Explotación de Información de Alto Valor para la Mitigación de Vulnerabilidades en Operaciones Militares Basadas en Redes

Bernardo Marcelo Gilman[1], Adrián Mario Tamburri[1],

[1] CIDESO – DIGID – Ejército Argentino, Director Proyecto REDES – PIDDEF 23/11, Bernardo Marcelo Gilman (marcelo.gilman@gmail.com) es Director del Proyecto REDES y Adrián Mario Tamburri (adrian.tamburri@gmail.com) es Investigador del Proyecto.

Resumen. En las actuales operaciones militares las Fuerzas Armadas de diversos países han adoptado un nuevo paradigma de combate denominado Operaciones Basadas en Redes. Este paradigma basado en el uso intensivo de nuevas tecnologías de la información y redes de comunicación ha cambiado radicalmente la doctrina militar. En el transcurso de estas operaciones, masas de datos e información fluyen libremente entre los actores que componen el escenario de combate. Si bien este paradigma aporta numerosos beneficios, no son pocas las vulnerabilidades a superar en un escenario donde las decisiones que afectan a vidas humanas están fuertemente basadas en la tecnología. En las Operaciones Basadas en Redes distintos sensores producen una inmensa masa de datos e información que de no llegar oportunamente o ser irrelevante para los decisores, puede traer terribles consecuencias sobre las vidas humanas afectadas. En este trabajo se plantea un abordaje que mediante la explotación de Información de Alto Valor (oportuna y relevante) pretende mitigar las vulnerabilidades en este tipo de operaciones militares.

Palabras Claves: Operaciones Militares Basadas en Redes, Toma de Decisiones, Bases de Conocimiento, Lenguajes Específicos de Dominio.

1. Introducción

A partir de la década de 1990 un nuevo paradigma de combate en operaciones militares denominado Operaciones Basadas en Redes (o NCO por sus siglas en inglés) ha sido adaptado por distintas autoridades nacionales de defensa y seguridad a lo largo y ancho del mundo. Este paradigma se basa en el uso intensivo de las nuevas tecnologías de la información y comunicación como medio para atacar y combatir eficazmente potenciales amenazas para la seguridad nacional. Este esquema de combate que comenzó en el terreno de la Defensa Nacional, está también siendo rápidamente adoptado por organizaciones civiles no gubernamentales relacionadas también con la Seguridad.

Básicamente una NCO propone interconectar a todos los recursos tecnológicos y humanos en una misma red que permita un mejor aprovechamiento de la información disponible y de esta forma lograr un mayor rendimiento colectivo (ver [1]).

En estas operaciones una gran cantidad de sensores produce una inmensa masa de datos e información que pueden ser rápida y eficazmente accedidos mediante un achatamiento de la pirámide de control y la utilización de Sistemas de Comando y Control (C^2) automatizados que permiten una rápida toma de decisiones y resolución de peticiones como así también una eficaz asignación de recursos en tiempo real.
Gracias al avance incesante de la tecnología de la información y las comunicaciones este modelo de operaciones funciona aún en los escenarios de combate más exigentes, brindando a los combatientes un conocimiento de su entorno como nunca antes existió.
Sin embargo, en una NCO existen vulnerabilidades que afectan el desempeño y hasta pueden poner en peligro a las propias tropas. A continuación se presentan algunas de estas vulnerabilidades:

Interoperabilidad. Una NCO depende fuertemente de la interoperabilidad de los diversos componentes de la red (como por ejemplo equipos de comunicación, datos, software, etc.) que permita una adecuada interconexión entre los diversos actores de la operación. Debe asegurarse un correcto acceso a la red como así también métodos veloces de monitoreo y manejo de los recursos involucrados en ella. El descuido de estas cuestiones será causal de un potencial fracaso general.

Comunicaciones satelitales. El buen funcionamiento de los satélites resulta crucial para establecer comunicaciones móviles en áreas remotas, obtener imágenes, información sobre el terreno, datos climáticos, alertas por ataques, etc. En ciertas operaciones de mediano o gran porte, la cantidad de datos que los satélites pueden manejar se ve ampliamente superada por la cantidad real de datos requeridos. Esta severa limitación en el ancho de banda de las comunicaciones satelitales para la enorme masa de datos a transmitir produce severos problemas tales como pérdidas o retardos en la transmisión de información vital para la seguridad de las personas y el éxito de las misiones.

Armamento telecomandado. En una NCO suele integrarse el comando y control de armamento como puede ser el caso de misiles aire-tierra. Este tipo de armamento puede reportar su estado desde que es activado hasta luego de su impacto, permitiendo su telecomando desde posiciones remotas. El problema de estas sofisticadas armas es que demandan un enorme y robusto ancho de banda para su efectivo control (como es el caso de misiles o aviones no tripulados). Esta excesiva demanda de recursos de la red puede afectar el normal funcionamiento de otros actores o componentes que podrían no recibir la información que necesitan de manera oportuna.

Comunicaciones limitadas. Es una incógnita si el ancho de banda disponible en las redes futuras será adecuado para soportar grandes sistemas basados en el paradigma NCO. Cuando las comunicaciones en red se ven limitadas los Comandantes se ven forzados a desconectar uno o más componentes conectados a la red con el fin de liberar ancho de banda para dar prioridad a los mensajes que ellos consideran prioritarios. Esto puede cancelar mensajes muy importantes desconocidos por el

Comandante que comprometen severamente la seguridad de personas o el cumplimiento de otras misiones.

Información inoportuna. Recibir información cuando ya no es de utilidad puede derivar en graves riesgos. A modo de ejemplo, en Abril de 2003 en Irak, tropas estadounidenses fueron sorprendidas por una gran fuerza de tanques enemigos debido a que los datos de posición de las tropas iraquíes no llegaron a tiempo a los sistemas de las tropas americanas, causando que ambas tropas estuviesen a una distancia de 100 metros la una de la otra. Investigaciones posteriores revelaron que la grave situación se debió a que por la saturación de la red de comunicación, la valiosa información no pudo ser transmitida a tiempo.

Achatamiento de la pirámide de control de acceso a la información. Un sistema en el que todos los usuarios o sistemas pueden acceder a toda la información presenta grandes riesgos de seguridad y de usabilidad para que la masa de información no entorpezca el proceso de toma de decisiones.

Con el fin de mitigar estas posibles vulnerabilidades en el marco del Proyecto REDES[1] estamos desarrollando un prototipo basado en el uso de Bases de Conocimiento, Lenguajes Específicos de Dominio y una política de acceso a las información mixta “push & pull”.

2. Modelo Conceptual

En este trabajo, llamaremos **Dato** a la unidad semántica producida por los sensores, **Información** a la unidad semántica consumida por los **Actores de Toma de Decisiones** (DMA por sus siglas en inglés) y **Conocimiento** a la pieza de información enriquecida y embebida en un contexto particular explotada por un DMA.
Para tomar buenas decisiones un DMA debe ser provisto de información de gran valor. El **Valor de la Información** (VOI) para un DMA, depende de la relevancia (utilidad) y oportunidad (en tiempo) de la información que se le provee. El Modelo Conceptual planteado fue pensado para proveer a cada DMA información con un alto VOI.
En la Figura 1, podemos observar un esquema del Modelo Conceptual. En el núcleo del modelo, una **Base de Conocimiento** (KB) provee los métodos necesarios para recolectar, organizar, compartir, buscar y explotar datos e información por parte de los actores externos como sensores y sistemas (más información y ejemplos en [2]).
En este modelo la KB es accedida usando un **Lenguaje Específico de Dominio** (DSL) del tipo declarativo llamado **MILK** especialmente diseñado para el Comando y Control de escenarios militares. Cualquier actor que acceda a la KB deberá crear y ejecutar una sentencia MILK.

[1] El Proyecto REDES – PIDDEF 23/11 es desarrollado en el Centro de Investigación y Desarrollo de Software del Ejército Argentino (CIDESO) y es subsidiado por el Ministerio de Defensa de la Nación.

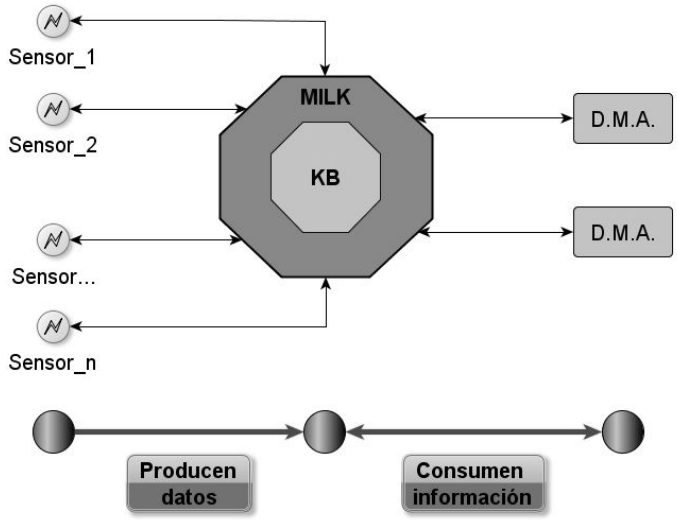

Figura 1: Modelo Conceptual REDES

Una KB es un tipo especial de base de datos que con un proceso conocido como **Extraer, Transformar y Cargar** (ETL) puede extraer datos desde los sensores, transformarlos para que cumplan los requerimientos operacionales de la KB y cargar los resultados dentro de la KB.
Dada la gran variedad de estructuras internas como bases de datos, sistemas expertos, redes semánticas, archivos planos y otros, el ETL resulta un proceso no trivial que requiere una gran cantidad de recursos computacionales.
La KB es el componente clave para gestionar el conocimiento. Nuestro modelo propone pasar de una política de distribución de información "push" en el que la información es enviada a todos los actores que el sistema considera relevante a una política mixta "push & pull" donde la información es enviada a quien la requiere en el momento oportuno mediante la introducción de elementos reactivos y proactivos en la KB.
Este modelo contribuye a mejorar la **consistencia** de la información debido a que en todo momento la KB provee un único estado y por lo tanto productores y consumidores tienen una vista homogénea de la información.
También mejoramos la **seguridad** de la información controlando el acceso a la KB, la **relevancia** distribuyendo únicamente información con un alto VOI y la **oportunidad** reduciendo los bits innecesarios en la red liberando de esta forma ancho de banda para que la información relevante llegue en tiempo al correcto DMA.

3. Modelo Computacional.

En el Modelo Conceptual toda interacción con la KB es realizada por medio del lenguaje MILK. Este DSL orientado al Comando y Control de operaciones militares conforma un módulo de la KB. Al ser MILK un lenguaje declarativo pretendemos

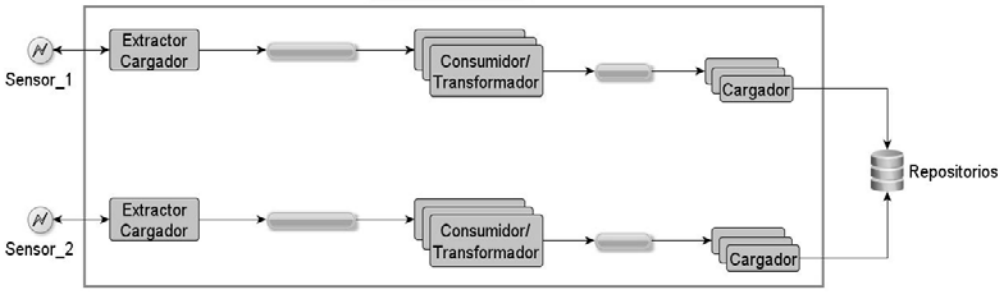

Figura 2: Modelo E.T.L.

lograr que cada componente que debe interactuar con el sistema pueda simplemente expresar qué necesita agregar u obtener de la KB y ocultar la complejidad de conocer, acceder y adaptarse a la estructura interna de la misma (para más información sobre Lenguajes Específicos de Dominio, ver [3]).

El lenguaje MILK está siendo desarrollado con JavaCC, un generador de analizadores sintácticos de código abierto para el lenguaje de programación Java. JavaCC genera analizadores descendentes (top-down) y por lo tanto se encuentra limitado a la clase de gramáticas LL(k).

Para los desarrolladores que necesitan implementar módulos de sistemas que deben acceder a la KB resulta muy conveniente la disponibilidad de un lenguaje como el MILK para lograr sistemas desacoplados y fáciles de mantener.

La existencia de una KB mejora la seguridad y permite mejorar el control de acceso a la información que es una de las principales vulnerabilidades de los sistemas NCO.

Recordemos que nuestro modelo utiliza una política de acceso a la información “push & pull” para que sólo se consulte (push) o reciba (pull) la información requerida. De esta manera se puede controlar el uso del ancho de banda con el fin de priorizar el uso de la red de comunicaciones para información de alto VOI.

En la Figura 2 vemos que la carga de datos desde los sensores se realiza con un modelo conocido como **Extracción, Transformación y Carga** (ETL) donde los datos primitivos producidos van siendo transformados y cargados en la KB de manera automática. Los módulos extractores encolan los datos de los sensores de manera asíncrona en colas que son consumidas por módulos de transformación. Estos módulos consumen los datos para transformarlos en las piezas de información que serán encoladas nuevamente para ser consumidas por módulos cargadores responsables de la carga final en la KB.

Por cada tipo de dato tenemos por lo menos un pipeline de ETL. La existencia concurrente de distintos pipelines permite aumentar la escalabilidad, robustez y desempeño del sistema de carga de la KB.

En este momento estamos trabajando en un primer prototipo en el que la KB está siendo desarrollada con el lenguaje JAVA y PostgreSQL como base de datos para el almacenamiento de la información. Con el fin de realizar pruebas preliminares, se han implementado algunos pipelines ETL en el que los sensores son emulados.

4. Conclusiones

Los resultados obtenidos en nuestras primeras pruebas son muy alentadores: la abstracción sobre la implementación es completa, el acceso a la información es sumamente sencillo y el control de acceso a la KB es total.
Creemos que el objetivo de priorizar la explotación de información con alto VOI como forma de mitigar las vulnerabilidades de las NCO está siendo alcanzado. Mejorar la implementación de este paradigma es muy importante porque mejora el proceso de toma de decisiones tanto en operaciones militares como en situaciones de crisis y esto contribuye directamente a salvaguardar vidas humanas.
En el futuro seguiremos ampliando nuestro prototipo mediante la incorporación de distintos sensores y extensión del lenguaje MILK para que este modelo sea utilizado en los sistemas C^2 del Ejército Argentino.

Referencias

1. Clay Wilson. CRS Report for Congress. Network Centric Operations: Background and Oversight Issues for Congress. Updated March 15, 2007.
2. Maj. R. Baijal, M. K. Arora and S. K. Ghosh. “A GIS Assisted Knowledge-Based Approach for Military Operations". Geomatics Engineering Section, Department of Civil Engineering. Indian Institute of Technology. Roorkee, Roorkee 247 667.
3. Abel Gómez Llana. “Implementación de un lenguaje de definición de operaciones complejas en Gestión de Modelos para la herramienta MOMENT”. Universidad Politécnica de Valencia. Departamento de Sistemas Informáticos y Computación. Cno. de Vera, s/n. 46022 Valencia. Dirigido por Isidro Ramos y José Á. Carsí.