in the coalition.

Initial setup and termination requirements involve the technological logistics of several groups or enclaves joined together to achieve a specific purpose. A coalition may require more than one CN (Northern Light, for example, has a NATO member component, and a component of participating nations that are not NATO members), or an entity may belong to more than one coalition and require connection to several CNs (Germany, the Netherlands, and the UK, for example, are members of both ISAF and Northern Light NATO). The CNs need to be both established and separated, and a mechanism provided for establishing initial membership to CNs. To participate in DCS, each participant must have a system capable of supporting VM technology, prior to the initial setup. Rapid remote setup may be required for specific coalition situations. Each CN to which a user belongs shall be separated on that user's system. Termination of a CN entails

removing all members. In some cases, rapid remote termination may also be required. Note that any cryptographic products must implement algorithms releasable according to multi-national requirements of the participating nations.

Coalition network membership management requirements provide centralized management of the CNs, and encompasses admission of additional members; termination of members, both voluntary withdrawal and involuntary severance; and authentication of participants. For example, the original lead nations for ISAF were UK, Turkey, the Netherlands and Germany; however, currently, the lead nations are Germany, the Netherlands and Canada. Membership changes may need to be rapidly administered. New members may need to be admitted rapidly to support the coalition mission; membership revocation must be instantaneous, and revoked members must revert completely to the state of non-members. DCS must establish a mechanism for authenticating requests to the CN and control network access accordingly.

Effective information sharing requirements encompass technology to support CN communication, timely interaction with other CN partners, sharing of communication resources, and sharing of data and information among members. Dissimilar electronic communications systems must be networked transparently. No assumptions can be made about the sophistication of the communications suites of the member nations; consequently, the DCS must be able to operate with a minimum communications suite. Provisions must be made for both information push and information pull, if a CN allows data to be placed in a shared area. Furthermore, information must be revocable, if necessary.

Data separation requirements include establishing multiple trust levels (e.g., coexistence of varying sensitivities of information on the same information system so a single user can participate in multiple CNs), labeling information as well as regrading to a different level of trust, transfer of information outside the CN, and management of derived information.

Data protection requirements encompass strict mechanisms for ensuring that non-members cannot gain access to data shared between CN members, including an approved key management system to comply with international policy concerning protection of keying material and a strong identification and authentication system, including biometrics technology to ensure that non-members cannot gain access. This must include both data at rest and data in transit, and address unclassified but sensitive information as well as classified information.

Communications protection requirements encompass establishment of trust over the network and protection of network resources. Knowledge of the existence of a CN must be protected in sensitive operations, so that non-member entities do not know it exists. Outside observers must not be able to determine CN traffic flow characteristics. Protection must be provided to enforce protection of network resources, availability of the channel, integrity of the channel. Remote user environments must provide equivalent protection.

Specialized services management requirements encompass integrating specialized capabilities into a common operating scheme, to include integration of voice, imagery, and data; distribution of compatible software suites; chat capabilities; and white-boarding capabilities.

Interoperability management requirements include: addressing the wide diversity of hardware and software that each participant may wish to utilize; common understanding of terminology; and adaptation of commercial products, standards and technologies, as well as connectivity via common carrier communications systems, into the DCS. DCS must be platform independent.

Compromise mitigation requirements encompass prevention, detection, and reaction to security vulnerabilities and incidents, in order to protect information from hostile entities on the network. Systems should be patched, and patches tested on isolated systems. OS patching, or patching of shared application suites should be CN-wide, and configuration of independent member systems should be as standardized as possible, with permissions set as tightly as possible. COTS and GOTS components should be selected with security features as standard elements.

6.0 VM TECHNOLOGY AND DYNAMIC COALITIONS

Virtual machine technology allows a user to run multiple operating systems at the same time on the same PC. A virtual machine is one system image in a computer that supports multiple system images. Each virtual machine consists of an operating system and associated applications. The multiple system images on a physical machine may either all run the same operating system or different ones.

There are several different models of virtual machines used in the field of computer science today. The model most relevant to the dynamic coalitions problem stems from IBM's original work in the 1960's. IBM's model effectively partitions a computer system into several copies of itself with those copies having some portion of the total resources of the system. Like all virtual machines the IBM model provides a mapping of functionality from the virtual machine to the real hardware. In the IBM model, most of the virtual machine's instructions can be mapped directly to real hardware. However, to preserve the security of the virtual machines, a special set of instructions is trapped by a monitor function. This special set of instructions contains any instruction that would allow a virtual machine to affect another virtual machine. After these instructions are trapped, the virtual machine system then tries to emulate the desired effect for the virtual machine. The instruction trapping and emulation preserves the appearance that functions running in the virtual machine are running on standard hardware but prevents interference with other virtual machines. The important aspect of the IBM model for the dynamic coalitions problem is the non-interference or separation of the virtual machines. While the direct execution of portions of the instruction set is desirable from a performance perspective, it is not necessary.

DCS consists of a collection of CNs – networks of user machines capable of supporting VMs, at least one CMS, and a special INE VM. Each VM would be used to host a single CN for a single user, to separate data and communications by level of trust. VM technology provides the framework for the paradigm proposed for DC networking. The DCS would include VM technology and an inline network encryptor (INE), plus a means of incorporating a VM for every CN to which a participant would belong.

The ability to provide multiple VMs on a single workstation in a secure manner can play an important role in solutions to the dynamic coalition network problem. For example, multiple VMs can be electronically configured for each CN member, allowing access to multiple CNs on a single machine. Figure 2 illustrates a sample CN VM set up. Each CN VM will use an INE VM to connect to a CN.

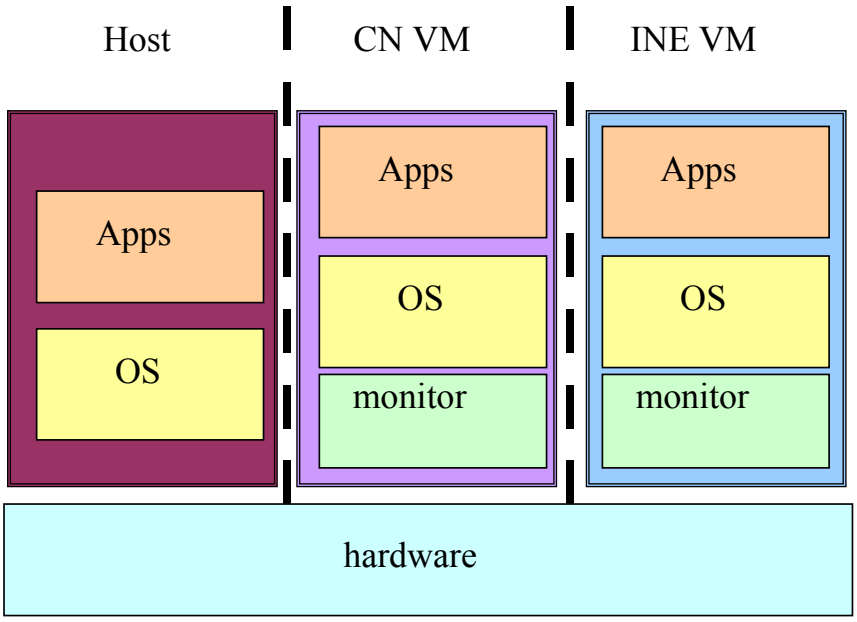

Figure 2 Coalition Network Virtual Machine Set Up

Figure 3 illustrates a possible architecture with three CNMs connected to a CMS. In this architecture all CN traffic passes through virtualized VPN routers on the CMS. This example utilizes the sample coalition setup described in Figure 1 and Table 1; both the Sweden and Germany CNMs are participating in the Northern Light – All (NL-ALL) CN. The Germany CNM also participates in the ISAF CN, along with the Turkey CNM. In addition the Germany CNM participates in the Northern Light – NATO (NL-NATO) CN along with other CNMs not shown in the figure. Each CNM requires a management network for communication with services on the CMS to manage its membership in the various communities of interest (COIs). For instance, a CNM might request membership in a COI and be notified of its acceptance via this management network.

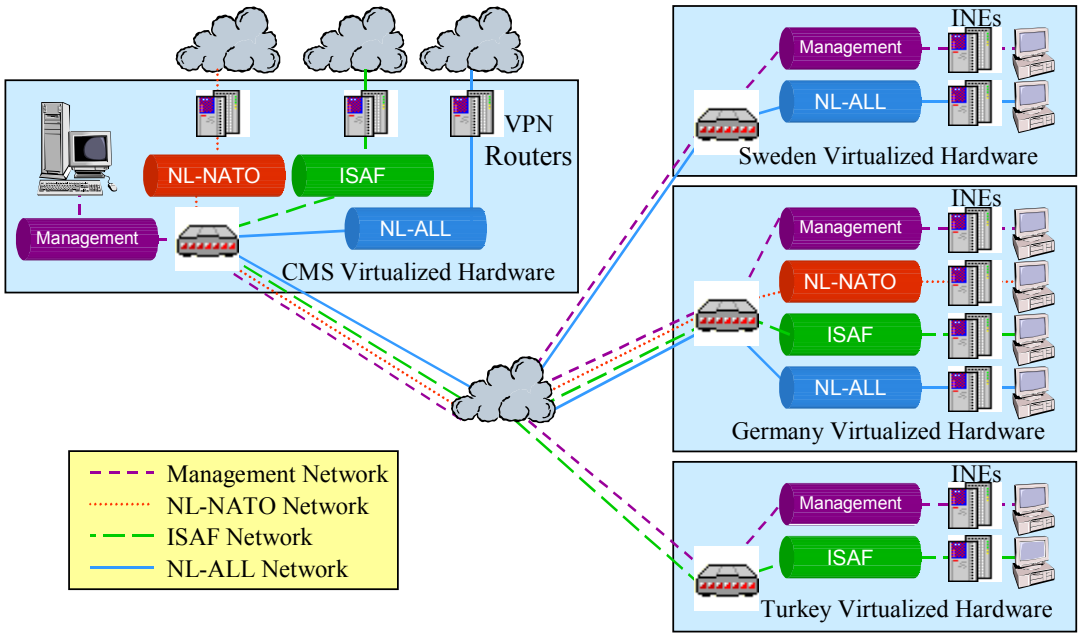

Figure 3 Example Coalition Network Virtualized Architecture

7.0 VM TECHNOLOGY APPLICABILITY

7.1 Security Policy Creation

VM technology does not provide any security policy and would rely on the host machine OS security policy. This has very little effect on the activities that take place inside the VM OS. The host OS security policy would primarily control the separation of the VMs and only control the VM's access to hardware, host file systems, and networks. Consequently, VM technology cannot address most security policy creation requirements for DCS.

For coalition operations, it is necessary to combine security policies of members to form a single cohesive policy that encompasses requirements of all participants, to create a merging of multiple security policies in use by member countries or organizations. The challenges may include reconciliation of policies written in different policy languages, if amalgamation is to be automated within DCS. This would dictate a need to establish a standard language for policy expression.

Because VM technology is unrelated to policy reconciliation, the assumption is that the policy combination will take place independent of VM technology and the CN policy is presented to the CN as a single cohesive unit. Consequently, new members will have to accept the existing policy; otherwise, manual adjustment of the CN policy will be necessary. Future work on DC may include technologies to combine policies.

Agreement on what a particular security level means is largely handled by the definition of CN, where data is equally available and approved for distribution to all members of a CN, who by definition are at an equal trust level. However, given data that is tagged by security level, separation and filtering can be securely enabled via a High Assurance Guard (HAG) in a VM.

7.2 Initial Setup and Termination

VM technology inherently supports joining coalition members on networks and allowing access to more than one network from a single computer. This allows coalition members to participate with different groupings of members or at different trust levels on separate networks.

A further goal is to allow networks of coalition members to be established and dismantled rapidly. The setup includes membership definition and communication capability. The CNO provides an approved membership list to the CMS for management. The challenges of this requirement include the logistics of secure, remote CN and the speed of CN setup with policy and membership in place. To handle the establishment and separation of CNs, a method to establish configuration settings for a standardized VM must be developed. This raises two important issues: (1) how the networks are set up and secured to all the different potential coalition members and (2) how the proper use of the VM or configuration for a standardized VM is assured. Actual time for rapid remote setup will depend on what logistics are agreed upon for distribution of Virtual Machine capability and configuration.

To start, all members must be possession of a machine that can support VM technology configured with dynamic CN capability. VM technology can be distributed in one of two ways: either pre-installed machines may be delivered with VM technology installed, or a CD containing VM technology software can be delivered for installation on a machine at each DCS site. Deploying among non-NATO allies[1] may be a critical problem. The technology for use in multi-national force (MNF) coalitions must be releasable. Available technologies exist to encrypt parts of the kernel, which can only be decrypted with a key provided by the CMS at runtime. It may be possible to meet this requirement via such concepts as a tamper-resistant box, but additional research would be required. Releasability of cryptographic algorithms is beyond the scope of this paper; however, any INE provided would have to meet releasability restrictions of the owner-nation or NATO group. Legal export restrictions for public key infrastructure (PKI) and encryption algorithms must be addressed for CNs with parties from multiple countries.

Initially, a secure network connection needs to be established with the coalition members. Each CNO submits a list of approved members to the CMS. The technical challenges include connecting members to the appropriate CN(s) only.

Rapid remote termination is supported by further VM technology development because the CMS or CNO will be able to turn off a VM once membership is terminated. When a CN is terminated, residual data storage becomes the responsibility of the CNO.

[1] Coalition partners with whom long standing alliances, joint policies, and protocols for data exchange have not been established.

7.3 Coalition Network Member Management

Participants must be configured with the correct VMs. While the central management may be controlled by a NATO entity, the control of a specific CN may be passed to the CNO. The CNO can then request from the CMS that access be given to or revoked from other participants. DCS will need a CNO that can be granted ownership of a particular CN and the ability to control its membership through interaction with the CMS. User registry is not provided directly by VM technology. VM technology does not provide user authentication. Although members are organizations or nations, actions performed in the context of the coalition need accountability to a particular person.

Member identity protection can only be partially provided via VM technology. The use of separate protected networks or encrypted tunnels should make the work required for an adversary to determine the real endpoints and content of the communications sufficiently high. It is assumed that with enough resources and/or time, an adversary could determine the real endpoints or content of the communications.

Using multiple VMs enables users to participate in more than one CN at a time by simultaneously using multiple VMs. CN membership revocation can either be developed or implemented with COTS products. DCS must be able to handle both voluntary withdrawal and involuntary severance. One approach may be to deny access keys for VPN tunnels of given networks. DCS must also consider automatic reconfiguration of the network as membership changes. Reconfiguration of the CN could be done by requiring all members to re-key.

7.4 Effective Information Sharing

By virtue of all CNMs using compatible VM technology, DCS provides transparency because all end-users are employing the same system. The establishment of a minimum communications suite carries the assumption of a minimum hardware standard, for example an X-86 personal computer (PC) with an Internet Protocol (IP) connection, to support VM technology.

The dynamic sharing of communication resources can be accomplished using VPN tunneling, which is supported by VM technology. Compatible VM technology can provide standardization of capabilities and environment. Timely interaction between CNMs can all be handled by the use of standard IP networking tools via network management of channel availability, load balancing, adaptive routing, and relief of traffic congestion. VM technology is not providing anything extra, but allows for IP quality of service provisions from IP networking tools.

Communications between the management server and clients may need to be handled separately. These communications could reveal information regarding which coalition participants are members of which networks. Because that kind of information could be very sensitive, some method of hiding that information or an out-of-band system needs to be developed. VPN tunneling may not be sufficient protection in all cases; either further protection of communication endpoint identities needs to be developed or separate physical networks will need to be used.

By standardizing CNs with compatible VM technologies, problems with process and procedure compatibility should be minimized from a technological point of view. Using common hardware and OS platform reduces the possibility of incompatibilities between coalition members, and allows for use of COTS products

Separation of information and users can be provided by either separate physical networks or an INE. VM technology can support information sharing. The complexity and type of information shared, processed, or

disseminated is limited to that which can be supported on those platforms. The CMS can manage multiple CNs at one time. VM technology will support data and information sharing if members use compatible application suites. VM-specific issues involve issuing a message to all selected potential participants – "You have been invited to participate in…" – which must be made understandable to the recipients, particularly if there is no de-facto standard language. CNMs of the same CN who do not share a common language are not precluded from employing technology to promote mutual understanding, but such technology is not directly provided by the VM.

Support of information push and pull is directly supported with common application suites that can be incorporated in each CN.

CNOs of all CNs involved in an information overlay must agree to share the overlay data. It will be difficult to implement information overlays using VM technology because it has no guards.

VM technology cannot directly revoke information that has been transferred to the CNM's machine, even if that information resides on the VM . Note that if information is pushed and/or pulled onto a CNMs machine, it can't necessarily be revoked when membership is revoked. The CNM's decryption capability can be disabled via a watchdog timer, rendering the information useless.

7.5 Data Separation

VM technology can support separation of multiple trust levels on the same system. Information and user activities will be separated by having each CN on a different VM within the user's system, and there is no mechanism for the information to cross VMs.

VM technology does not provide for proper labeling of classified information on the system, but does not preclude it. The user interface to each VM can be labeled with its trust level. The OS in each VM may be able to support labeling of the data or files within that VM. Data owners need to be responsible for information labeling or a COTS/Government off-the-shelf (GOTS) product would need to be incorporated.

The requirement for the data owner's permission to transfer data to other CN's must be handled via Concept of Operations (CONOPS) or use of third-party software. Data cannot be transferred between CNs except by the member(s) belonging to multiple CNs, and it can only be their own data.

VM technology cannot directly provide for re-grading; it must be developed from scratch or implemented via a COTS re-grader. The derived data (data correlation) restriction occurs when CNs share limited information and then use that information in analysis with other data that is not coalition-wide. Provisions must be made to keep any resulting analysis out of the CN. Derived data restrictions cannot be supported directly via VM technology; it must be a process handled in the CONOPS.

7.6 Data Protection

Data at rest can be protected by the host machine OS security policy and file system encryption. Data in transit can be protected with VPN via the INE, or by physically protected networks.

Standards required for DCS are: (a) security protocols, (b) authentication information, (c) key management and distribution, and (d) voice communications. The INE can support IPsec and probably many other tunneling protocols. A PKI system will be needed to handle VPN key distribution. Voice communications might be provided and protected by using Voice over Internet Protocol (VOIP) applications with the INE.

The host authentication system could include a biometrics authentication device. The VPN keying system and the host authentication together should provide a strong identification and authentication system for the DCS.

Protection of unclassified but sensitive information can be provided by limiting the information to the CN on which it is distributed.

Secure display implementations minimally will include screen lock provided via the OS. Not all OSs have a screen lock. For example, Windows NT/2000/XP do provide a screen lock capability; MS DOS does not. Unix/Linux variants require X Windows for the screen lock capability. However, the host machine OS could provide a host-based screen lock, if needed.

7.7 Communications Protection

An important aspect of protecting communications will be ensuring member confidentiality. A method for configuration of VMs, setup of CNs, and normal interaction on those networks should be designed so that CN participation is only known to the participants of that network and the server. It is always possible for an outside observer to determine that communications are taking place between two endpoints. The use of separated protected networks or encrypted tunnels should help increase the work required for the outside observer to determine this while still concealing the true endpoints and communications content. It would be impossible to develop a solution to provide full protection. One possibility is to produce constant artificial traffic at all times.

The host machine OS security policy can only provide protection for virtualized network resources running on VMs, such as filtering routers and INEs. Any real physical resources would fall outside of its scope.

VM technology can use separate protected networks for each CN. To deploy these networks dynamically, VPN tunneling or some other VPN technology will need to be used. Communication of management clients and server should be designed to provide availability and integrity. This will protect against denial of service, preventing CN member changes from being propagated to members in a timely manner and preventing members from communicating effectively. Aside from the existing protection offered through VPNs, this could be further enhanced by the addition of options like a biometric authentication system for the host machine OS.

The method of configuring VM technology systems to end-users will help ensure that the remote user environments provide equivalent protection. Configuration is dictated by standard distribution. Physical security protection cannot be controlled, but if preinstalled systems are shipped out and hard drive encryption is used, the security provided by a Virtual Machine Technology system will be assured. With a distribution method involving the installation of a Virtual Machine Technology system with CDs at the end user's location, the certainty that equivalent security is being provided is not as high.

7.8 Specialized Services Management

VM technology can already support a large number of specialized services with existing COTS products on the supported platforms. VMs can be preconfigured to include the compatible software suites. The specific services can be fulfilled to the extent that any application running on the supported the chosen VM OSs and virtual hardware can be supported by VM technology under DCS. However, any applications falling outside this suite will either not be supported or need to be developed for VM technology applicability.

7.9 Interoperability Management

Interoperability will be provided for those platforms supported by compatible VM technology. CNMs may span a wide diversity of hardware and software systems and varying levels of technology.

The use of common carrier communication systems will require certification and accreditation (C&A) of an INE VM to declare that the protection is sufficient. VMs are COTS products. Additional technologies may also include COTS components. A dynamic coalition solution using VM technology cannot guarantee that there is a version of the selected technology that can run on every platform.

7.10 Compromise Mitigation

All OS vulnerabilities are open to exploitation. The VM OS vulnerabilities are only exposed to whatever applications and services the user connects to the VM OS. If everything is tunneled, the VM OS is only exposed to other CN members. If the tunnels run on open networks, any INE vulnerabilities[2] that might surface would be exposed to the outside world.

An intrusion detection system (IDS) could be added to the system to provide for detection of security incidents, but one is not within the scope of VM technology. Audit logs can be maintained as well.

Procedural methods for mitigating compromise should be handled via a CONOPS. It may be possible to incorporate an auto-patcher as a COTS add-on, but that is not recommended by JHU/APL because it removes the necessary decision-making control over patch advisability. Because the security policy used on the host machine OS does not have any real control over the interactions internal to the VM OS, it cannot provide or enforce security policy for the CN. New components used for dynamic coalitions should be designed to further enhance these features.

VMs will provide the standard configuration necessary for dynamic coalition implementation, and users should be prevented from changing the specified configuration due to the host OS security policy. Security mechanisms for protection against hostile entities would have to be developed. Assessment of vulnerabilities of chosen or candidate technologies and COTS components is necessary. The host machine OS must enforce prevention of members changing the VM configurations. Key management is not provided by VM technology and would have to be addressed by third-party products.

Certain security features are provided by VM technology, such as isolation between VMs, which helps to ensure integrity and confidentiality. The issue of security features (e.g., access management) must be considered for additional technologies beyond VM technology. New VMs or VM patches could be distributed CN-wide when vulnerabilities are found in the existing VM configurations.

Non-persistent disk features should be used to provide the capability to revert to a clean state in a VM if the disk is corrupted. Incident recognition and a system for executing possible responses would need to be developed to implement a capability to support a documented recovery process for VMs; otherwise, it remains a policy issue.

Note that it may be possible for the VM can become corrupted if it crashed or the computer was turned off while the VM was running. In those cases, procedures would have to be instituted to recover from any corruption that might occur. Host machine OS corruption is possible with some file systems in the event that the disks are not cleanly shutdown. Using journaling file systems might eliminate the potential for corruption.

[2] None known at this time.

8.0 ARCHITECTURE OPTIONS

This section discusses ways to implement the DCS concept with VM technology. To implement this concept it is necessary to allow the creation and, possibly, removal of VMs, as well as allow a specific VM or host process to communicate with a management server to manage these VMs.

CN configuration can be centralized or decentralized. Table 2 summarizes the advantages and disadvantages of both configuration options, and the details are discussed in Section Table 2.

Table 2 Dynamic Coalition System Architecture Configuration Options

Configuration	Advantages	Disadvantages
Centralized	Membership revocation easier – remaining CNMs do not need to be re-keyed CN membership information more easily hidden – use network address translation (NAT) to obfuscate addresses at CMS	Central network services create a possible bottleneck (processing – encryption/ decryption, network bandwidth) Central network servers are an additional single point of failure (all CNs cease operating)
Decentralized	Possibly higher total throughput Normal CN operation does not rely on central resources	Membership revocation more difficult and takes longer – requires re-keying all CNMs Hiding CN membership is more difficult and less efficient – all possible CNMs must communicate random data constantly amongst themselves CNO loses control of membership if the CMS fails

8.1 Dynamic Coalition Network Concepts

Using virtual machine technology as part of the solution to the dynamic coalitions problem will allow multiple CNs to be accessed from a single end-user system. One of the hard problems is managing the creation of these CNs. The CMS controls the initial construction of CNs and manages interaction with the CNO by handling either the keying of VPN routers (for centralized control) or keying all CNMs (for decentralized control) to get them synchronized for the CN. A CN is created based on interaction between the CNO and the server. The CNO supplies the CMS with an initial list of participants. The CMS establishes the CN. The CNO is then given authority over the network and may add or remove members as needed.

Using a centralized network routing architecture, all CN communications pass through the VPN router responsible for that CN, and the CMS passes the membership information to that VPN router. The CMS can update this membership information on the VPN router as needed, based on communications with the CNO. With a centralized network system, membership revocation is easier than with a decentralized network system because a VPN server simply denies that member access. Another advantage of the centralized network architecture is that CN membership information can be more easily hidden using a form of NAT to hide which CNMs are talking to which servers. A disadvantage of the centralized network architecture is that the central network services pose a potential bottleneck and a single point of failure. The central networks services are a potential bottleneck for cryptographic processing and for network bandwidth. If the central network servers are unavailable, the CNs can no longer operate.

A decentralized network would allow the CN communications to travel only to the intended destinations and are not routed through a central VPN router. In the decentralized network, the CMS must pass out the proper key information to establish tunnels between CN members. The use of a decentralized network makes it difficult, if not impractical, to conceal the CN membership information from those outside the CN.

One advantage with a decentralized network architecture is that the cryptographic processing is distributed among all of the CNMs and there are no central network bottlenecks. Another advantage is that even if the CMS is unavailable, the CNs may continue to operate. A disadvantage with a decentralized network architecture is that membership revocation is more difficult and may take longer than with a centralized network system because all the CNMs need to re-key for the new membership list. Hiding CN membership information is also more difficult with a decentralized network architecture because all of the possible CNMs would need to constantly transmit random data amongst themselves to mask the real communications amongst actual CNMs.

9.0 CONCLUSION

VM technology can be used to meet many Dynamic Coalition requirements. Specifically, VM technology supports establishment and separation of coalition networks, membership in multiple coalition networks, transparent networking, multiple trust levels, protection of data at rest and in transit, management of specialized services, and interoperability. Further development would be necessary to address remote distribution of coalition technology, termination of a coalition network, addition and termination of participants, protection of communications, and compromise mitigation. Additional technologies or policies would be needed to address creation and management of joint security policies, authentication, access control, and protection of derived information.

A dynamic coalitions solution employing VM technology will solve many issues paramount to rapid remote coalition operations. Additional development and incorporation of third party technologies can provide the remaining functionality.

10.0 REFERENCES

[1] Department of Defense Technical Architecture Framework for Information Management, “Volume 6: Department of Defense (DoD) Goal Security Architecture, Version 3.0,” 30 April 1996

[2] Chairman of the Joint Chiefs of Staff, “Joint Vision 2010,” 1996

[3] Director for Strategic Plans and Policies, “Joint Vision 2020,” 2000

[4] NATO Update webpage, “Same name, same banner, same mission a NATO enhances ISAF role,” http://www.nato.int/docu/update/2003/04-april/e0416a.htm

[5] NATO International Military Staff webpage, “Exercise Northern Light 2003: NATO exercises a joint combined Task Force in Northern Europe,” http://www.nato.int/ims/2003/p030903e.htm