INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS ESTADO DE MÉXICO

AUTENTICACIÓN EN REDES ad hoc BASADO EN MODELADO DIFUSO DE NIVELES DE CONFIANZA.

TESIS PARA OPTAR EL GRADO DE
MAESTRO EN CIENCIAS DE LA COMPUTACIÓN CON ESPECIALIDAD EN REDES
QUE PRESENTA

URIEL EDGAR CEDILLO RAZO

Asesor:	Dr. Miguel González Mendoza.	
Comité de tesis:	Dr. Andrés David García García. Dr. Jaime Mora Vargas.	
Jurado:	Dr. Andrés David García García.	Presidente
	Dr. Jaime Mora Vargas.	Secretario
	Dr. Miguel González Mendoza.	Vocal

Atizapán de Zaragoza, Edo. Méx., 23 de noviembre 2007

RESUMEN

Los dispositivos móviles han venido a cambiar el estilo de vida que tenemos, no hace mucho hubiera sido muy difícil pensar en la gran cantidad y variedad de dispositivos que tenemos hoy en día. Las comunicaciones inalámbricas se han vuelto indispensables y el estar conectado y compartiendo información se ha vuelto vital, como veremos a lo largo de este trabajo de tesis realizamos un estudio de las características principales de las redes *ad hoc* y su gran variedad de aplicaciones, sin embargo, se tienen varios problemas aún abiertos, debido al dinamismo que por su naturaleza este tipo de redes presenta.

En particular, el tema de seguridad es muy amplio y su aplicación en la tecnología de redes *ad hoc* no es la excepción, repasaremos los conceptos básicos para entender las carencias en el manejo de la seguridad que tienen las redes *ad hoc*, y en la forma en la que se pueden implementar estas políticas de seguridad a través de un sistema de inferencia difusa.

Así, esta tesis propone un modelo de inferencia difusa para la autenticación en redes *ad hoc* y su implementación para un entorno dinámico con diferentes tipos de comportamientos, presentaremos los resultados obtenidos al aplicarlo en una serie de nodos, analizándolos y generando las conclusiones y perspectivas del trabajo.

CONTENIDO

Resumen

Contenido

1 INTRODUCCIÓN 6

1.1 ANTECEDENTES 6
1.2 COMPUTO MÓVIL 6
1.3 PRIMERA GENERACIÓN 8
1.4 SEGUNDA GENERACIÓN 8
1.5 GENERACIÓN 2.5 9
1.6 TERCERA GENERACIÓN 9
1.7 REDES INALÁMBRICAS 10
1.7.1 REDES INALÁMBRICAS CON INFRAESTRUCTURA (WLAN) 11
1.7.2 REDES INALÁMBRICAS SIN INFRAESTRUCTURA (ad hoc). 13

2 PLANTEAMIENTO DEL PROBLEMA Y OBJETIVOS 14

2.1 PLANTEAMIENTO DEL PROBLEMA 14
2.2 HIPÓTESIS. 17
2.3 OBJETIVOS. 18

3 REDES AD HOC 19

3.1 CARÁCTERISTICAS DE LAS REDES AD HOC 19
3.2 REDES MÓVILES AD HOC (MANETS). 22
3.3 REDES DE SENSORES INTELIGENTES. 23
3.4 PROTOCOLOS DE RUTEO EN REDES AD HOC. 24
3.4.1 PROTOCOLOS DE RUTEO ad hoc PROACTIVOS. 25
3.4.1.1 Dsdv. 25
3.4.2 PROTOCOLOS DE RUTEO ad hoc REACTIVOS. 26
3.4.2.1 Aodv. 26
3.4.2.2 Dsr. 27
3.4.2.3 Tora. 28

4 SEGURIDAD. 30

4.1 TIPOS DE SEGURIDAD 30
4.1.1 SEGURIDAD FÍSICA 31
4.1.2 SEGURIDAD LÓGICA. 31

4.2 SERVICIOS DE SEGURIDAD. 32
4.2.1 AUTENTICACIÓN. 34
4.2.2 CONTROL DE ACCESO. 35
4.2.3 CONFIDENCIALIDAD. 35
4.2.4 INTEGRIDAD. 36
4.3 MODELOS Y POLÍTICAS DE SEGURIDAD. 36

5 SISTEMAS DE INFERENCIA DIFUSA. 39

5.1 CONCEPTOS BASICOS DE LA LÓGICA DIFUSA. 39
5.1.1 VARIABLES LINGÜISTICAS Y CONJUNTOS DIFUSOS. 39
5.1.2 PROPOSICIONES DIFUSAS COMPUESTAS Y OPERACIONES CON CONJUNTOS DIFUSOS. 42
5.1.3 REGLAS DIFUSAS Y RAZONAMIENTO APROXIMADO. 43
5.2 SISTEMAS DE INFERENCIA DIFUSA. 44
5.2.1 BASE DE REGLAS DIFUSAS. 45
5.2.2 MECANISMO DE INFERENCIA DIFUSA. 47
5.2.3 TIPOS DE SISTEMAS DE INFERENCIA DIFUSA. 48
5.2.4 MODELADO RELACIONAL DIFUSO 49

6 MODELO PROPUESTO. 50

6.1 COMPONENTES DEL MODELO. 50
6.1.1 AMBIENTE DE PRUEBAS. 52
6.1.2 VARIABLES DE ENTRADA. 52
6.1.2.1 Tráfico promedio. 52
6.1.2.2 Última transmisión. 54
6.1.2.3 Comportamiento. 56
6.1.3 DIFUSIÓN. 58
6.1.4 BASE DE CONOCIMIENTO. 58
6.1.5 MECANISMO DE INFERENCIA DIFUSA. 59
6.1.6 DEFUSIÓN. 60
6.1.7 NIVEL DE CONFIANZA. 60
6.2 OPERACIÓN DEL MODELO. 61
6.2.1 OBTENCIÓN DEL NIVEL DE CONFIANZA. 61
6.2.2 VENTANA ESTÁNDAR. 62
6.2.3 LARGO PLAZO. 62
6.2.4 APLICACIÓN DEL NIVEL DE CONFIANZA. 63
6.3 DINAMISMO DEL MODELO. 65
6.4 DEFINICIÓN DEL TAMAÑO DE LA MUESTRA. 66
6.5 RESULTADOS OBTENIDOS DEL PROGRAMA. 67
6.5.1 AMBIENTE IDEAL. 67
6.5.2 NODOS MALICIOSOS. 68
6.5.3 NODOS INTERMITENTES. 69
6.5.4 NODOS INTERMITENTES MALICIOSOS. 70
6.5.5 NODOS INTERMITENTES IDEALES. 71
6.5.6 ANÁLISIS DE LOS RESULTADOS OBTENIDOS. 72

7 CONCLUSIONES Y RECOMENDACIONES 73

7.1 CONCLUSIONES. 73
7.2 TRABAJO FUTURO. 73

8 REFERENCIAS 75

1 INTRODUCCIÓN

1.1 ANTECEDENTES

Los sistemas inalámbricos son muy utilizados en la actualidad por las grandes ventajas que presentan con respecto a los sistemas cableados, básicamente la eliminación de los cables facilita la instalación, ahorra costos, permite utilizar equipos móviles, genera nuevas aplicaciones y flexibilidad para abrir nuevas áreas de oportunidad.

Sin embargo, a pesar de las ventajas mencionadas, aún existen varios problemas a resolver en las redes inalámbricas entre ellos los derivados del medio de transmisión, la movilidad de los equipos, la falta de estándares y la seguridad, entre otros.

El desarrollo de las redes ha ido evolucionando a pasos agigantados tanto en protocolos, seguridad, tasas y medios de transmisión. Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un sólo lugar.

1.2 COMPUTO MÓVIL

Las comunicaciones inalámbricas han capturado nuestra atención e imaginación, convirtiéndose en el segmento de mayor y más rápido crecimiento dentro del área de las telecomunicaciones. Sus principales ingredientes han sido el deseo de movilidad en la comunicación y la ruptura de las conexiones físicas (alámbricas) a la red. La visión de los beneficios de los sistemas inalámbricos futuros se resume en escenarios que posibilitan servicios múltiples que van desde una simple conversación telefónica, hasta la transferencia de archivos o videoconferencia sin restricciones de tiempo y lugar [1].

En los últimos años, se han presentado al menos dos cambios dramáticos en la forma de utilizar las computadoras. El primer cambio tiene su origen en el aumento de la conectividad entre computadoras heterogéneas, a través de diferentes tecnologías de comunicación (satélite, celular,

radio frecuencia, infrarrojo, etc.). El segundo cambio fue ocasionado por el incremento en la miniaturización y disponibilidad de componentes de hardware y suministros de energía (baterías).

La combinación de estas dos tendencias permitió el desarrollo de computadoras portátiles poderosas y económicas. Debido al aumento del uso de estos sistemas portátiles, la visión de un usuario móvil que accede a la red en cualquier lugar y en cualquier momento, se hace cada vez más factible.

En la figura 1.1 se muestra la evolución natural del computo desde los usuarios simples interactuando sólo con el sistema operativo hasta el computo móvil, mostrando las ventajas que se tienen tanto por el uso más flexible de los recursos como la libertad con la que podemos colocarlo dichos recursos.

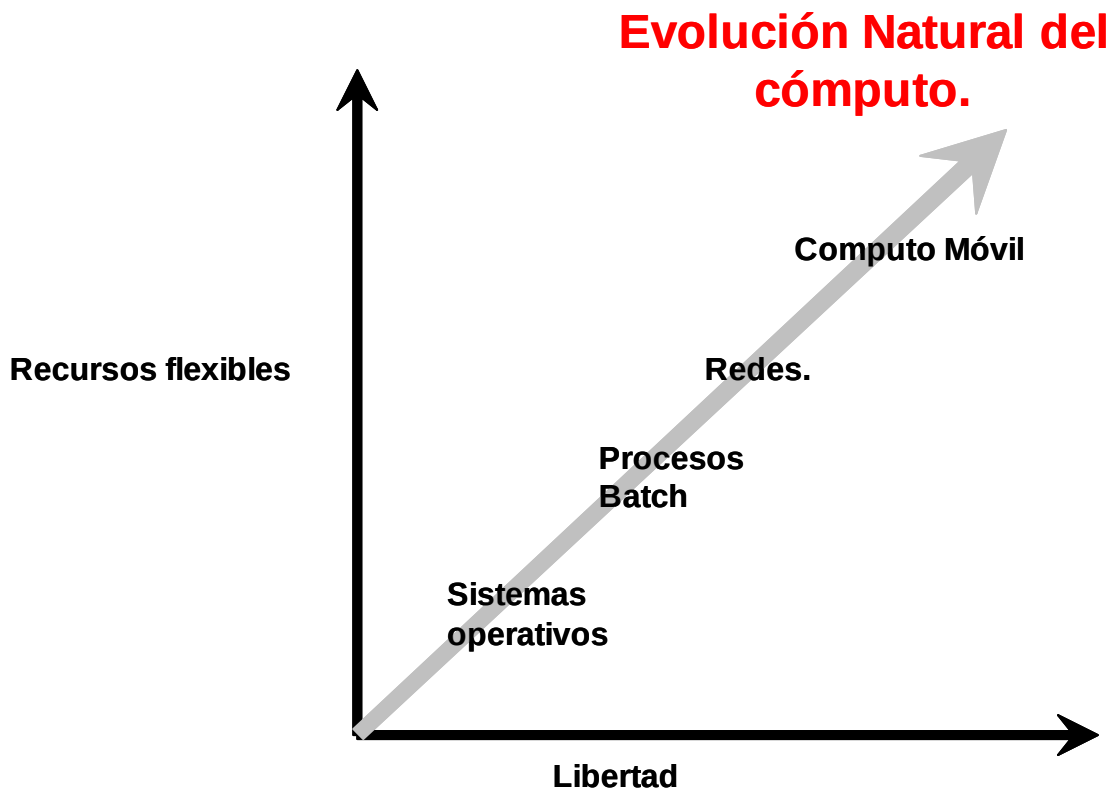

Fig. 1.1 Evolución natural del cómputo (Original en colores).

Diversas tecnologías y sistemas han sido propuestos para proveer servicios de comunicación inalámbrica

Los aspectos principales que han provocado el crecimiento de la tecnología inalámbrica han sido: el deseo de movilidad en la comunicación y la ruptura de las conexiones físicas (alámbricas) a la red. Los sistemas inalámbricos se resumen en escenarios que posibilitan servicios múltiples. [2].

Diversas tecnologías y sistemas se propusieron para proveer servicios de comunicación inalámbrica como son [3]:

- La Telefonía Inalámbrica que aparece en los años 70 para proveer servicios de baja movilidad, potencia y, principalmente, servicios económicos dentro de pequeñas áreas de cobertura.
- Los Sistemas Móviles Celulares, diseñados para proveer servicios de alta movilidad, en amplias, medianas e incluso pequeñas áreas de cobertura a bajas potencias.
- Los Servicios de Localización y Mensajería (Paging/Messaging).

La evolución de las redes inalámbricas en generaciones se clasifica de la siguiente forma:

1.3 PRIMERA GENERACIÓN

La primera generación de los sistemas de telecomunicación celular móvil apareció en los años 80´s. La primera generación usaba técnicas de transmisión análoga y fue estrictamente para uso de voz. No había un estándar dominante pero si mucha competencia. Los estándares más exitosos fueron Nordic Mobile Telephone (NMT), Total Access Comunications System (TACS), y Advanced Mobile Phone Service (AMPS).

1.4 SEGUNDA GENERACIÓN

La segunda generación de los sistemas celulares móviles usa radio transmisión digital, tiene mayor capacidad a comparación de los sistemas de la primera generación y es conocida en los Estados Unidos como Personal Communications Services (PCS). Usa tres tecnologías que dividen las ondas de aire para permitir un mayor tráfico; Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA) y Global System for Mobile Communications (GSM).

Los estándares de los sistemas de segunda generación IS-136 e IS-95 se caracterizan por la transmisión digital de voz y datos a tasas bajas y medias de transmisión (hasta 100 kbps). El crecimiento de Internet y el continuo incremento en la demanda de servicio, dio origen a nuevos e innovadores servicios de banda ancha, los cuales son los impulsores de los sistemas de tercera generación.

1.5 GENERACIÓN 2.5

Esta generación incluye todas las ventajas de la segunda generación pero, además posee algunas características de los sistemas de tercera generación. La generación 2.5 está basada en intercambio de paquetes, con lo que se ahorra espacio e incrementa velocidad de transmisión, incluye las siguientes tecnologías: High-speed circuit-switched data (HSCSD), General Packet Radio Services (GPRS), y Enhanced Data Rates for Global Evolution (EDGE). Alcanza una velocidad de hasta 144 Kb/seg. Muchas compañías en Europa y Estados Unidos hacen una transición intermedia de la segunda generación en vez de gastar grandes cantidades de dinero en reconstruir la infraestructura de ir directamente a la tercera generación.

1.6 TERCERA GENERACIÓN

En las comunicaciones móviles, también conocidas como sistemas personales de comunicación, la creciente necesidad de introducir aplicaciones adicionales a las de voz, como datos y video, dieron origen a los sistemas de tercera generación, cuyos objetivos van más allá de los que caracterizaban a los sistemas de segunda generación IS-54, GSM o IS-95, en aspectos como:

- Una amplia gama de servicios: voz, video y datos, a altas tasas de transmisión de al menos 144 kbps, preferentemente de 384 kbps para usuarios de alta movilidad, en una amplia zona de cobertura, y de 2 Mbps para usuarios de baja movilidad, en un área de cobertura local.
- Altos niveles de calidad en el requerimiento de los servicios relacionados, con tasas de error menores a 10-6.
- Operación en múltiples escenarios (macro, micro, pico, etcétera) y diferentes ambientes.
- Alta eficiencia espectral, flexibilidad en la asignación y manejo de los recursos.
- Alta flexibilidad para introducir nuevos servicios.

La estandarización de los sistemas de tercera generación ha progresado rápidamente en la mayor parte del mundo. Los estándares de tercera generación se aprobaron por la Unión Internacional de Telecomunicaciones (ITU) en Noviembre de 1999 como Telecomunicaciones Móviles Internacionales 2000 (IMT-2000) y bajo el Instituto de Estandarización Europea de Telecomunicaciones (ETSI) como Sistema Universal de Telecomunicaciones Móviles (UMTS) para extender los servicios provistos por los sistemas de segunda generación en Europa y Japón, en América el Instituto de Estandarización Americana (ANSI).

Las computadoras de la tercera generación se distinguen por estar constituidas por circuitos monolíticos integrados (circuitos con miles de transistores encapsulados en una pequeña pieza de semiconductor). Con ellos se generaliza el concepto de “sistema operativo” o programas básicos de control del equipo. También mejoran los dispositivos periféricos. Estos avances implicaron entre otras ventajas: menores costos, mayores velocidades, menor gasto de energía, menores

requerimientos de espacio, mayor facilidad de uso, aprovechamiento más eficiente del equipo; y posibilidades de utilizar teleproceso y tiempo compartido.

En esta generación es posible la ejecución de varios programas simultáneamente, sin que para ello haya que recurrir a un ordenador auxiliar. Por supuesto, en cada instante dado, sólo un programa es el que está ocupando la actividad de la unidad central, si bien los programas restantes trabajan simultáneamente con las unidades de entrada y salida. Cuando el programa que ejecuta la unidad central necesita algún dato, otro programa pasa a ocupar su lugar, mientras que el anterior ingresa en el conjunto de programas que realizan operaciones de entrada o salida. Este método de funcionamiento se denomina multiprogramación.

La tercera generación permitió a los usuarios finales, profesionales informáticos así como a los de otras especialidades experimentar el teleprocesamiento en los sistemas convencionales. El teleprocesamiento permite al usuario realizar la entrada de datos desde terminales remotos, y recibir los resultados en el mismo lugar. Los sistemas convencionales permiten a los usuarios, no sólo enviar y recibir datos desde sus terminales, sino también seguir e intervenir en el desarrollo de sus programas a través del diálogo con la máquina.

1.7 REDES INALÁMBRICAS

Son, como su propio nombre lo indica, red sin cables, con este tipo de red es posible comunicar un conjunto de computadoras sin necesidad de tener conectado un cable entre la computadora y la red dando así una movilidad total en el espacio donde se haya proporcionado cobertura igualando las prestaciones que dan la mayoría de las redes cableadas.

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI [4]. La capa física indica cómo son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir cómo se empaquetan y verifican los bits de modo que no tengan errores las demás capas, la MAC es utilizada por puentes, ruteadores o compuertas para obtener conectividad. Los dos métodos para utilizar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas, al contrario se busca lo mejor de 2 mundos con la “Red Híbrida”, velocidad y movilidad, considerando al sistema cableado cómo la parte principal y la inalámbrica para resolver los últimos metros hacia las estaciones de trabajo y que ésta proporcione movilidad adicional para que se pueda desplazar con facilidad dentro de un almacén, oficina, casa, escuela etc.

Entre las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son [5]:

- Instalación: La instalación es sencilla, rápida, sin costosas obras y sin ningún impacto visual.
- Movilidad: Un usuario podría moverse con su computadora por toda una empresa, campus o el hogar sin perder conexión con la red, las impresoras podrían cambiarse fácilmente de ubicación.
- Los empleados que no dispongan de un lugar fijo de trabajo pueden llegar a la oficina, situarse en cualquier estancia y conectarse a la red.
- Las redes inalámbricas son fácilmente integrables, al no necesitar instalar cableado de ningún tipo.
- Son mucho más sencillas de administrar que las redes cableadas.
- Al contrario que las redes cableadas, en donde una vez instalada pasa a ser propiedad física del lugar (oficina, local, etc.), las redes inalámbricas se pueden transportar con mayor facilidad si fuese necesario.
- El costo de instalar ambos tipos de redes es similar, pero las redes inalámbricas permiten una mayor y más sencilla escalabilidad que las redes cableadas.
- Por limitaciones físicas del edificio: Esto puede ocurrir en edificios alquilados o emblemáticos en donde esta prohibido el hacer instalaciones de cables que puedan perjudicar el estado del edificio.

Dado el modo de operación [5], las redes inalámbricas pueden ser divididas en: redes ad hoc y redes con infraestructura.

1.7.1 REDES INALÁMBRICAS CON INFRAESTRUCTURA (WLAN)

La tecnología WLAN (Wireless Local Area Network; Red de área local inalámbrica) está regida por el estándar 802.11, especificado por el Institute of Electrical and Electronics Engineers (IEEE). Mediante la estandarización se garantiza la interoperabilidad entre diferentes fabricantes y un funcionamiento dentro de las capas del modelo de comunicaciones igual que cualquier otra tecnología de LAN. Por tanto, la interacción de la tecnología WLAN con protocolos de comunicación como TCP/IP es totalmente transparente. De esa forma, la utilización de un adaptador WLAN o uno LAN tradicional no representa ningún cambio desde el punto de vista del sistema operativo.

Actualmente, existen 4 estándares básicos para comunicación inalámbrica en redes locales:

Tabla 1.1 Estándares básicos para comunicaciones inalámbricas en redes locales.

Estándar	*Velocidad*	*Banda*	*Observaciones*
802.11	2 Mbps	2.4 GHz ISM[1]	Es el primero que apareció y también puede operar dentro del espectro infrarrojo
802.11b	11 Mbps	2.4 GHz ISM	Surgió casi inmediatamente después del anterior y actualmente es el sistema más extendido.
802.11a	54Mbps	5 GHz UNII[2]	Se aprobó a la vez que el 802.11b.
802.11g	> a 20 Mbps	2.4 GHz ISM	Es una extensión del 802.11b para mayores anchos de banda.

En términos generales, podemos resumir el funcionamiento de una red inalámbrica con infraestructura de la siguiente forma:

1.- Debe existir uno o varios puntos de acceso responsables de dar cobertura a los clientes en un área determinada, este punto de acceso se encarga de gestionar y administrar las comunicaciones de los clientes, tanto en lo referente a conexiones como en el control de la seguridad.

2.- Por otro lado están las tarjetas clientes, encargadas de comunicarse con el punto de acceso e instaladas en las computadoras, o en los PDA´s.

En la figura 1.2 se muestra el esquema básico de una red inalámbrica, un punto de acceso, su radio de alcance y un dispositivo. El access point se encuentra conectado a la infraestructura de la red y el dispositivo está dentro del radio de cobertura del access point.

Fig. 1.2. Red Inalámbrica tradicional (Original en colores).

En el IEEE se ponen en marcha iniciativas en torno a las redes inalámbricas entre las que destacan [5]:

- Calidad de servicio.
- Operación de puentes.
- Interoperabilidad entre puntos de acceso.
- Extensiones a mayores anchos de banda.
- Mejoras de seguridad.

[1] ISM: Industrial, Scientific and Medical es una frecuencia donde no hace falta licencia para operar.

Además de las mejoras a la seguridad, uno de los puntos más esperados es el estándar sobre calidad de servicio (QoS), denominado 802.11e, para aplicaciones multimedia (como la videoconferencia o el video bajo demanda) además del estándar 802.11g (HiperLan/2) que ofrece compatibilidad con el 802.11b para altas velocidades.

1.7.2 REDES INALÁMBRICAS SIN INFRAESTRUCTURA (ad hoc).

Las redes inalámbricas móviles sin infraestructura son las llamadas redes ad hoc, donde cada nodo funciona como ruteador y tiene la función de descubrir y mantener rutas a otros nodos. En este tipo de redes no se tienen antenas instaladas ya que los nodos que se encuentran en una zona geográfica se atienden a si mismos sirviéndose como puentes para comunicarse.

Los nodos en una red ad hoc son con frecuencia móviles, pero también pueden ser estacionarios, los nodos son libres de entrar y salir en una red como ellos deseen, además de ser una dirección IP válida cada uno puede ser una entidad que entre otras cosas corre un protocolo de ruteo. En este tipo de redes es muy importante tener en cuenta las características de los nodos; capacidad de CPU, almacenamiento, poder de energía y ancho de banda limitados, por lo que la buena administración de estos recursos debe ser considerada.

A lo largo de esta tesis vamos a profundizar con más detalle en las redes ad hoc analizando sus ventajas, desventajas, limitantes y ejemplos del estado del arte de los trabajos presentes y futuros para redes ad hoc.

2 PLANTEAMIENTO DEL PROBLEMA Y OBJETIVOS

2.1 PLANTEAMIENTO DEL PROBLEMA

En nuestros días el uso de la computadora se ha vuelto tan cotidiano como el uso de los vehículos automotores para desplazarnos, cada vez más nuestra sociedad la convierte en un artículo de primera necesidad aunado a los avances tecnológicos y el abaratamiento de la tecnología la computación se vuelve una de las áreas de mayor investigación y crecimiento. Basta con observar a nuestro alrededor que cada vez son más las personas que tienen una computadora en su casa, en su oficina o en la escuela.

En un principio, las computadoras trabajaban corriendo programas de cálculo para un solo usuario, esto ha venido evolucionando a pasos agigantados de tal forma que ahora es una herramienta de trabajo indispensable y las aplicaciones que se le han dado son extremadamente variadas. Uno de los grandes logros que ha tenido la computación es el poder comunicar y compartir información entre las computadoras por medio de una red, esto derivó en la creación de miles de redes de distintos tamaños, desde redes de área local, hasta la red más grande que opera en nuestros días: La Internet.

Las redes se han vuelto la columna vertebral del cómputo para el manejo e intercambio de información entre computadoras, debido a las aplicaciones y servicios que éstas ofrecen. Las redes han venido evolucionando y los medios de transmisión no se limitan a los cables; el desarrollo de las redes inalámbricas ha sido muy bien adoptado principalmente por las ventajas en movilidad que nos ofrecen.

Típicamente las redes se habían venido conceptualizando sobre una infraestructura para su funcionamiento pero su evolución llegó al siguiente nivel, las redes ad hoc son redes inalámbricas sin infraestructura que permiten su creación utilizando las tarjetas como ruteadores y permitiendo la libre comunicación entre los nodos de la red.

Aparte de las computadoras, existen dispositivos inalámbricos como los PDA (Personal Digital Assistant; Asistentes Personales Digitales) de tamaño pequeño y que no necesita de cables para establecer una comunicación además de que su desarrollo tecnológico nos permite comunicarnos con facilidad.

El auge tecnológico que estamos viviendo nos ofrece un nuevo panorama para la creación de redes de menor escala, ya que ahora es factible el poder generar una red con los distintos dispositivos que puedes tener en tu hogar como son: Hornos, Refrigeradores, Video Juegos, PDA’s y Computadoras, donde cada uno de estos dispositivos es un nodo dentro de la red.

Siguiendo con las redes a menor escala encontramos a las PAN (Personal Area Network) que se conforman con dispositivos personales como son teléfonos celulares y asistentes personales. En este tipo de redes se ocupan transmisiones de no largo alcance como lo es BlueTooth o tecnología infrarroja.

Una de las principales preocupaciones dentro del uso de la tecnología inalámbrica es la falta de seguridad en el medio, ya que la información viaja en el aire y se pueden llevar a cabo con facilidad ataques como: Parking lot (lote de estacionamiento) en el cual una persona se sitúa cerca de la red para escuchar que es lo que pasa por ella, aunque ya se tienen desarrollados protocolos como WEP para el cifrado de datos en redes inalámbricas dependemos de la infraestructura.

Las redes ad hoc son redes sin infraestructura y su creación o desaparición es muy dinámica. Un nodo cualquiera puede entrar y salir de la red las veces que requiera por ello el esquema típico de seguridad de una red con infraestructura en donde se tienen las características de seguridad de forma centralizada y siempre disponible no se puede adaptar a un entorno de red ad hoc debido a que los nodos entran y salen de la red y no siempre se tiene a un nodo que pueda certificar a los demás nodos de la red.

Mientras que los temas relacionados con la seguridad en redes ad hoc y redes con infraestructura son diferentes, los requerimientos son los mismos: disponibilidad, confidencialidad, integridad, autenticación y no repudiación, y las investigaciones en el campo de las redes ad hoc se realizan de manera diferente por las constantes de los sistemas como son: microprocesador pequeño, poca memoria, ancho de banda reducido, batería reducida, además de los conocidos ataques de negación de servicios en las redes ad hoc existen otros ataques como la inyección de paquetes, batería exhausta, y ruteo no seguro como cada nodo puede actuar como ruteador, puede afectar gravemente la transmisión de los paquetes.

Existen diversos problemas en las redes ad hoc, pero en esta tesis nos vamos a enfocar al problema de la autenticación.

En la década pasada se ha podido ver un auge en el desarrollo de las tecnologías inalámbricas y microprocesadores, la industria de la electrónica y comunicaciones nos provee ya de varios dispositivos electrónicos de primera necesidad como son: celulares, televisores, asistentes personales y computadoras portátiles, y en un futuro no muy lejano se va a extender a más electrodomésticos para el hogar, no va a ser difícil encontrar cafeteras, estufas, refrigeradores, lavadoras con comunicación inalámbrica dentro del hogar. Cada uno de estos dispositivos tendra la capacidad de conectarse en red y podrá comunicarse sin necesidad de una infraestructura y para lograrlo utilizará redes inalámbricas ad hoc generadas por nodos móviles que no requieren de una infraestructura para comunicarse. Éste tipo de redes mantiene restricciones de acuerdo al tipo de dispositivo.

Entre estas restricciones podemos encontrar:

- Procesadores de baja capacidad de procesamiento.
- Poca memoria y ancho de banda.
- Limitaciones de energía.

Aunque las limitantes de los equipos se han venido superando, las investigaciones en redes ad hoc se han enfocado en la resolución del problema de ruteo. Sin embargo existen otros más que faltan de resolver como es el caso de los servicios de seguridad que nos dejan vulnerables a ataques de negación de servicios, nodos maliciosos, sniffers e inyección de paquetes.

Debido a que en el mundo inalámbrico el medio de transmisión es el aire fácilmente cualquier individuo que se encuentre dentro de perímetro puede extraer la información que circula en la red y si aunamos que las redes ad hoc sufren de diversos cambios en su topología debido a que los nodos entran y salen con gran movilidad nos encontramos bajo un ambiente dinámico y con grandes oportunidades de investigación.

Las redes ad hoc utilizan algoritmos de ruteo como pueden ser: AODV, TORA, DSR. Estos involucran a cualquier nodo que pretenda entrar a la red y tienen como objetivo el envío de información de un nodo origen a un destino, por ello en su lógica se generan uno o múltiples caminos para establecer el canal de comunicación sin tomar en cuenta la autenticación del nodo. Esto provoca que no podamos evitar que uno de los nodos sea malicioso y se quede con la información o que nos encontremos dando servicios a un nodo que es ajeno a la red.

De la misma forma en que se genera una red ad hoc también puede desaparecer debido a la movilidad de sus nodos al entrar y salir de la red sin poderlo controlarlo, esto da como resultado que los esquemas que se utilizan en redes con infraestructura no se puedan adaptar fácilmente a este tipo de redes. Por ejemplo el tener un servidor para centralizar la información sobre la seguridad o como autoridad certificadora no es posible ya que puede no estar alcanzable para algún nodo cuando este la requiera, además una red ad hoc se puede fragmentar y volverse a unir de forma transparente, otros esquemas que incluyen tener distribuidos varios servidores para poder autenticar requieren de una configuración inicial para poder comunicarse entre ellos además de que se puede comprometer la red. En nuestro modelo podemos iniciar con la autenticación desde la creación como lo vamos a ver más adelante.

En la siguiente figura podemos observar las propiedades para una red inalámbrica configurada en modo ad hoc. La autenticación sólo está permitida para aquellas redes con infraestructura ya sea cableada o inalámbrica, en esté caso por medio de WEP hacia el punto de acceso.

Como podemos ver en la figura 2.1 la autenticación en redes ad hoc es un problema que no ha sido resuelto y por lo tanto no se puede ofrecer los demás servicios de seguridad, nuestro modelo es una propuesta para el manejo de la autenticación en redes ad hoc.

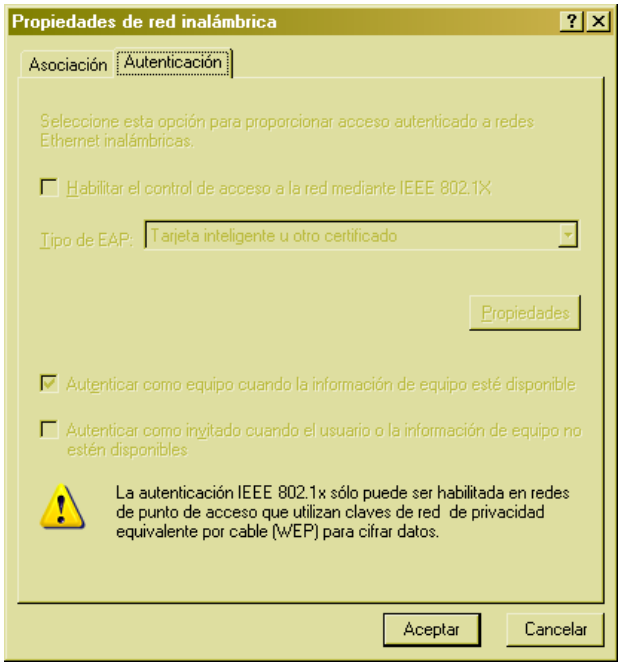

Fig. 2.1 Configuración de redes ad hoc en Windows XP (Original en colores).

La autenticación en los sistemas con infraestructura se lleva a cabo de forma centralizada o distribuida ante entidades que avalan el acceso a la red y cada vez que un usuario entra tiene que proporcionar una característica de seguridad que va a ser utilizada para poder autenticarlo en base a las políticas de seguridad que se tengan, estas características de seguridad pueden ser:

- Usuario y Password.
- Lectores biométricos.
- Lectura de retina.
- Lectura de huella digital.
- Reconocimiento de voz.
- NIP.
- Passwords dinámicos vía tokens.

Estos elementos finalmente terminan siendo comparados con datos almacenados y calculados por una autoridad dentro de la red y permiten o no el acceso, además de aplicar las políticas de seguridad que le correspondan.

2.2 HIPÓTESIS.

Ésta tesis nos va a ayudar a contestar la siguiente hipótesis:

Definir un modelo de autenticación dinámico en redes ad hoc de acuerdo a los distintos escenarios en donde se encuentra un nodo que permitan la creación de una red segura sin tener

una autoridad certificadora basado en niveles de confianza para definir sus políticas de seguridad ofreciendo servicios en base a la confianza que genera entre los nodos de la red.

2.3 OBJETIVOS.

De acuerdo al planteamiento del problema y la hipótesis mencionada los objetivos de nuestra tesis los dividimos en dos generales y seis particulares.

Generales:

- Construir un modelo de autenticación en redes ad hoc basado en los niveles de confianza que pueden generar los nodos entre si a partir de variables difusas configurables definidas.
- Obtener a partir del nivel de confianza la autenticación de los nodos y las políticas de seguridad aplicables a cada uno de ellos dentro de la red.

Particulares:

- Estudiar la lógica difusa como un apoyo para la implementación de variables difusas.
- Generar el modelo difuso para determinar el nivel de confianza entre los nodos.
- Definir las variables que afectan al modelo.
- Generar el mecanismo de inferencia difusa.
- Definir los niveles de confianza con respecto a las políticas de seguridad.
- Presentar los resultados del modelo.

3 REDES ad hoc

3.1 CARÁCTERISTICAS DE LAS REDES ad hoc

Una red ad hoc es un tipo de red formada por un grupo de nodos móviles que generan una red temporal sin la ayuda de infraestructura externa. Para que esto se pueda llevar a la práctica es necesario que los nodos se puedan ayudar mutuamente y así conseguir un objetivo común: “Que cualquier paquete llegue a su destino aunque el destinatario no sea accesible directamente desde el origen”.

Las redes inalámbricas y el cómputo móvil se han integrado sobre redes con infraestructura (redes celulares, satelitales) y se basan en las relaciones preestablecidas entre un subscriptor y un operador, sin embargo, la rápida proliferación de estos dispositivos móviles con la capacidad de conectarse entre si, ha hecho que sea imposible establecer un contrato con cada uno de ellos y aunque fuera posible esto la configuración manual de cada uno podría llegar a ser una tarea muy compleja. Estas razones iniciaron la búsqueda de un nuevo paradigma de comunicación. Las redes ad hoc son la solución, establece relaciones y configuración en automático entre dispositivos.

Las redes del futuro van a utilizar las comunicaciones ad hoc extensivamente para habilitar conectividad para todo mundo sobre cualquier cosa, en cualquier lugar y en cualquier momento, en el centro del mundo inalámbrico estarán las WPAN (redes inalámbricas de área personal), [5].

Un ejemplo muy sencillo de las ventajas de una WPAN es el siguiente: Imaginemos que tenemos por separado dispositivos personales utilizándolos con sus respectivas aplicaciones y no pueden interactuar entre si, ¿Cómo podríamos intercambiar información entre ellos?, tendríamos que tomar en cuenta sus características, periféricos, unidades de almacenamiento entre otras cosas ya que no se encuentran en red. Ahora imaginemos el mismo escenario con los mismos dispositivos interactuando directamente entre si creando una red donde la información fluye entre ellos. Este tipo de redes se les conoce como PAN (Personal Area Network).

Este tipo de redes pueden constantemente estar en línea cuando se cuenta con una conexión a la infraestructura vía WLAN, 3G UMTS o GPRS. Por su naturaleza este tipo de redes son muy volátiles, es por ello que el concepto de ad hoc puede ser aplicado para crear una conectividad robusta y flexible, [6].

En la Figura 3.1 vemos un esquema en donde cuatro PAN's se encuentran interconectadas entre si, una de ellas cuenta también con un acceso a Internet vía WLAN y otra tiene acceso vía GPRS.

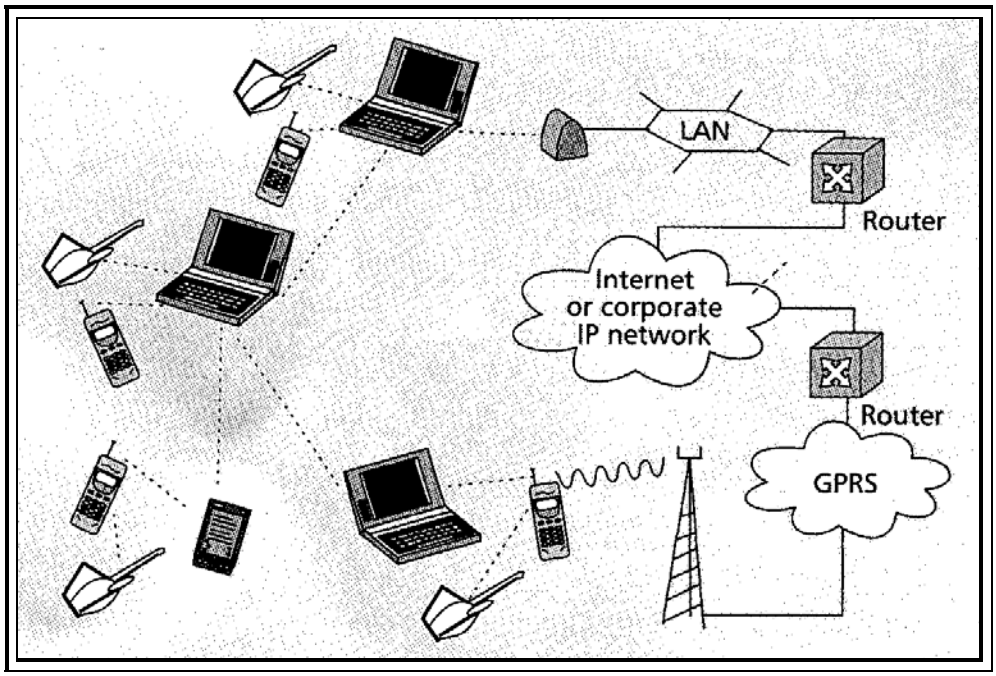

Fig. 3.1. WPAN's Interconectadas.

En general, las redes ad hoc se definen como: "Redes formadas por usuarios o dispositivos queriéndose comunicar sin la necesidad de la ayuda o existencia de infraestructura y sin haber establecido relaciones entre los miembros potenciales de la red", [7]. Las redes ad hoc se forman por un conjunto de nodos que se quieren comunicar cada uno por un canal inalámbrico.

Cada nodo tiene la habilidad de conectarse con otro en su vecindario físico, un paquete de red es enviado a su destinatario a través de un conjunto de nodos intermedios que actúan como ruteadores para su retransmisión.

En la Figura 3.2 se muestra una sencilla red ad hoc, el nodo origen quiere enviar un paquete al nodo destino pero éste se encuentra fuera del alcance de su área de transmisión (representado por círculos en la figura) por lo que es necesario que los nodos intermedios formen parte de la ruta de transmisión y retransmitan el paquete, como se puede observar existen distintas rutas por las cuales puede viajar el paquete. En el ejemplo la ruta utilizada para el envío del paquete de datos es representada por flechas.

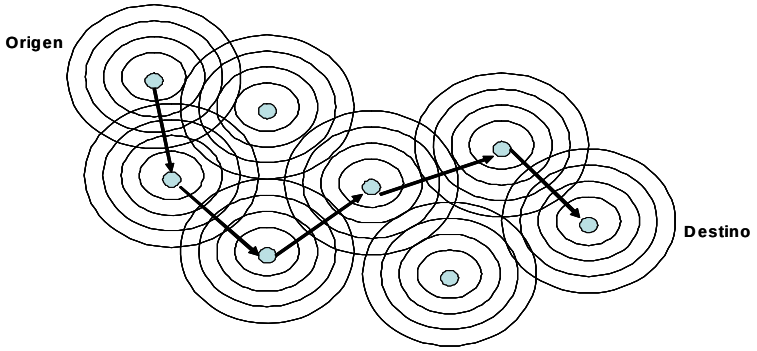

Fig. 3.2 Red ad hoc.

Algunos ejemplos de aplicaciones de redes ad hoc son:

- Tácticas militares.
- Emergencias.
- Misiones de rescate.
- Salones virtuales.
- BAN (Redes de área corporal).
- Redes de sensores.
- Redes vehiculares.
- Redes de área personal (WPAN).
- Análisis de datos en terrenos catastróficos.

En la Figura 3.3 se muestran un par de aplicaciones de las redes ad hoc con dos diferentes objetivos, el primero para la atención a emergencias y el segundo para tácticas militares.

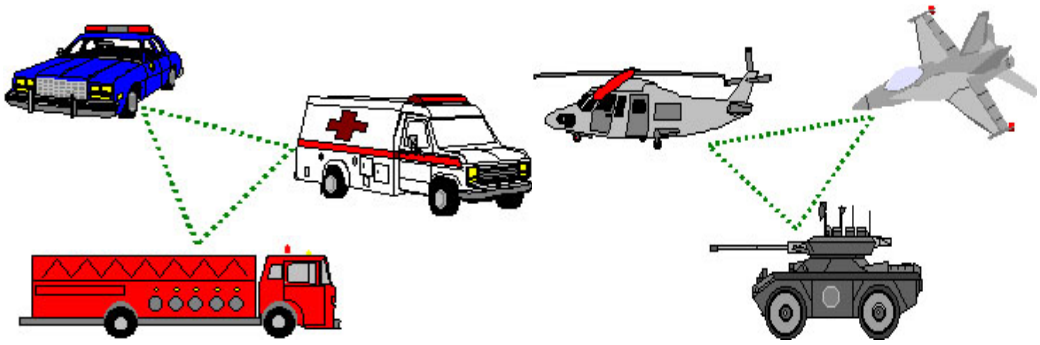

Fig. 3.3. Aplicaciones de redes ad hoc.

Cada nodo en una red ad hoc tiene las funciones de nodo, ruteador y control de la red. Dado que la conectividad en cada uno de los nodos varia la topología de la red es dinámica esto significa

que al mismo tiempo que un nodo sale, nuevos nodos arriban y la posibilidad de tener nodos móviles es amplia.

El párrafo anterior implica la necesidad de tener un protocolo de ruteo eficiente que permita a los nodos comunicarse sobre distintos caminos, de múltiples saltos en varios enlaces, de forma que no se utilicen más recursos de los necesarios.

Las redes ad hoc a su vez pueden ser divididas en dos grandes tipos: Redes móviles ad hoc (MANETS) y redes de sensores inteligentes.

El estudio de las redes ad hoc presenta gran variedad de problemas abiertos a la investigación y oportunidades de hacer aportaciones significativas al área, [8], principalmente en ruteo, seguridad, direccionamiento y diseño de la capa MAC.

3.2 REDES MÓVILES ad hoc (MANETS).

Este tipo de redes inalámbricas representa la próxima generación de redes de área local y se encuentran respaldadas por la necesidad del rápido desarrollo de usuarios móviles independientes. Una red ad hoc no puede contar con una conectividad centralizada, las MANETS son una colección autónoma de usuarios móviles que se comunican relativamente sobre un ancho de banda construido con enlaces inalámbricos, dado que los nodos son móviles, la topología de la red puede cambiar de manera rápida e impredecible sobre el tiempo. Las redes se descentralizan y toda su actividad, incluyendo el descubrimiento de la topología y entrega de mensajes, deben ser ejecutados por los nodos mismos.

El conjunto de aplicaciones para MANETS es muy diverso y va desde la más pequeña red estática construida con fuentes de poder hasta las redes móviles de larga escala altamente dinámicas. El diseño de protocolos de ruteo para este tipo de redes es un tema complejo. A pesar de ello, las aplicaciones para MANET’S necesitan algoritmos distribuidos eficientes para determinar la organización de la red, el plan de enlaces y de ruteo. Como siempre, determinar la ruta viable y los caminos de entrega de mensajes en un ambiente descentralizado donde la topología de la red fluctúa es un problema no bien definido por la movilidad que se encuentra en la red. Mientras el camino más corto (basado sobre la función de costo dada) de una fuente a un destino en una red estática es usualmente la ruta óptima, esta idea no es tan fácil de extender a una MANET.

Algunas de las ventajas de las MANET’S son:

- Fácil instalación y escalabilidad.
- Bajo costo de mantenimiento.
- Mayor flexibilidad.
- Facultad de utilizar nuevos y eficientes protocolos de comunicación inalámbrica.

Supongamos que queremos conectar dos pisos de oficinas utilizando mecanismos inalámbricos de bajo rango. Cada empleado cuenta con su propio dispositivo móvil y existen además algunos dispositivos fijos como las impresoras. La conexión se podría dar directamente a la infraestructura a través de un punto de acceso sin embargo esta solución ofrece una movilidad limitada y adhiere carga a la red cableada, otra solución sería el construir una red dedicada, con estaciones base habilitadas con comunicación celular, pero esto es muy caro con respecto a la instalación y mantenimiento. La mejor solución es crear una red ad hoc en la que se utilizan los dispositivos inalámbricos como conmutadores intermedios si es que se encuentran desocupados y puedan llevar a cabo esta tarea, [9].

Por ejemplo, el paquete de un dispositivo puede saltar a un teléfono móvil de otra persona, pasando de ahí al otro que se encuentra enfrente, de ahí a una impresora láser de la siguiente oficina, de ahí a una pulsera digital en el piso de abajo, de la pulsera digital a la máquina de café y finalmente de la máquina de café al dispositivo destino.

Algunas aplicaciones de las MANET's son:

- Manejo de desastres naturales: incendios, inundaciones o terremotos. Los rescatistas pueden generar una red ad hoc en el momento para compartir información.
- Industria.
- Aplicaciones comerciales que involucren intercambio cooperativo móvil de datos.
- Alternativas económicas o aumento para la infraestructura de redes celulares móviles (cell-based).

Los conceptos y los requerimientos asociados a la idea de las MANET'S son discutidos en la literatura del computo móvil y redes, algunos documentos notables y estándares se pueden encontrar en MANET Working Group, [10], de la Internet Engineering Task Force (IETF).

3.3 REDES DE SENSORES INTELIGENTES.

Las redes de sensores inteligentes consisten de una variedad de sensores extendidos de un lado a otro en un área geográfica, cada sensor cuenta con la capacidad de procesar señales y datos en red de forma inalámbrica, aumentando así la eficiencia operativa de las aplicaciones que los utilizan. El objetivo básico de una red de sensores inteligentes generalmente depende más del objetivo de la aplicación que de las capacidades de los sensores mismos.

Podemos clasificar las redes de sensores inteligentes de dos formas: Si los nodos son o no individualmente direccionados y si los datos en la red son totalizados. Por ejemplo, los nodos de sensores en un estacionamiento podrían estar direccionados individualmente, para que cada uno pueda determinar si las localizaciones de espacios que monitorean están libres, con esta aplicación se muestra que puede ser necesario transmitir un mensaje a todos los nodos en la red.

Si se requiere determinar la temperatura en una esquina de un cuarto, entonces el direccionamiento no es tan importante, cualquier nodo en la región dada puede responder. La habilidad de las redes de sensores para totalizar los datos colectados puede reducir el número de mensajes que se necesitan ser transmitidos sobre la red.

Algunos ejemplos de redes de sensores inteligentes son:

- Redes ambientales: Sirven para conocer datos como temperatura, presión atmosférica, cantidad de luz solar y humedad
- Redes para tráfico: Se pueden ocupar para detectar vehículos en movimiento a través de intersecciones estimando velocidad y dirección del vehículo.
- Redes para clasificación: Sirven para la determinar objetos detectados.
- Redes para obtener rutas de objetos: Sirve para mostrar la ruta de un objeto que se mueve a través de la red.

3.4 PROTOCOLOS DE RUTEO EN REDES ad hoc.

El protocolo de ruteo tiene dos funciones principales, selección de rutas para varios pares de nodos origen-destino y la entrega de mensajes en sus destinos correctos.

Algunas propiedades deseables en los protocolos ad hoc, [11]:

- Operación distribuida.
- Libre de ciclos.
- Operación basada en demanda.
- Soporte para conexiones unidireccionales.
- Seguridad.
- Conservación de energía.
- Rutas múltiples.
- Soporte para QoS *(Quality of Service, Calidad de Servicio).*

Ninguno de los protocolos propuestos hasta el momento cuentan con todas estas propiedades, pero; es necesario recordar que los protocolos ad hoc aún están en desarrollo. La función primordial es aún encontrar una ruta al destino, no encontrar la mejor ruta, óptima o el camino más corto.

Dependiendo de sus características, los protocolos de ruteo en redes ad hoc pueden clasificarse como: Proactivos y Reactivos (o bajo demanda). Por una parte, en los protocolos proactivos, periódicamente se envía información de encaminamiento para que en cualquier momento cualquier nodo pueda comunicarse con cualquier otro de la red, los protocolos reactivos sólo crean las rutas cuando es necesario, [20].

3.4.1 PROTOCOLOS DE RUTEO ad hoc PROACTIVOS.

El llamado protocolo proactivo; es aquel donde cada nodo mantiene una o varias tablas de rutas a todos los destinos de la red. Estas tablas con rutas son actualizadas constantemente, incluso cuando los nodos no necesiten enviar algún mensaje. Los protocolos proactivos pierden más tiempo actualizando sus tablas de rutas, siendo esto una desventaja cuando la topología de la red cambia con mucha frecuencia, ya que muchas de las rutas que tiene como actuales, en un momento dado, pueden ser ya obsoletas al siguiente segundo. Este tipo de protocolo es más recomendado para redes ad hoc semidinámicas.

3.4.1.1 Dsdv.

El protocolo de ruteo DSDV (Destination-Sequenced Distance-Vector, Vector de Distancias con Destino Secuenciado), es una propuesta de Charles E. Perkins y Pravin Bhagwat, [12], donde se modifican los mecanismos de ruteo del Bellman-Ford básico. El protocolo resultante es un protocolo de ruteo para redes ad hoc móviles. Entre las principales mejoras hechas al algoritmo Bellman-Ford sobresale el manejo de rutas libres de ciclos.

El protocolo DSDV funciona de la siguiente manera: Cada nodo móvil en la red ad hoc mantiene una tabla de rutas a todos los destinos posibles. Para mantener la consistencia de dichas tablas en una topología variable dinámicamente, cada nodo transmite periódicamente a sus vecinos, actualizaciones de rutas, mediante broadcast o multicast, y transmite actualizaciones tan pronto como obtenga nueva información sobre rutas. Cada entrada de las tablas de ruteo contiene los siguientes datos:

- Dirección del nodo destino.
- Número de nodos a visitar para alcanzar el destino.
- Un número de secuencia de la ruta, originada por el nodo destino.

Debido a las características del medio de transmisión en redes inalámbricas, pueden presentarse conexiones unidireccionales, las cuales son más difíciles de manejar que las conexiones bidireccionales. Para evitar la inserción de rutas que contengan conexiones unidireccionales en las tablas de ruteo, el protocolo asegura que un nodo *x* no almacene rutas que vienen de un vecino *y* al menos que *y* compruebe que puede recibir paquetes de *x*. Por lo tanto, el presente algoritmo de ruteo utiliza únicamente conexiones bidireccionales.

Cuando se necesita que la red ad hoc interactúe con una red cableada, DSDV maneja las direcciones de las estaciones base de dicha red cableada como direcciones fijas en las tablas de ruteo. De esta forma los nodos móviles de la red ad hoc pueden alcanzar a otros nodos lejanos, transmitiendo los paquetes a través de una red cableada o bien, visto desde otra perspectiva, las estaciones base de una red pueden alcanzar a nodos móviles lejanos mediante ruteo de paquetes a través de nodos de una red ad hoc.
DSDV también contempla la utilización de direcciones MAC (Media Access Control, Control de Acceso al Medio), de la capa 2 de redes, para la especificación de las direcciones de los nodos. Es

decir, que puede ser implementado para funcionar tanto con direcciones de red de la capa 3, como con direcciones MAC de la capa 2. En el caso de las direcciones MAC, el único inconveniente es que dado que los protocolos de red de la capa 3 manejan direcciones de red, es necesario proporcionar un método para pasar a través de las direcciones MAC, las direcciones de red. La solución que los autores proponen es la inclusión en cada uno de los nodos, tanto de la información del protocolo de la capa 3 como la información del protocolo de la capa 2.

La propiedad más importante de este protocolo es que garantiza que no se formen rutas que contengan ciclos. Para evitar la formación de ciclos en las rutas se procede de la siguiente manera. La ruta a un destino *x* en una tabla *i*, sólo será actualizada por otra ruta al nodo *x* si alguna de las siguientes dos cosas pasan:

- La nueva ruta contiene un número de secuencia más reciente.
- El número de secuencia es el mismo que el número de secuencia actualmente almacenado pero, la nueva ruta ofrece un camino más corto.

3.4.2 PROTOCOLOS DE RUTEO ad hoc REACTIVOS.

Los protocolos reactivos son aquellos que comienzan su proceso de búsqueda de rutas en el instante en que un nodo necesita una ruta para enviar paquetes a otro nodo. En general, por la manera en que funciona, este tipo de protocolo es más adecuado para redes donde los nodos están en constante movimiento.

3.4.2.1 Aodv.

El protocolo ad hoc On-Demand Distance Vector (AODV). Descrito en, [13], se construye a partir del DSDV descrito anteriormente. AODV es una mejora del DSDV porque típicamente minimiza el número broadcasts requeridos para crear rutas por demanda, a diferencia de mantener una lista completa de rutas como en el caso del algoritmo DSDV. Los autores del AODV lo clasifican como un sistema de adquisición de rutas por demanda puro, debido a que los nodos que no están en una ruta seleccionada no mantienen información de rutas ni participan en ningún intercambio de tablas de rutas.

Cuando un nodo origen desea mandar un mensaje a algún nodo destino y no tiene aún una ruta válida al destino, entonces inicia proceso de descubrimiento de ruta para localizar al otro nodo. El nodo envia un paquete broadcast de solicitud de ruta RREQ a sus vecinos, los cuales posteriormente reenvían la solicitud a sus vecinos, y así sucesivamente, hasta que se llega al nodo deseado o bien, se llega a un nodo que tenga una ruta actual al nodo destino. AODV utiliza números de secuencia de destinos para asegurar que todas las rutas estén libres de ciclos y contienen la información de enrutamiento más reciente. Cada nodo mantiene su propio número de secuencia así como su ID de broadcast. El número de ID de broadcast es incrementado cada vez que es iniciado un RREQ y se identifica de manera única un RREQ mediante la dirección IP del nodo. Los nodos intermedios pueden contestar el RREQ solamente si poseen una ruta al

destino deseado, cuyo número de secuencia correspondiente sea mayor o igual que el contenido en el RREQ.

Durante el proceso de reenviar paquetes RREQ, los nodos intermedios graban en sus tablas de rutas las direcciones de los vecinos de los cuales reciben las copias de los paquetes, y de esta forma establece una ruta de regreso. Una vez que el paquete RREQ llega al destino a un nodo intermedio con una ruta actual al destino, responde enviando un paquete de respuesta RREP al nodo de donde recibió el mensaje RREQ. Mientras que el paquete RREP es reenviado a través de la ruta de regreso, los nodos a lo largo de la ruta van actualizando sus tablas de rutas que apuntan al nodo de donde reciben el RREP. Estas nuevas rutas indican son las rutas activas. Además se asocia a cada ruta un cronómetro de vida, después de cierto tiempo las rutas se van borrando de las tablas. Debido a que AODV reenvía los paquetes a lo largo de la ruta establecida por los RREQs, AODV sólo soporta el uso de enlaces simétricos.

Las rutas son administradas de la siguiente forma. Si un nodo origen se mueve, se llama a la rutina de descubrimiento de ruta, para encontrar una nueva al nodo destino. Si se mueve un nodo localizado a lo largo de una ruta, sus vecinos notan que se ha movido o desaparecido y propagan un mensaje de notificación de fallo de enlace (un RREP con métrica infinita), a cada uno de sus respectivos vecinos hace lo mismo sucesivamente hasta que este paquete de notificación llega al nodo origen. El nodo origen entonces decide si llama de nuevo a la rutina de descubrimiento de ruta dependiendo si la ruta aun se requiere.

3.4.2.2 Dsr.

El protocolo Dynamic Source Routing (DSR) propuesto por David B. Johnson y David A. Maltz, [14], se compone de dos rutinas básicas: descubrimiento de rutas y mantenimiento de rutas. Cuando un nodo requiere una ruta a un destino, genera una ruta conteniendo todos los nodos que deben ser visitados hasta llegar al destino. Esta ruta creada es almacenada entonces en la cabecera de cada uno de los paquetes que necesiten ser transmitidos al nodo destino. Entonces, el nodo origen envía el paquete al primer nodo en la ruta. Si este nodo no es el nodo destino simplemente retransmite el paquete al siguiente nodo especificado en la ruta. Cuando el paquete llega a su destino el paquete es entregado al software de la capa de red de ese nodo.

Cada nodo móvil mantiene una caché donde almacena todas las rutas que ha aprendido. Cuando un nodo envía un mensaje a otro, primero checa si en su caché tiene ya una ruta al nodo deseado. Si la ruta ya existe en su caché, utiliza esa ruta. Si la ruta no existe en la caché entonces el nodo intenta descubrir una ruta ejecutando su rutina de descubrimiento de rutas. Mientras espera por una ruta, puede continuar con sus tareas ya programadas y puede seguir intercambiando paquetes con otros nodos. El nodo puede guardar en un buffer el mensaje original para poder enviarlo posteriormente cuando ya se cuente con una ruta al destino o bien, puede descartar el paquete, dejando la responsabilidad de la retransmisión del paquete al software de una capa más arriba. Cada entrada en la tabla de caché en los nodos tiene asignado un período de expiración, después del cual la entrada es eliminada de la caché.

Cuando un nodo inicia una búsqueda de ruta envía un mensaje de broadcast en la red, con un paquete de solicitud de ruta. El paquete de solicitud contiene la identificación del nodo destino. El paquete viaja por la red hasta llegar al nodo destino. Si este proceso se realiza con éxito, el nodo que originó la solicitud de ruta recibe un paquete de respuesta de ruta conteniendo la secuencia de nodos que deben ser visitados para llegar hasta el destino. Además de la dirección del nodo de origen y del nodo destino, el paquete de solicitud guarda la secuencia de nodos que visita hasta llegar al destino. Asimismo, cada uno de estos paquetes posee un número único de identificación. El número de identificación de solicitud junto con la dirección del nodo que originó el mensaje, ayudan a evitar la generación de rutas duplicadas.

Mientras un nodo utiliza una ruta, se mantiene monitoreando que funcione correctamente. Por ejemplo, si uno de los nodos pertenecientes a una ruta en especifico se sale del rango de transmisión del nodo inmediato anterior o posterior en la ruta, entonces esa ruta ya no es válida y los paquetes enviados por ella no logran llegar a su destino. Una ruta también puede fallar si uno de los nodos en ella falla o se apaga por razones de energía. A este monitoreo de las rutas se le refiere como mantenimiento de rutas. Cuando la rutina de mantenimiento de rutas detecta un problema con alguna ruta en uso, se utiliza la rutina de descubrimiento de rutas para descubrir una nueva ruta al nodo destino.

3.4.2.3 Tora.

El protocolo TORA (Temporally-Ordered Routing Algorithm, Algoritmo de Ruteo Temporalmente Ordenado), fue propuesto por Vincent D. Park y M. Scott Corson, [15]. Este algoritmo está diseñado para minimizar la reacción a cambios en la topología de la red. Desde el punto de vista de los autores, un algoritmo bien diseñado para ambientes como los de las redes ad hoc debe contar con las siguientes propiedades:

- Ejecutarse distribuidamente
- Proporcionar rutas libres de ciclos
- Proporcionar múltiples rutas (para aliviar el congestionamiento)
- Establecer rutas rápidamente (para que puedan ser utilizadas antes de que cambie la topología)
- Minimizar el overhead localizando reacciones algorítmicas a cambios en la topología cuando sea posible (para mantener el ancho de banda e incrementar la escalabilidad)

El funcionamiento del TORA es de la siguiente manera. Cada vez que se requiera una ruta a nodo destino se ejecuta una versión lógica separada del protocolo. El protocolo puede separarse en tres funciones básicas: creación de rutas, manutención de rutas y borrado de rutas.
Para la creación de una ruta de un nodo dado al destino se requiere el establecimiento de una secuencia de ligas dirigidas que conduzcan del nodo al destino. Esta función sólo se inicia cada vez que un nodo sin ligas dirigidas requiere una ruta a un destino. Así podemos decir que la creación de rutas consiste en asignar direcciones a las ligas de una red o porción de una red. Para lograr esto se construye un grafo aciclico dirigido con raíz en el nodo destino.

La manutención de rutas se refiere a reaccionar a cambios en la topología de la red de forma tal que las rutas al destino puedan ser re-establecidas en un tiempo finito. Al momento de detectarse una partición de la red, todas las ligas (en la porción de la red que ha quedado particionada desde el destino) deben quedar sin dirección.

El protocolo logra estas tres funciones mediante el uso de tres paquetes de control distintos: de solicitud (QRY), de actualización (UPD), y de limpieza (CLR). Los paquetes QRY son usados para crear rutas, los paquetes UPD son usados tanto para crear rutas como para mantenerlas y los paquetes CLR son utilizados para borrar rutas.

TORA asocia una altura a cada nodo en la red. Todos los mensajes fluyen de nodos con mayor altura hacia nodos con menor altura. Cuando un nodo no tiene algún vecino con una altura menor a la de él mismo, entonces envía un mensaje QRY a toda la red. Este mensaje QRY se propaga hasta encontrar un nodo que tenga una ruta al destino deseado o bien, hasta que el paquete llegue al destino. Entonces ese nodo genera un paquete UPD que contiene la altura del nodo. El paquete UPD es enviado a todos los nodos de la red y conforme los nodos vayan recibiendo este paquete, deben de ir actualizando sus propias alturas con valores mayores que el especificado en el mensaje UPD. A su vez cada nodo que recibe un paquete UPD envía su propio mensaje UPD a los demás nodos de la red. Con esta serie de acciones se obtiene un número de ligas dirigidas que van desde el nodo que originó el paquete QRY hasta el nodo destino.

4 SEGURIDAD.

La masiva utilización de las computadoras y redes como medios para almacenar, transferir y procesar información se ha incrementado en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

Se entiende por seguridad de los sistemas de información al conjunto de recursos:

- Metodologías.
- Planes.
- Políticas.
- Documentos.
- Programas ó dispositivos físicos.

Todos ellos encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo, el objetivo de la Seguridad Computacional es el de detectar, prevenir, detener y corregir las violaciones de seguridad que involucra la transmisión de información.

La seguridad se puede definir como: “El conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema”.

4.1 TIPOS DE SEGURIDAD

La seguridad en una organización es un tema muy amplio y complejo, pero en general lo podemos dividir en dos:

- Seguridad Física.
- Seguridad Lógica.

4.1.1 SEGURIDAD FÍSICA

La seguridad física es un subsistema de la organización que consta de dos áreas principales: Seguridad del personal y Seguridad del material y equipo. Actualmente las empresas empiezan a comprender la importancia de mantener buenos sistemas de seguridad que protejan tanto a las personas como al equipo de trabajo.

La seguridad del personal tiene como objetivo eliminar el riesgo de los accidentes de trabajo, alejando al individuo de ese riesgo, el material y equipo de trabajo son activos importantes para toda organización ya que con ellos puede ejercer la actividad principal de la organización.

Como herramienta de seguridad podemos utilizar el análisis de riesgo, cuyo objetivo principal es ayudar a seleccionar medidas de protección de costo adecuado y nos sirve para identificar amenazas, vulnerabilidades y medidas de protección para reducir el impacto de que una amenaza se concrete.

Aunque nuestra tesis no se va a enfocar en la seguridad física es muy importante su estudio e implementación.

4.1.2 SEGURIDAD LÓGICA.

La seguridad lógica involucra la definición de métodos y procedimientos para cumplir con los objetivos de la organización implantando políticas y mecanismos de seguridad.

Toda organización tiene que fomentar una cultura de la seguridad y aunque el objetivo de este trabajo no es la definición ni implementación de políticas, es importante recalcar que forman parte de cualquier departamento de seguridad.

Los mecanismos de seguridad son técnicas o métodos que implementan uno o más servicios de seguridad, cada servicio garantiza la seguridad de los datos que residen en un nodo o que circulan en una red. La mayoría de los mecanismos actuales se basan en la criptografía, podemos clasificar los diferentes tipos de mecanismos en:

- Mecanismos de Prevención: Estos mecanismos nos sirven para proteger la información de nuestra organización previniendo accesos no autorizados, podemos citar el uso de una buena configuración de equipos, los antivirus, firewalls, el uso de kerberos, secure shell etc.

- Mecanismos de Detección: Estos mecanismos nos sirven para monitorear nuestra red de accesos indebidos por medio de sniffers u otras herramientas de monitoreo.
- Mecanismos de Recuperación: Estos mecanismos nos ayudan a recuperar la información en caso de que se presente un incidente, principalmente se apoya en un plan de contingencia, en donde se estipulan las acciones a seguir cuando ha ocurrido o esta ocurriendo un incidente de seguridad.

4.2 SERVICIOS DE SEGURIDAD.

Hoy en día, ninguna organización puede ignorar el uso de mecanismos de seguridad para protegerse de accesos no autorizados que puedan comprometer la confidencialidad, integridad y disponibilidad de su información.

El tema de la seguridad en redes es muy amplio y se aplica a distintos niveles, como lo son los protocolos, las aplicaciones, las personas, las restricciones de acceso etc.

Los problemas que se tienen para las comunicaciones inalámbricas son muchos y muy variados, dependientes de variables tanto físicas como operativas. Sin embargo podemos converger en un tema que es preocupante para toda empresa y es la seguridad de la información. Las comunicaciones entre dispositivos para el intercambio de información siempre ha sido el tema principal, pero los servicios que proporcionan las redes no se limitan sólo a ello, es aquí donde la seguridad en una red cobra vital importancia, ya que el acceso y manejo de la información se ha vuelto el pilar de toda industria y, por lo tanto, su manejo es restringido. Si bajo un medio de transmisión físico controlado, como puede ser el cableado estructurado, se registran múltiples incidentes de seguridad más aun se van a presentar cuando el medio de transmisión son ondas electromagnéticas que viajan en el aire y que pueden ser recibidas y/o capturadas por *n* cantidad de dispositivos.

En ésta que es la era de la información, la seguridad toma un rol preponderante en toda empresa y es que la información se tiene que cuidar y proteger.

El problema principal, no se encuentra sólo en la escuchar de las comunicaciones de terceros y la consiguiente obtención de información útil, sino también en la accesibilidad a las máquinas que forman parte de la red por parte de los intrusos. El cable obliga a las comunicaciones de la red a pasar por un camino predeterminado para poder acceder a la información y los intrusos tratan de encontrar un punto de conexión para entrar a la red y formar parte de ella. Sobre este tipo de caminos se pueden aplicar medidas concretas (como la aplicación de firewalls), pero en el entorno inalámbrico, las comunicaciones viajan por el aire y, por lo tanto, todo el mundo dentro del área de alcance de la red puede escucharlas.

La conclusión a la que se llega es que, si bien una red local inalámbrica facilita tareas administrativas y de infraestructura, también implica un conjunto de premisas que hay que considerar muy seriamente desde el punto de vista de la seguridad durante su concepción.

Uno de los aspectos que más preocupa a los usuarios es el tema de la seguridad, cuando hablamos de redes inalámbricas se nos viene a la mente la imagen de alguien que ha subido a una escalera con una pequeña antena intentando captar las ondas inalámbricas que atraviesan nuestra oficina para robarnos datos. Sin embargo, la infraestructura alámbrica como la inalámbrica cuentan con el mismo grado de seguridad lo que lleva a la pregunta ¿Dónde estará más cómodo un hacker? ¿Debajo de nuestra ventana con una sombrilla o un paraguas para intentar captar parte de la información o cómodamente sentado en su mesa, atacando nuestra red desde su computadora? El mensaje desde este punto de vista sería que las redes inalámbricas son tan seguras como el cable, si son bien utilizadas ya que no existen redes 100 por ciento seguras y si el Pentágono ha sido hackeado, ¿Qué empresa va a estar más segura que una institución militar norteamericana?.

La realidad es que los problemas de seguridad que afectan a una red inalámbrica son los mismos que afectan a una red basada en cable. Es incorrecto pensar que la información transmitida sobre el cable está más protegida y, lamentablemente, es igual de difícil encontrar una red local, ya esté basada en cable o no, que sea una auténtica isla y que no corra riesgos de accesos no autorizados.

Un clásico ejemplo de ataque a una red inalámbrica es el ataque de estacionamiento que se grafica en la Fig. 4.1, en este ataque el intruso se sienta en el estacionamiento fuera del edificio pero dentro del alcance de la red para atacar máquinas desde ahí.

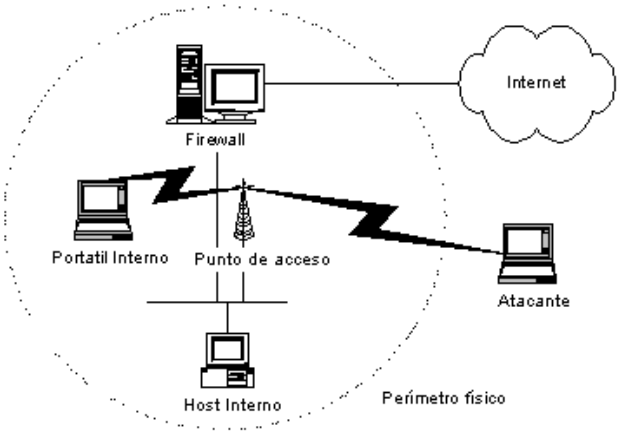

Fig. 4.1 Ataque de Estacionamiento

Las corporaciones están preocupadas por la seguridad, es por ello que utilizan los algoritmos de encripción para generar canales seguros. Dentro de las redes inalámbricas se utilizan distintos algoritmos como son: Wired Equivalent Privacy (WEP) y Wi-Fi Protected Access (WPA).

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios de seguridad son requerimientos que deben cumplir los sistemas de comunicación, haciendo uso de uno o varios mecanismos de seguridad, [16]. Una clasificación útil de los servicios de seguridad es la siguiente:

4.2.1 AUTENTICACIÓN.

Ya sabemos que dentro de los requerimientos primordiales de los sistemas informáticos son los mecanismo de seguridad adecuados a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como archivos o recursos de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retinales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, en la computación existe una gran diferencia entre ellos. Imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector, y el sistema sería capaz de decidir si es un usuario válido, y en ese caso decir de quién se trata; esto es identificación. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario.) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo comprobando los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser y estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido.

Nos permite comprobar la identidad de usuarios, entidades homologas, orígenes de datos por medio de ciertos mecanismos. Este servicio corrobora la fuente de una unidad de datos. La autenticación puede ser sólo de la entidad origen o de la entidad destino, o ambas entidades se pueden autenticar la una o la otra. Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

Los métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad:

- Algo que el usuario sabe.
- Algo que éste posee.
- Una característica física del usuario o un acto involuntario del mismo.

4.2.2 CONTROL DE ACCESO.

El control de acceso constituye una poderosa herramienta para proteger la entrada a un sistema o red habilitando sólo a ciertos directorios concretos e incluso a archivos o programas individuales. Este control consta generalmente de dos pasos:

- En primer lugar, la autenticación, que identifica al usuario o a la máquina que trata de acceder a los recursos, protegidos o no.
- En segundo lugar, procede la verificación de permisos, es decir, la autorización, que dota al usuario de privilegios para poder efectuar ciertas operaciones con los datos protegidos, tales como leerlos, modificarlos, crearlos, etc.

El control de acceso, permite proteger los recursos del sistema contra su uso no autorizado, se basa en credenciales y atributos de usuarios ya autenticados, requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación. Este servicio se utiliza para evitar el uso no autorizado de recursos. Este mecanismo se utiliza para autenticar las capacidades de una entidad, con el fin de asegurar los derechos de acceso a recursos que posee. El control de acceso se puede realizar en el origen o en un punto intermedio, y se encarga de asegurar si el emisor está autorizado a comunicar con el receptor y/o a usar los recursos de comunicación requeridos. Si una entidad intenta acceder a un recurso no autorizado, o intenta el acceso de forma impropia a un recurso autorizado, entonces la función de control de acceso rechazará el intento, al tiempo que puede informar del incidente, con el propósito de generar una alarma y/o registrarlo.

4.2.3 CONFIDENCIALIDAD.

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere ala capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. La confidencialidad asegura que los usuarios pueden acceder a la información que les está permitida en base a su grado o nivel de autoridad en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados,

documentos internos sobre estrategias, nuevos productos o campañas, etc. Algunos de los mecanismos utilizados para salvaguardar la confidencialidad de los datos son:

- El uso de técnicas de control de acceso a los sistemas.
- El cifrado de la información confidencial o de las comunicaciones.

Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación [19].

4.2.4 INTEGRIDAD.

Permite proteger los datos de ataques activos. Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que los bloques o unidades de datos recibidas no han sido alteradas y que no hay unidades repetidas o perdidas, por ejemplo mediante time stamps. Es necesario diferenciar entre la integridad de una unidad de datos y la integridad de una secuencia de unidades de datos ya que se utilizan distintos modelos de mecanismos de seguridad para proporcionar ambos servicios de integridad. Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor. Para proporcionar la integridad de una unidad de datos la entidad emisora añade a la unidad de datos una cantidad que se calcula en función de los datos. Esta cantidad, probablemente encriptada con técnicas simétricas o asimétricas, puede ser una información suplementaria compuesta por un código de control de bloque, o un valor de control criptográfico. La entidad receptora genera la misma cantidad a partir del texto original y la compara con la recibida para determinar si los datos no se han modificado durante la transmisión.

4.3 MODELOS Y POLÍTICAS DE SEGURIDAD.

Un modelo de seguridad proporciona una representación semántica que describe las propiedades funcionales y estructurales de la seguridad de nuestro sistema. Permite trabajar con una definición de alto nivel de los requerimientos de protección y las políticas de seguridad así como producir una descripción concisa y precisa del comportamiento esperado del sistema. Una política de seguridad define las expectativas de nuestra organización en cuanto a seguridad, tomando las decisiones necesarias para completar el diseño previsto en el modelo de seguridad, estableciendo las reglas y procedimientos necesarios para garantizarla. Finalmente, ambos diseños se implementan mediante procedimientos de seguridad que se recogen en el manual de seguridad.

Una referencia importante en esta área es el denominado libro naranja (orange book), que durante años ha procurado un estándar para la evaluación de sistemas. Divide los sistemas en cuatro categorías (algunas se subdividen en clases) en función de los requerimientos que satisfacen. La categoría más baja es la D, que corresponde a sistemas que, tras ser evaluados, no satisfacen los requerimientos de las categorías superiores. La siguiente categoría, la C, se divide en dos clases, C1 y C2, e introduce controles de acceso discrecionales. La categoría B, con tres clases B1, B2 y B3, introduce controles de acceso obligatorios. La categoría A se reserva a sistemas que, aunque son funcionalmente equivalentes a los de la categoría B, disponen de completas especificaciones formales de diseño y en los que se han aplicado técnicas de verificación. Cada una de las clases, excepto la D, especifica requerimientos en cuatro grandes áreas:

- Política de seguridad: conjunto de reglas que especifican si un sujeto puede acceder a un objeto.
- Gestión: funciones de identificación, autenticación y auditoria.
- Compatibilidad: criterios de evaluación del nivel de satisfacción de los restantes requerimientos (comprobaciones de seguridad, protección de los mecanismos de seguridad, etc.).
- Documentación: especificación de los documentos requeridos para cada una de las clases y el contenido básico de cada documento (por ejemplo: Guía de Usuario de Capacidades de Seguridad, Documentación de Comprobación, Documentación de Diseño de Seguridad).

Aunque el orange book describe cuatro clases, realmente los divide en dos categorías: sistemas que incorporan controles de acceso discrecionales (categoría C), con seguridad limitada a un único nivel de seguridad, y sistemas que incorporan controles de acceso obligatorios, que permiten procesar información de diferentes niveles de seguridad (categorías A y B).

Los controles de acceso discrecionales exigen un proceso de identificación y verificación del usuario a la entrada al sistema. Una vez verificado que se trata de un usuario autorizado, este podrá acceder a toda la información que no tenga definidas restricciones de acceso. Un ejemplo de este tipo de controles es el mecanismo de permisos de UNIX: cuando un usuario crea un objeto, puede o no definir un conjunto de permisos de manipulación para él, su grupo y los restantes usuarios.

Los controles de acceso obligatorios requieren múltiples niveles de seguridad. Los objetos y sujetos del sistema deben, obligatoriamente, tener un nivel de seguridad asociado. El sistema no debe permitir la creación de objetos o usuarios sin definir su nivel de seguridad, o que sean duplicados total o parcialmente con diferente nivel de seguridad. Cuando un usuario desea

acceder a un objeto, el sistema comprueba los niveles de ambos y evalúa si se permite o no el acceso.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información.

Las políticas de seguridad definen las expectativas en cuanto a seguridad se refiere, tomando las decisiones necesarias para completar el diseño previsto en el modelo de seguridad, estableciendo las reglas y procedimientos necesarios para garantizarla.

La tarea de las políticas de seguridad es responder a los qués: qué necesita protección, qué es más importante y qué aproximación general nos planteamos ante los problemas. Los cómos se especifican en los procedimientos de seguridad, recogidos en el manual de seguridad.

Una política que no sea implementable ni ejecutable es inútil.

Existen diferentes aspectos a contemplar en el desarrollo de la política, cómo son:

- Quién está autorizado a usar cada recurso.
- Cuál es el uso correcto de cada recurso.
- Quién es el responsable de conceder acceso al recurso.
- Quién puede tener privilegios de administrador de sistema.
- Cuáles son los derechos y responsabilidades de los usuarios.
- Cuáles son los derechos y responsabilidades del administrador frente a los de los usuarios.
- Qué debe hacerse con la información sensible (incluyendo la política y el manual de seguridad).

Resulta obvio que en el momento en que definimos una política, abrimos la posibilidad de que sea violada. Esto puede ocurrir por negligencia, error, falta de información o comprensión de la política, o deliberadamente. Cuando se detecta una violación de la política, el curso de acción debe estar predefinido para asegurar una reacción rápida y efectiva, incluyendo una investigación para determinar cómo, cuándo, quién y por qué. Y tomar las acciones necesarias, tanto disciplinarias como de corrección si se descubre un error en la política.

En gran medida, el éxito o fracaso de la seguridad depende del esfuerzo realizado en implementar los controles de seguridad que diseñamos para nuestra organización. Antes de poder implementar dichos controles, necesitamos comprender los requerimientos de seguridad específicos de nuestro sistema. Y este es el objetivo de un modelo de seguridad: especificar con precisión dichos requerimientos. El modelo que escojamos para expresar los requerimientos debe ser fácil de comprender, implementable, carente de ambigüedad y capaz de incorporar las políticas de la organización, [17].

5 SISTEMAS DE INFERENCIA DIFUSA.

La teoría difusa tiene sus inicios en la década de 1960 a partir de las publicaciones de Lofti A. Zadeh quien en sus publicaciones introduce una teoría cuyos objetos “conjuntos difusos” son conjuntos cuyas fronteras no son precisas, [22]. La pertenencia o membresía de un conjunto difuso no es exclusiva a la afirmación o negación, sino más bien a cuestiones de grado. Como principio se busca que los conjuntos difusos transformen las descripciones vagas en lenguaje natural a términos matemáticos precisos, esto por medio de funciones de membresía que definen y especifican conocimiento humano. Al arreglar los conjuntos difusos en enunciados Si-Entonces se conforman las llamadas reglas difusas que son la base de la lógica difusa. El objetivo de la lógica difusa es proveer fundamentos para la realización de razonamiento aproximado; es decir, se estudian métodos y principios para obtener nuevas proposiciones a partir de los enunciados existentes. Tales procedimientos se generalizan a través de un mecanismo de inferencia, que en conjunto con una base de conocimiento, conforma un sistema de inferencia difusa.

5.1 CONCEPTOS BASICOS DE LA LÓGICA DIFUSA.

En nuestra vida diaria, las palabras son comúnmente usadas para describir variables. En la teoría de sistemas de inferencia difusa, una variable de este tipo toma valores que son caracterizados por conjunto difusos definidos en el universo de discurso en el cual tal variable es definida. Los conjuntos difusos son una forma básica de agrupación del conocimiento cualitativo sobre un sistema, esto a través de funciones de membresía que mapean valores del dominio físico del universo de discurso a palabras. En esta sección se plantean estos conceptos básicos de sistemas de inferencia difusa para dar paso a la conformación de proposiciones difusas y a la descripción de operaciones de lógica en conjuntos difusos. De esta manera se describen las reglas difusas cuya relación entre proposiciones en las premisas y en el consecuente se da en términos de implicaciones. Por último se introduce el principio de inferencia deductivo Modus Ponens, el cual en su forma generalizada es la base del proceso de razonamiento aproximado en la teoría de lógica difusa.

5.1.1 VARIABLES LINGÜISTICAS Y CONJUNTOS DIFUSOS.

Una variable lingüística se considera como el elemento fundamental en la representación del conocimiento ya que toma palabras en el lenguaje natural como sus valores. En la teoría difusa

cada valor lingüístico o palabra que conforma una variable lingüística es un objeto “conjunto difuso” cuyas fronteras no son precisas y cuya definición está caracterizada por una función de membresía en un universo de discurso *U*. Un universo de discurso contiene todos los posibles elementos concernientes a un contexto en particular o aplicación; de esta forma, cada palabra de una variable lingüística está asociada a valores numéricos del universo de discurso de manera que existe una relación semántica entre el correspondiente valor lingüístico y su conjunto difuso en el dominio físico.

Una manera de representar la relación entre un valor lingüístico de una variable lingüística *X* y un conjunto difuso *A* en *U* es por medio de pares ordenados de los elementos genéricos *x* y su valor de membresía $\mu_A(x)$ *a, A:*

$$A = \{(\mu_A(x)) \mid x \in U\} \tag{1}$$

De manera general, un conjunto difuso A en un universo de discurso *U* continuo es descrito como:

$$A = \int_U \mu_A(x)/x \tag{2}$$

En el caso discreto, el conjunto difuso se representa como:

$$A = \sum_U \mu_A(x)/x \tag{3}$$

Cada conjunto difuso se encuentra definido de manera única por una función de membresía, cuando un conjunto es infinito, que normalmente se presenta cuando utilizamos los números reales es imposible enlistar a todos los elementos junto con su respectivo grado de membresía este tipo de conjunto difuso llamado número difuso es frecuentemente representado por una forma analítica la cual describe la forma del número difuso, entre las formas más utilizadas tenemos:

Forma triangular.

En la figura 5.1 encontramos una forma triangular caracterizada por los 3 parámetros a, b, y s, representada de forma genérica como:

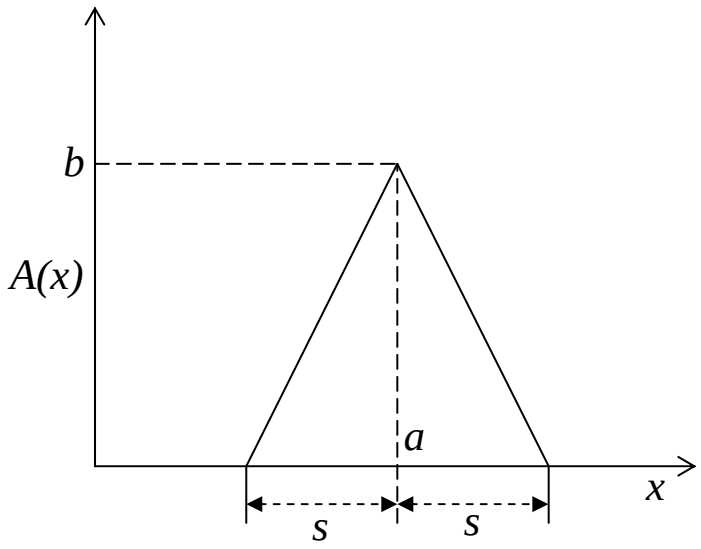

Fig. 5.1 Forma triangular.

definida por la función:

$$A(x) = \begin{cases} b\left(1\frac{|x-a|}{s}\right) & cuando \quad a - s \le x \le a + s \\ 0 & en \quad otro \quad caso \end{cases} \tag{4}$$

Forma trapezoidal:

En la Fig. 5.2 encontramos otra clase de función de membresía de forma trapezoidal caracterizada por los 5 parámetros a, b, c, d y e, representada de forma genérica como:

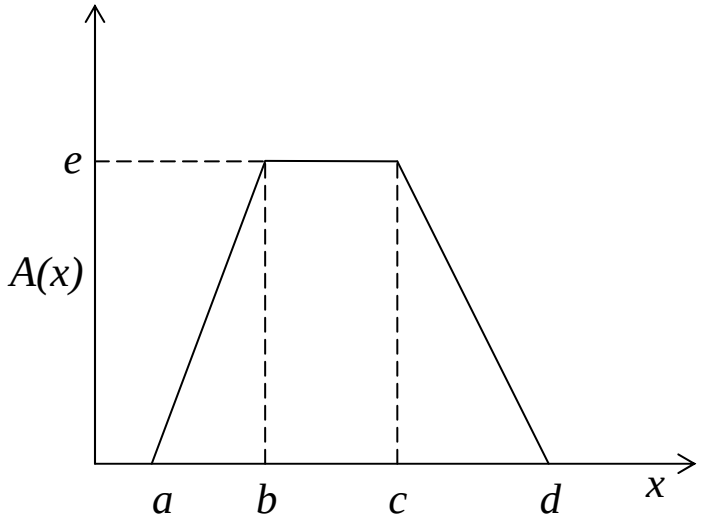

Fig. 5.2 Forma trapezoidal.

definida por la función:

$$A(x)\begin{cases} \dfrac{(a-x)e}{a-b} & cuando \quad a \le x \le b \\ e & cuando \quad b \le x \le c \\ \dfrac{(d-x)e}{d-c} & cuando \quad c \le x \le d \\ 0 & en \quad otro \quad caso \end{cases} \tag{5}$$

Forma campana.

En la Fig. 5.3 encontramos la forma más común utilizada para representar los conjuntos difusos, la campana, es caracterizada por 3 parámetros a, b y c, representada de forma genérica como:

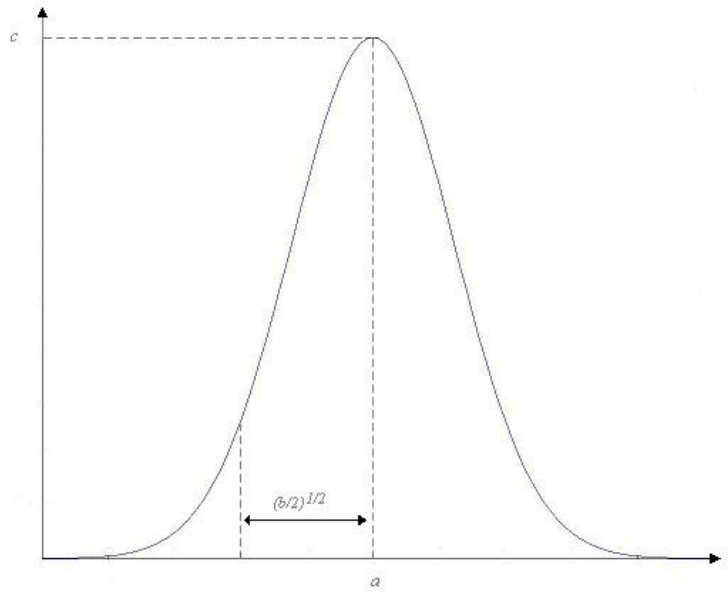

Fig. 5.3 Campana de gauss.

definida por la función:

$$A(x) = ce^{\frac{(x-a)^2}{b}} \tag{6}$$

5.1.2 PROPOSICIONES DIFUSAS COMPUESTAS Y OPERACIONES CON CONJUNTOS DIFUSOS.

La diferencia fundamental entre las proposiciones clásicas y las proposiciones difusas se encuentra en el rango de los valores de verdad, mientras que en una proposición clásica es requerido solamente un valor verdadero o falso, la verdad o falsedad en las proposiciones difusas dependen del grado. Asumimos que la verdad o falsedad son expresadas por los valores 1 o 0 respectivamente, el grado de verdad o falsedad en una proposición difusa es expresado por un número en el intervalo [1,0].

Por ejemplo en la proposición difusa: Viajar en la noche por carretera es más peligroso.

Para la lógica difusa no le interesa encontrar si es verdadero o falso, lo importante es encontrar el grado de verdad de la proposición.

La composición de dos o más proposiciones difusas atómicas para formar una proposición difusa compuesta se da a través de conectivos "Y", "O" y "NO", de manera que en lógica difusa tal intersección, unión y negación respectivamente tienen su propia definición.

La negación es una operación de complemento difuso c: [0,1] —> [0,1], el cual es un mapeo que transforma las funciones de membresía de un conjunto difuso *A* en la función de membresía del complemento de $A : c[\mu_A(x)] = \mu_A(x)$. La operación complemento más comúnmente utilizada para la negación es:

$$\mu_A(x) = 1 - \mu_A(x) \tag{7}$$

Considerando un conjunto universo *X* y 2 conjuntos difusos *A* y *B* definidos en *X*. la unión es una operación Norma S estándar denotada por $A \cup B$ esta definida por la fórmula de la función de membresía:

$$\mu_{A \cup B}(x) = \max[\mu_A(x), \mu_B(x)] \tag{8}$$

Considerando de nuevo los 2 conjuntos difusos *A* y *B* definidos en *X* la intersección es una Norma T denotada por $A \cap B$ esta definida por la fórmula de la función de membresía:

$$\mu_{A \cup B}(x) = \min[\mu_A(x), \mu_B(x)] \tag{9}$$

La proposición difusa compuesta es, en otras palabras, una relación difusa de dos o más conjuntos difusos (i.e. *A, B)* comprendidos en variables lingüísticas (i.e. *x, y).*

5.1.3 REGLAS DIFUSAS Y RAZONAMIENTO APROXIMADO.

Las reglas difusas son enunciados condicionales de la forma:

SI (*premisa difusa* FP_1), ENTONCES (*consecuencia difusa* FP_2) (10)

Donde las proposiciones difusas de las premisas están relacionadas con las proposiciones difusas de las consecuencias, a través de implicaciones como las siguientes:

La implicación Dienes-Rescher está conformada por los operadores lógicos de negación y unión definidos en la sección anterior, para así obtener una relación difusa Q_D en *Ux V* con la siguiente función de membresía

$$\mu_{Q_D}(x, y) = \max[1 - \mu_{FP1}(x), \mu_{FP2}(y)] \tag{11}$$

La implicación Zadeh es una relación difusa Qz en Ux V expresada por la función de membresía

$$\mu_{Q_Z}(x, y) = \max[\min(\mu_{FP1}(x), \mu_{FP2}(y)), 1 - \mu_{FP1}(x)] \tag{12}$$

Las implicaciones Mamdani son implicaciones locales en el sentido que pueden ser interpretadas como SI (FP1) ENTONCES (FP2) DE LO CONTRARIO (NADA). La relación difusa QMM ó QMP en Ux V del anterior enunciado estaría expresada por las funciones de membresía respectivas:

$$\mu_{Q_{MM}}(x, y) = \min[\mu_{FP1}(x), \mu_{FP2}(y)] \tag{13}$$

$$\mu_{Q_{MP}}(x, y) = \mu_{FP1}(x) * \mu_{FP2}(y) \tag{14}$$

Al representar una regla o enunciado condicional por medio de alguna de las anteriores implicaciones se obtiene una relación que a su vez es una premisa en un proceso de inferencia deductivo llamado Modus Ponens. En lógica clásica, la regla de inferencia Modus Ponens declara que para dos proposiciones p y q —> q, se infiere la verdad de la proposición q; esto se expresa como:

Premisa 1, proposición atómica p: x es A
Premisa 2, p → q: SI a; es 4 ENTONCES y es B (15)
Conclusión q: y es B

En lógica difusa se sigue un principio de inferencia análogo usando proposiciones imprecisas representadas por conjuntos difusos. Tal proceso de razonamiento aproximado se realiza con la regla Modus Ponens generalizada, la cual declara que para dos proposiciones difusas x es A' y SI x es A ENTONCES y es B, se infiere una nueva proposición difusa y es B' de manera tal que lo más cercano esté A' de A, lo más cercano estará B' de B; es decir:

Premisa 1, í es A'
Premisa 2: SI x es A ENTONCES y es B (16)
Conclusión: y es B'

La conclusión del proceso de razonamiento aproximado es el resultado de la composición del conjunto difuso de la Premisa 1 con la implicación de la Premisa 2 la cual se expresa como una relación difusa en el producto cartesiano de los dominios de x y y. La composición es el resultado de integrar dos relaciones binarias (i.e. P(U,V) y Q,{V,W)), o un conjunto difuso con una relación binaria difusa.

5.2 SISTEMAS DE INFERENCIA DIFUSA.

En los conceptos de lógica difusa se explicó el proceso de razonamiento Modus Ponens usando un sólo enunciado condicional difuso y alguna proposición correspondiente al antecedente de la implicación, lo que nos daba como resultado el consecuente de la regla. Al describir un sistema dinámico a través de múltiples reglas difusas se debe considerar cada una de ellas en el proceso de razonamiento para obtener el próximo estado del sistema; este proceso es desarrollado por un

mecanismo de inferencia difusa, la cual en conjunto con una base de reglas conforma un sistema de inferencia difusa.

5.2.1 BASE DE REGLAS DIFUSAS.

La base de reglas está compuesta por enunciados condicionales difusos que en su forma básica se expresan como:

$$R_u^{(t)} : SI\, x_1 es A_1^t Y \ldots Y x_n es A_n^t ENTONCES\, y es B^t$$

Donde A_i^t y B^t son conjuntos difusos en $U_i \subset RyV \subset R$ respectivamente y $x = [x_1, \ldots, x_n]^T \in U$ y $y \in V$ son variables lingüísticas de entrada y salida. De otra manera podemos decir que cada premisa está formada de i = 1,2, ...,n variables lingüísticas, las cuales a su vez tienen de j = 1,2, ...,m valores diferentes que son representados de manera difusa por medio de funciones de membresía.

La cantidad de funciones de membresía para cada variable puede ser diferente dependiendo del dominio cuantitativo que represente la variable. En la definición de la estructura de las funciones de membresía que cubren el dominio de una variable lingüística habrá que considerar la condición de anchura, representada en la Fig. 5.4 la cual establece que la anchura izquierda de μ_{A_2} debería ser igual a la anchura derecha de μ_{A_1} y ambas son iguales a la longitud del intervalo entre el centro de dos funciones de membresía adyacentes.

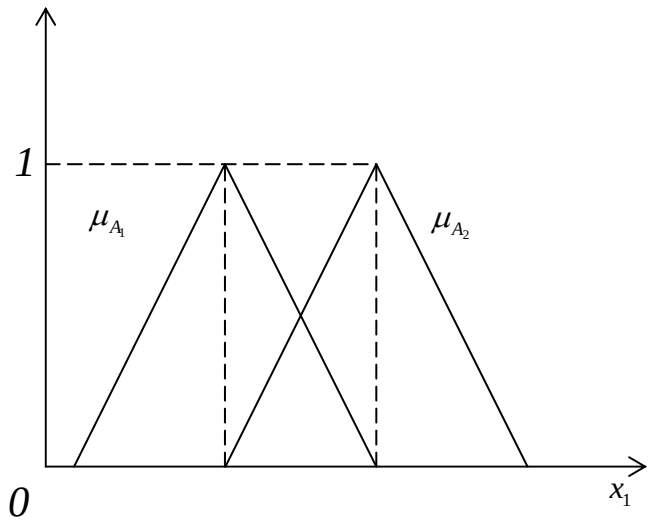

Fig. 5.4 Funciones de anchura.

En la Fig. 5.5 podemos observar un par de funciones de membresía que no cumplen con la condición de anchura, existe una región de valores en el dominio de la variable x_1 para el cual sólo se activaría una regla, esto evita transiciones suaves a la salida dado que no se pondera la pertenencia de un valor en la frontera de los dos conjuntos difusos.

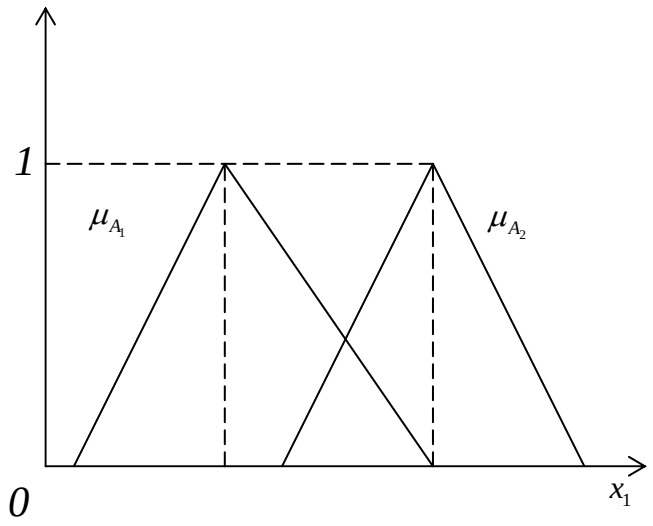

Fig. 5.5 Funciones de membresía que no cumplen anchura.

Las reglas difusas SI… ENTONCES que se pueden formar dependen del número de variables lingüísticas y los valores de las mismas por ejemplo:

Supongamos 2 variables x_1 y x_2 en la primera tenemos 3 funciones de membresía $\mu_{A_1^1}$, $\mu_{A_2^1}$ y $\mu_{A_3^1}$ y en la segunda tenemos sólo 2 $\mu_{A_1^2}$ y $\mu_{A_2^2}$ al determinar el grupo completo de enunciados difusos Si … Entonces tendríamos:

1.-SI x_1 es $\mu_{A_1^1}$ Y x_2 es $\mu_{A_1^2}$ ENTONCES y es B^1

2.-SI x_1 es $\mu_{A_1^1}$ Y x_2 es $\mu_{A_2^2}$ ENTONCES y es B^2

3.-SI x_1 es $\mu_{A_2^1}$ Y x_2 es $\mu_{A_1^2}$ ENTONCES y es B^3

4.-SI x_1 es $\mu_{A_2^1}$ Y x_2 es $\mu_{A_2^2}$ ENTONCES y es B^4

5.-SI x_1 es $\mu_{A_3^1}$ Y x_2 es $\mu_{A_1^2}$ ENTONCES y es B^5

6.-SI x_1 es $\mu_{A_3^1}$ Y x_2 es $\mu_{A_2^2}$ ENTONCES y es B^6

En la Fig. 5.6 podemos observar de manera gráfica la representación de estos enunciados.

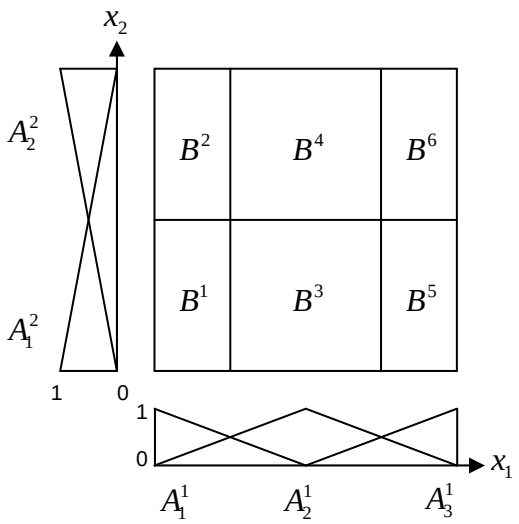

Fig. 5.6 Representación del grupo completo de enunciados.

Cuando se forman reglas con todas las posibles combinaciones de funciones de membresía de cada variable, se dice que se tiene una base de reglas completa. Una desventaja de este tipo de base de reglas es que su tamaño aumenta exponencialmente con la dimensión de espacio de entradas U_i . En general, en la mayoría de los procesos a modelar, las entradas no toman valores arbitrarios por lo que para tener completa la base no sería necesario combinar todas las funciones de membresía para cada variable, sino más bien se busca tener una base de reglas en la que para vectores factibles de entrada *x* e *U* exista al menos una regla $R_u^{(t)}$ tal que $\mu_{A_i^t}(x_i) \neq 0$ para toda *i* = 1,2, ...n.

Se define a un grupo de reglas como consistente si no existe alguna regla que tenga el mismo antecedente pero diferente consecuente. Así también, se dice que un grupo de enunciados SI … ENTONCES difusos es continuo si los conjuntos difusos del consecuente de reglas adyacentes dan como resultado salidas con transiciones suaves.

5.2.2 MECANISMO DE INFERENCIA DIFUSA.

En los sistemas de inferencia difusa se manejan dos perspectivas generales de la manera en que el proceso de razonamiento aproximado debería utilizar el grupo de reglas para inferir nuevos estados. Por una parte, en un mecanismo de inferencia basada en composición, cada relación difusa $R_u^{(t)}$ representando un enunciado condicional en el espacio de entrada salida en *UxV* es combinada para formar una sola relación difusa Q_M en *UxV* que es interpretada como una sola regla difusa; de esta manera, al tener un conjunto difuso *A'* como premisa de entrada al mecanismo de inferencia, se aplicaría el principio de razonamiento Modus-Ponens generalizado para a partir de la relación difusa Q_M obtener un conjunto difuso resultante $\mu_{B'}(y)$. Por otra parte, en un mecanismo de inferencia basada en reglas individuales, el principio de razonamiento Modus-Ponens generalizado se aplica a cada regla por separado, por lo que al tener un nuevo conjunto difuso de entrada *A'* en *U*, el proceso de inferencia generaría un conjunto difuso $\mu_{B'}(y)$ por cada regla, los cuales tendrían que ser combinados por alguna norma-t ó norma-s.

El mecanismo de inferencia basada en composición realiza el proceso de inferencia de manera interpretable, por lo que tiene sentido considerar la combinación de las reglas como la unión de las relaciones difusas que representan cada regla. De esta manera, *M* número de reglas de la se interpretarían como una sola relación Q_M en *UxV*.

En los sistemas de inferencia difusos, la implicación representa una relación causal entre los conjuntos difusos de entrada y de salida, donde las ideas de la representación local del conocimiento son muy importantes. En general, un FIS está compuesto de un conjunto de reglas de producción, correspondientes a una partición del espacio de variables (multidimensional) que puede realizarse según dos grandes esquemas:

- Partición compartida; que define un cierto número de conjuntos difusos por cada una de las dimensiones. Estos conjuntos introducen, en consecuencia, valores lingüísticos comunes al conjunto de reglas. Este tipo de particiones es muy utilizado en la construcción de modelos difusos, en la que el nivel de interpretabilidad es muy importante, [21],
- Partición por grupos (clustering); que conduce a una partición del espacio en grupos homogéneos siguiendo un criterio. Esta partición conduce a una regla por grupo. De esta forma, los conjuntos difusos son propios a una regla y no son compartidos por el conjunto de reglas. Este tipo de particiones ha demostrado ser más adecuado en la construcción de controladores difusos, así como en la identificación de sistemas, [20].

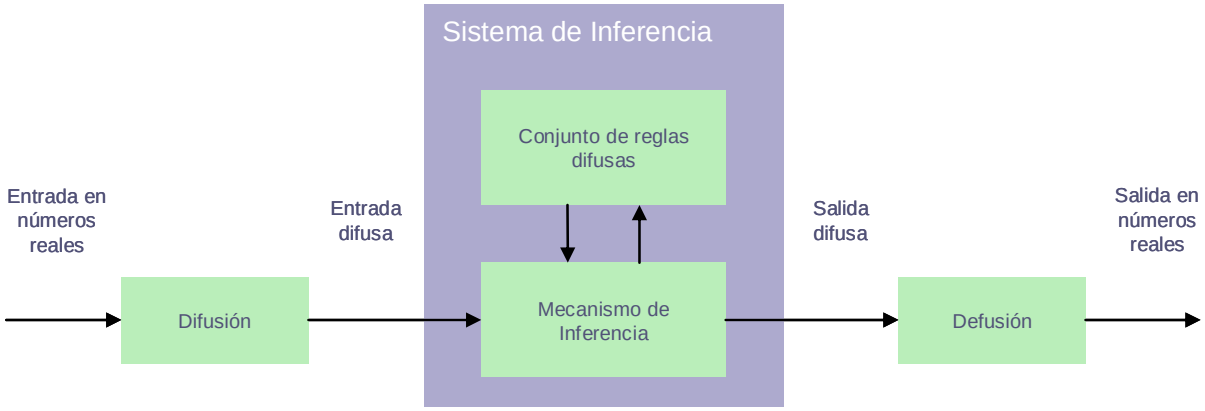

Fig. 5.7 Componentes básicos de un sistema de inferencia difuso.

5.2.3 TIPOS DE SISTEMAS DE INFERENCIA DIFUSA.

Según la estructura de la parte consecuente de la regla, podemos distinguir tres tipos principales de modelado difuso:

- Modelado difuso lingüístico, en el que la premisa y la consecuencia son proposiciones difusas.
- Modelado relacional difuso, que es, de alguna manera, una generalización del modelo difuso lingüístico, permitiendo la asociación de una premisa a diferentes proposiciones consecuentes, por una relación difusa.

- Modelado difuso de Takagi-Sugeno (TS), donde la parte consecuente es una función matemática de variables antecedentes más que una proposición difusa.

En nuestra investigación adoptamos esencialmente el modelado relacional difuso.

5.2.4 MODELADO RELACIONAL DIFUSO

El objetivo de este tipo de modelo es de hacer que la base de reglas (1) esté representado como una relación difusa $R=[r_{i,j}]$ entre el conjunto de términos antecedentes $\mathcal{A}_j$ y el conjunto de términos consecuentes $\mathcal{B}$. De esta forma, R está representado por una matriz de dimensión $k_R \times k_y$, restringida a tener un elemento diferente de cero en cada línea. Cada regla contiene todos los términos consecuentes posibles, cada una con sus propios factores de peso, correspondiente al elemento $r_{i,j}$ de la relación difusa. Estos pesos permiten al modelo ser fácilmente ajustado para adaptarse, si se disponen de datos. La figura muestra un ejemplo en $\Re^2$, con k_1=3 para la variable x_1 y k_2=3 para la variable x_2. Este tipo de FIS es el más utilizado en el ámbito del modelado difuso.

Premisa		***Consecuencia***		
si		**Entonces**		
			Y	
x_1	Y x_2	B_1	B_2	B_3
A_1^1	A_1^2	$r_{1,1}$	$r_{1,2}$	$r_{1,3}$
A_1^1	A_2^2	$r_{2,1}$	$r_{2,2}$	$r_{2,3}$
A_1^1	A_3^2	$r_{3,1}$	$r_{3,2}$	$r_{3,3}$
A_2^1	A_1^2	$r_{4,1}$	$r_{4,2}$	$r_{4,3}$
A_2^1	A_2^2	$r_{5,1}$	$r_{5,2}$	$r_{5,3}$
A_2^1	A_3^2	$r_{6,1}$	$r_{6,2}$	$r_{6,3}$
A_3^1	A_1^2	$r_{7,1}$	$r_{7,2}$	$r_{7,3}$
A_3^1	A_2^2	$r_{8,1}$	$r_{8,2}$	$r_{8,3}$
A_3^1	A_3^2	$r_{9,1}$	$r_{9,2}$	$r_{9,3}$

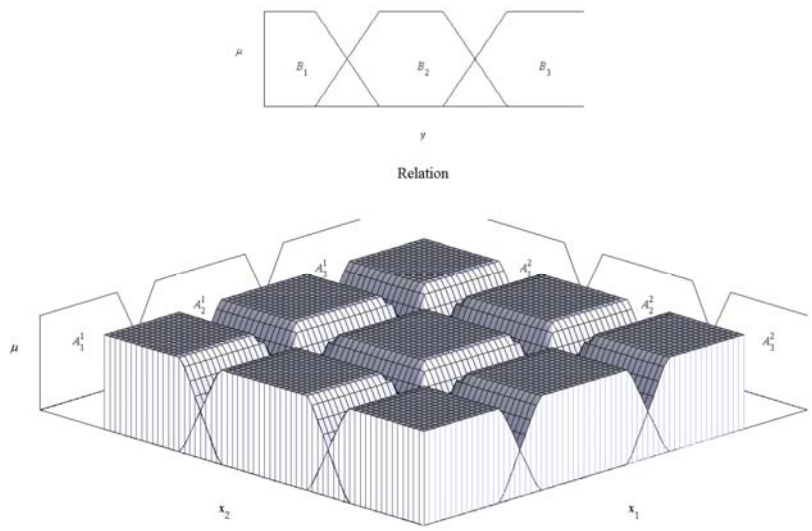

Fig. 5.8 Modelo relacional difuso en $\Re^2$, con k_1=3 para la variable x_1 y k_2=3 para la variable x_2.

6 MODELO PROPUESTO.

Cómo solución al problema de autenticación en redes ad hoc, se presenta el modelo de niveles de confianza basado en sistemas de inferencia difusa. Esta herramienta determina el nivel de confianza a partir de las variables difusas tráfico promedio, última transmisión y comportamiento.

En el análisis del modelo de niveles de confianza nos encontramos con el problema de una variable ambigua no bien definida, buscando una solución formal entramos al campo de la lógica difusa y decidimos implementar un modelo Mamdani con una matriz de inferencia generada a partir de nuestro expertisse.

Para la implementación del modelo, se genero un programa en java que calcula el nivel de confianza a partir de las variables definidas, utilizamos este lenguaje de programación debido a su portabilidad (multiplataforma).

6.1 COMPONENTES DEL MODELO.

Nuestro modelo de solución para la autenticación de redes ad hoc se encuentra basado en el comportamiento humano y la lógica difusa, tomando en cuenta que los hombres vivimos en sociedad y mantenemos vínculos con los diversos grupos de personas que nos rodean. Tendemos a generar un grado de confianza especial para cada una de las personas, por ejemplo una persona que esta casada, tiene familia y trabaja mantiene diferentes grados de confianza para cada una de las personas que la rodea en su entorno, es decir podría confiar más en su pareja después en su familia y por último en la gente con la que trabaja o al revés pero no los trata de la misma forma, al conocer a una nueva persona puede darle un nivel de confianza dependiendo de quien se la presente o de la circunstancia por la cual la integre a su entorno.

En nuestra vida diaria las palabras son comúnmente utilizadas para describir variables de forma vaga. En la teoría de sistemas de inferencia difusa, una variable de este tipo toma valores que son caracterizados por conjuntos difusos definidos en el universo de discurso en el cual tal variable es definida.

Los conjuntos difusos son una forma básica de agrupación del conocimiento cualitativo sobre un sistema, esto a través de funciones de membresía que mapean valores del dominio físico del universo de discurso a palabras. Por ejemplo al hablar de un número grande podríamos interpretar esta prioridad de dos maneras: un número será grande si es igual o mayor a cierto valor, y será no

grande si es menor o bien existen números grandes, números no grandes, y otros que no tienen una clasificación determinada porque no son ni grandes ni son no grandes. Esta última interpretación nos indica la existencia de la vaguedad en la manera de representar las cosas.

Tomando en cuenta que en principio se busca que los conjuntos difusos transformen las descripciones vagas de lenguaje natural a términos matemáticos precisos, esto por funciones de transferencia que definen y especifican conocimiento.

Para nuestro modelo vamos a ocupar un sistema de inferencia difusa con difusión y defusión como se muestra en el siguiente diagrama Fig. 6.1:

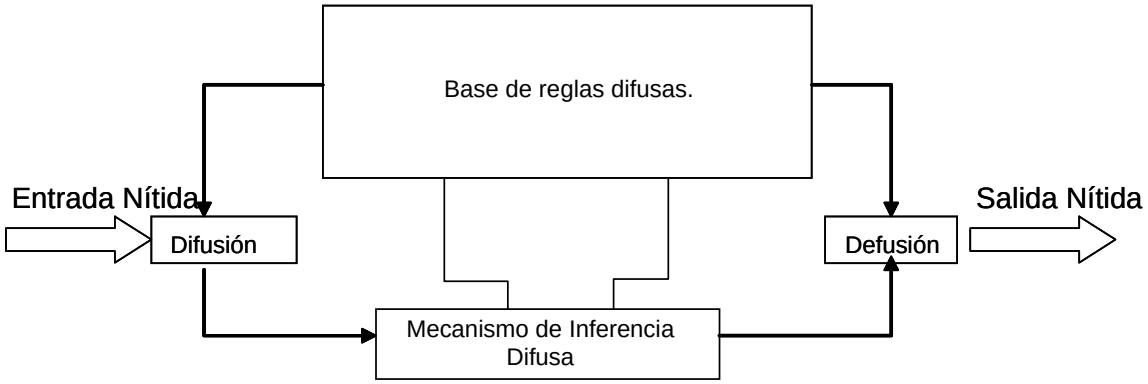

Fig. 6.1 Modelo de inferencia Difusa.

Los seres humanos autenticamos a la gente por su voz, su físico, por su olor u otras características o intuitivas que en base a la relación que vamos generando a través del tiempo tendemos a aumentar nuestro nivel de confianza o lo disminuimos hasta llegar al extremo de ignorarlo y no hablarle de acuerdo a los hechos que se susciten en la relación.

Es importante destacar que nuestro modelo esta basado en la autenticación de nodos tomando en cuenta reglas de comportamiento humano por lo que no podemos garantizar que cada uno de los nodos deba de comportarse de forma debida durante el tiempo que forman parte de la red. Podemos tener el caso que una serie de nodos después de un determinado tiempo y al escalar en los niveles de confianza puedan atacar al resto de la red o que sus niveles de confianza varíen con respecto a los demás.

En las redes ad hoc los nodos entran y salen de la red, al entrar reconocen a los demás nodos y con nuestro modelo para la autenticación en redes ad hoc basado en el cálculo del nivel de confianza generado en el sistema de inferencia difusa con difusión y defusión generan un nivel de confianza entre ellos. Aunque las computadoras son herramientas de trabajo y no poseen el concepto de nivel de confianza podemos basarnos en los sistemas de inferencia difusa para obtenerlo.

La mayoría de las investigaciones que se tienen en redes ad hoc se basan en solucionar los protocolos de ruteo asumiendo que todos lo nodos tiene una dirección única este problema sigue abierto, es necesario un protocolo para la asignación dinámica de direcciones únicas que sea verdaderamente espontáneo y sin infraestructura de red.

Las redes ad hoc son muy dinámicas y para nuestro caso vamos a tomar en cuenta que los nodos pueden identificarse unos de otros sin entrar a más detalle, por lo que al referirnos al nodo X asumimos que cualquier otro nodo en la red lo puede identificar como nodo X.

A diferencia de las máquinas nosotros manejamos inconscientemente nuestros conceptos vagos para determinar el nivel de confianza y lo hacemos con n variables y apoyandonos en frases como: “Yo medio confío en X persona”, “Confío con los ojos cerrados en Y”, “La verdad es que Z no es una persona de fiar” entre otras descripciones que podemos utilizar para catalogar la confianza con respecto a una persona. Sin embargo para nuestro modelo difuso vamos a definir 3 variables que nos van a servir como referencia para calcular el nivel de confianza en nuestro sistema:

6.1.1 AMBIENTE DE PRUEBAS.

Para nuestro ambiente de pruebas generamos una red ad hoc con tres equipos que contienen las siguientes características:

Tabla 6.1 Características del ambiente de pruebas.

Característica	*Equipo 1 (Nodo 1)*	*Equipo 2 (Nodo 2)*	*Equipo 3 (Nodo 3)*
Sistema Operativo.	Windows XP Professional Service Pack 2.	Windows Vista.	Windows XP Professional Service Pack 2.
Marca y Modelo.	HP Pavilion	Sony VAIO	Dell INSPIRON
Procesador	Celeron a 2.4 GHZ.	Core Duo 1.8 Ghz	Core Duo a 1.6 GHZ
Memoria	512 MB	2 GB	1 GB
Disco duro.	40 GB	120 GB	80 GB

6.1.2 VARIABLES DE ENTRADA.

Para nuestro modelo estamos definiendo tres variables nítidas de entrada, cada una de ellas se tomo en cuenta por su representatividad hacia el modelo que proponemos, sin embargo se pueden agregar, eliminar o cambiar variables según la justificación que se tenga para ello, lógicamente al afectar las variables se tendría que redefinir la matriz de inferencia.

6.1.2.1 Tráfico promedio.

El objetivo primordial de una red es el de poder compartir información entre los distintos nodos que la conforman, por ello al compartir esta información generamos un tráfico de paquetes tanto de información como de control, nos vamos a apoyar en esta variable para determinar el

intercambio de información que se genera entre los nodos incluyendo el que se esta ruteando de los demás nodos.

Nuestro procedimiento para determinar el valor del tráfico promedio se basa en la obtención del tráfico que tienen los nodos por sesión con un máximo de 30 muestras, con ellas obtenemos su promedio, este valor resultante es nuestra variable de entrada tráfico promedio que vamos a meter en nuestro modelo. El siguiente ejemplo vamos a generar un cálculo de tráfico promedio.

Tabla 6.2 Cálculo de tráfico promedio.

Nodo	Fecha	Mega Bits
Nodo B	10/09/2007	120.38
Nodo B	11/09/2007	60.57
Nodo B	12/09/2007	202.50
Nodo B	13/09/2007	146.43
Nodo B	14/09/2007	95.23
Nodo B	15/09/2007	40.10
Nodo B	16/09/2007	15.62
Nodo B	17/09/2007	10.52
Nodo B	18/09/2007	140.93
Nodo B	19/09/2007	63.75
Nodo B	20/09/2007	35.28
Promedio		84.66

En esta tabla el nodo A lleva el registro del tráfico con respecto al nodo B, el cálculo promedio obtenido es nuestra primera variable de entrada que tiene un universo de discurso de todos los números reales positivos, los conjuntos difusos que ocupamos los definimos de la siguiente manera:

Tenemos cuatro conjuntos difusos para esta variable con las siguientes funciones de membresía:

$$\text{Tráfico Nulo (TNU)} = \begin{cases} e^{-\frac{(X)^2}{426}} & \text{Cuando } x \leq 106.66 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Tráfico Bajo (TB)} = \begin{cases} e^{-\frac{(X-106.66)^2}{426}} & \text{Cuando } 0 \leq x \leq 213.32 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Tráfico Normal (TNO)} = \begin{cases} e^{-\frac{(X-213.32)^2}{426}} & \text{Cuando } 106.66 \le x \le 320 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Tráfico Alto (TA)} = \begin{cases} e^{-\frac{(X-320)^2}{426}} & \text{Cuando } 213.32 \le x \le 320 \\ 1 & \text{Cuando } X > 320 \\ 0 & \text{En otro Caso} \end{cases}$$

A partir de las funciones de membresía se obtiene la siguiente gráfica Fig. 6.2 variable tráfico promedio.

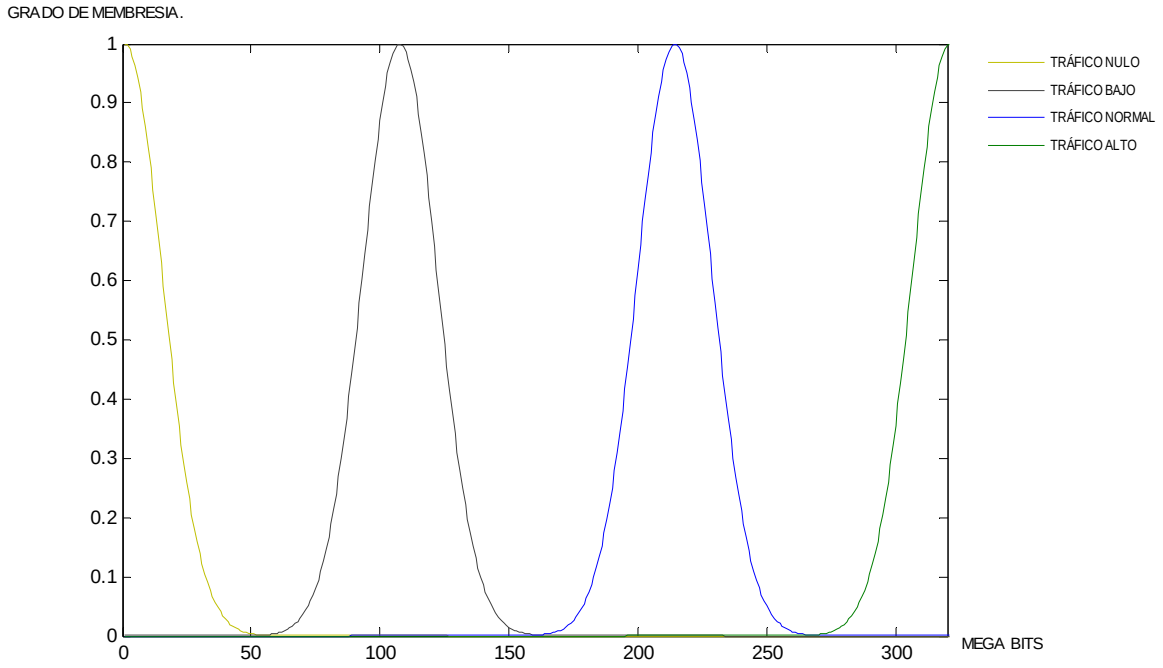

Fig. 6.2 Gráfica de la variable Tráfico Promedio (Original en colores).

En caso de que el nodo A no tuviera el registro de tráfico con respecto al nodo B entonces el tráfico promedio que se toma es 0.

6.1.2.2 Última transmisión.

Para el caso de la variable de última transmisión vamos a tomar la última fecha en la cual tuvimos intercambio de información con el nodo en cuestión por ejemplo si el día de hoy estamos a 22/09/07 y la fecha de última transmisión es el 20/09/07 entonces se contabilizan dos días desde

la fecha de última transmisión, esta variable nos va a servir para determinar que tanto tiempo tiene que dejamos de recibir información de un nodo dentro de la red.

Para esta variable el universo de discurso son todos los números enteros positivos incluyendo el 0 y vamos a generar los siguientes 3 conjuntos difusos definidos con las funciones de membresía:

$$\text{Última Transmisión Reciente (UTR)} = \begin{cases} e^{-\frac{(X)^2}{56}} & \text{Cuando } x \leq 28 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Última Transmisión Poco (UTP)} = \begin{cases} e^{-\frac{(X-28)^2}{56}} & \text{Cuando } 0 \leq x \leq 56 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Última Transmisión Ya tiene Tiempo (UTY)} = \begin{cases} e^{-\frac{(X-56)^2}{56}} & \text{Cuando } 28 \leq x \leq 56 \\ 1 & \text{Cuando } x > 56 \\ 0 & \text{En otro Caso} \end{cases}$$

A partir de las funciones de membresía se obtiene la siguiente gráfica Fig. 6.3 variable última transmisión.

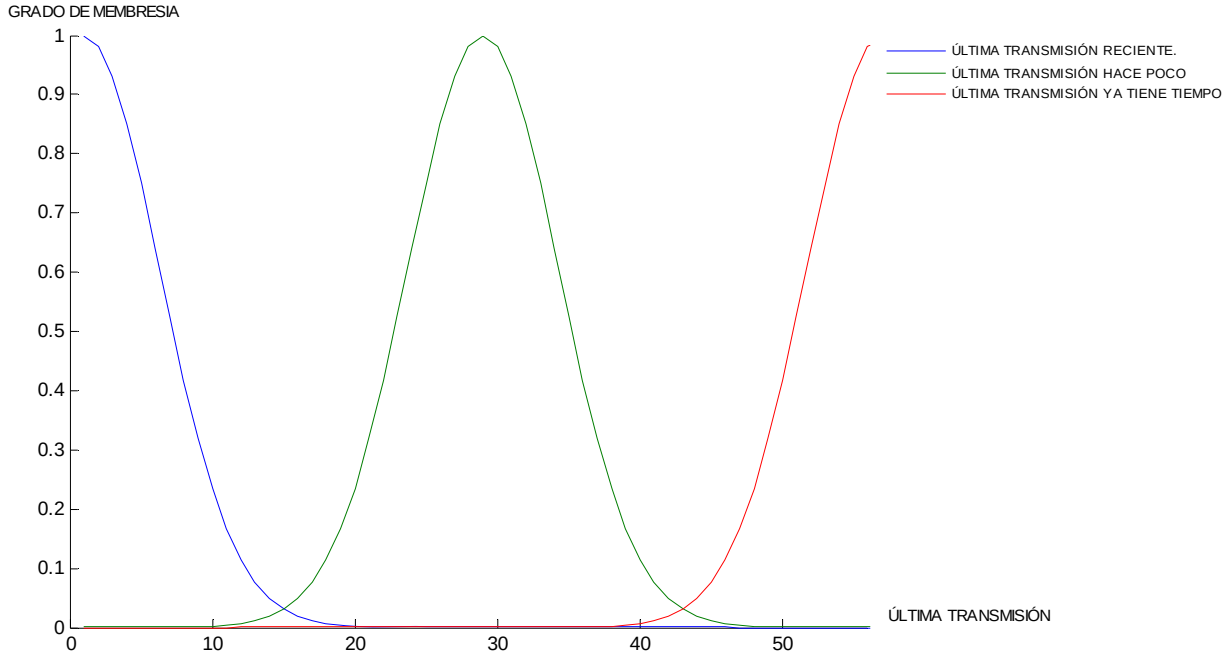

Fig. 6.3 Gráfica de la variable última transmisión (Original en colores).

6.1.2.3 Comportamiento.

El concepto de comportamiento puede tener varias connotaciones sin embargo para nuestro modelo lo vamos a utilizar para retroalimentarlo en base a la evaluación obtenida del nivel de confianza. La evaluación se obtiene inicialmente al inyectar al modelo los primeros datos y nos sirve para dar seguimiento a la variación que tiene el nivel de confianza, más adelante vamos a revisar el uso que se le da a esta variable dentro del modelo con un enfoque dinámico temporal.

Cuando un nodo acaba de conocer a otro y no tiene datos precedentes entonces el comportamiento inicial se coloca en tres.

Para esta variable el universo de discurso son los números enteros positivos desde el 1 hasta el 7, incluyendo el 0 y vamos a generar los siguientes cinco conjuntos difusos definidos con las funciones de membresía:

$$\text{Comportamiento Inaceptable (CI)} = \begin{cases} e^{-\frac{(X)^2}{3.5}} & \text{Cuando } x \leq 1.75 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Comportamiento Regular (CR)} = \begin{cases} e^{-\frac{(X-1.75)^2}{3.5}} & \text{Cuando } 0 \leq x \leq 3.5 \\ & \end{cases}$$

$$0 \qquad \text{En otro Caso}$$

$$\text{Comportamiento Bueno (CB)} = \begin{cases} e^{-\frac{(X-3.5)^2}{3.5}} & \text{Cuando } 1.75 \le x \le 5.25 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Comportamiento Muy Bueno (CMB)} = \begin{cases} e^{-\frac{(X-5.25)^2}{3.5}} & \text{Cuando } 3.5 \le x \le 7 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Comportamiento Excelente (CE)} = \begin{cases} e^{-\frac{(X-7)^2}{3.5}} & \text{Cuando } 5.25 \le x \le 7 \\ 0 & \text{En otro Caso} \end{cases}$$

A partir de las funciones de membresía se obtiene la siguiente gráfica Fig. 6.4 variable comportamiento.

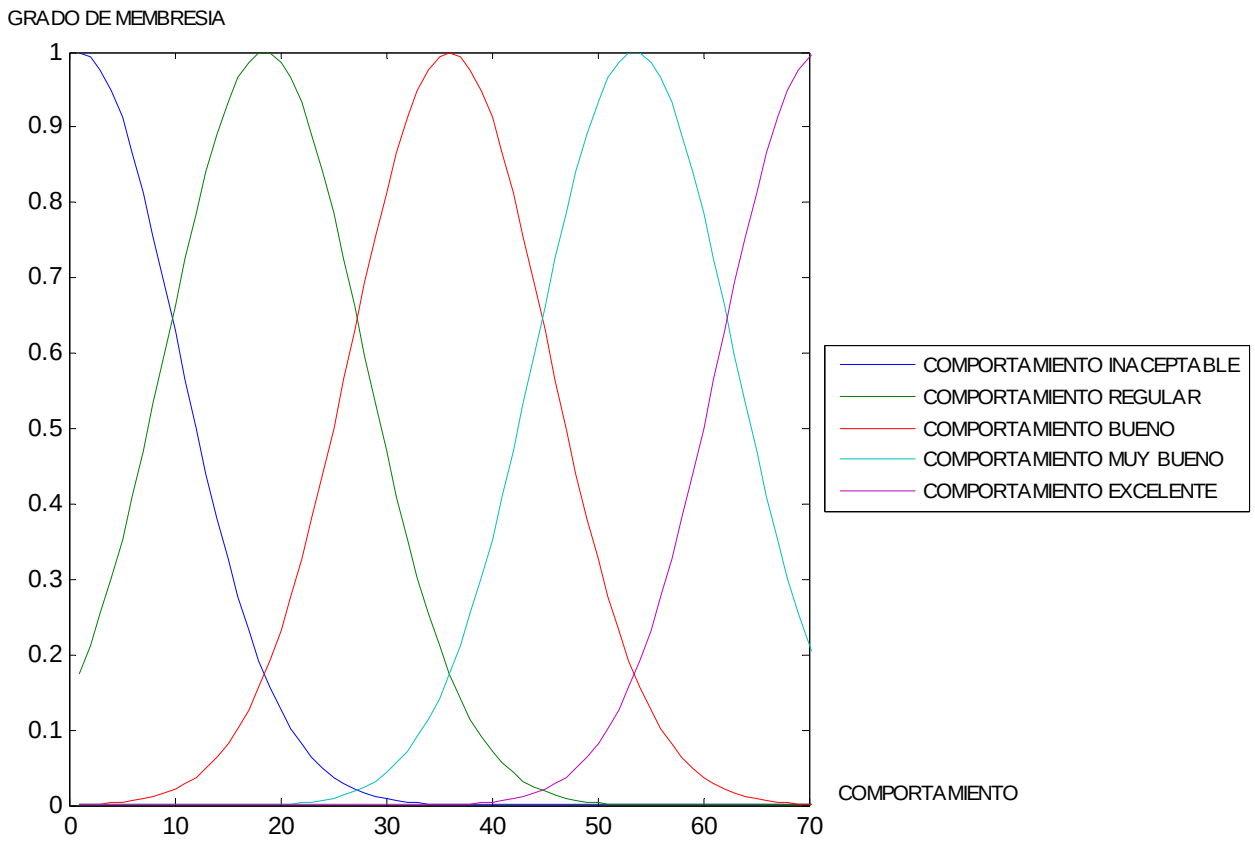

Fig. 6.4 Gráfica variable comportamiento (Original en colores).

Para poder observar de mejor manera la gráfica tiene una escala de 10 a 1.

6.1.3 DIFUSIÓN.

La difusión transforma un valor numérico nítido de entrada a un conjunto difuso que es combinado con alguna(s) regla(s) difusa(s) para obtener por medio de un mecanismo de inferencia, un conjunto(s) de salida difuso(s).

6.1.4 BASE DE CONOCIMIENTO.

La base de reglas difusas esta compuesto por enunciados condicionales difusos que en su forma básica se expresan como:

Si x_1 es A1 Y x2 es A2… **entonces** y es B

En otras palabras:

Si (premisas) **entonces** consecuente.

En donde nuestras reglas van a ser consistentes y continuas.

Un grupo de reglas es consistente si no existe alguna regla que tenga el mismo antecedente pero diferente consecuente, y se dice que un grupo de reglas es continuo si los conjuntos difusos del consecuente de reglas adyacentes dan como resultado salidas con transiciones suaves.

Derivado de las variables de entrada y salida que tenemos generamos nuestra base de conocimiento que consta de 60 reglas.

Tabla 6.3 Base de Conocimiento.

Última transmisión

UTY

Comportamiento \ Tráfico	TNU	TB	TNO	TA
CI	NCN	NCN	NCN	NCN
CR	NCN	NCN	NCS	NCS
CB	NCS	NCS	NCS	NCC
CMB	NCS	NCS	NCC	NCC
CE	NCS	NCC	NCC	NCC

UTP

Comportamiento \ Tráfico	TNU	TB	TNO	TA
CI	NCN	NCN	NCN	NCN
CR	NCS	NCS	NCS	NCS
CB	NCS	NCS	NCC	NCC
CMB	NCS	NCC	NCT	NCT
CE	NCC	NCT	NCT	NCT

UTR

Comportamiento \ Tráfico	TNU	TB	TNO	TA
CI	NCN	NCS	NCS	NCS
CR	NCS	NCS	NCC	NCC
CB	NCS	NCS	NCT	NCT
CMB	NCC	NCC	NCT	NCT
CE	NCC	NCT	NCT	NCT

6.1.5 MECANISMO DE INFERENCIA DIFUSA.

Se pueden tener dos tipos de mecanismo de inferencia, por composición y reglas individuales. El basado en composición combina cada enunciado condicional para obtener una sola relación

difusa mientras que el basado en reglas individuales se aplica a cada regla por separado por lo que en la salida se genera un conjunto difuso.

6.1.6 DEFUSIÓN.

La defusión es el proceso de convertir la salida del mecanismo de inferencia difusa (conjunto difuso) a un valor nítido que represente la distribución de valores, existen varios tipos de defusión entre ellos están: altura, centro de gravedad y media de los máximos. En nuestro programa se pueden configurar estos tipos de defusión sin embargo utilizamos la media de los máximos para generar los resultados.

6.1.7 NIVEL DE CONFIANZA.

Esta variable de salida representa el concepto fundamental de la tesis, el nivel de confianza generado define el nivel de servicio que tenemos respecto a los demás nodos de la red ad hoc, con esta evaluación podemos definir si un nodo es malicioso, tiene un comportamiento normal o podemos confiar plenamente en él. Aunque una computadora por si misma no puede definir el nivel de confianza que tiene con los otros nodos de la red si podemos inducir este concepto abstracto vía nuestro modelo.

Al igual que las variables de entrada se definieron conjuntos difusos para representarla, el universo de discurso son los números enteros positivos desde el 1 hasta el 7, incluyendo el 0 y vamos a generar los siguientes cuatro conjuntos difusos definidos con las funciones de membresía:

$$\text{Nivel de Confianza No Confiable (NCN)} = \begin{cases} e^{-\frac{(X)^2}{2.5}} & \text{Cuando } x \leq 2.5 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Nivel de Confianza Semiconfiable (NCS)} = \begin{cases} e^{-\frac{(X-2.5)^2}{2.5}} & \text{Cuando } 0 \leq x \leq 5 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Nivel de Confianza Confiable (NCC)} = \begin{cases} e^{-\frac{(X-5)^2}{2.5}} & \text{Cuando } 2.5 \leq x \leq 7 \\ 0 & \text{En otro Caso} \end{cases}$$

$$\text{Nivel de Confianza Total (NCT)} = \begin{cases} e^{-\frac{(X-7)^2}{2.5}} & \text{Cuando } 5 \le x \le 7 \\ 0 & \text{En otro Caso} \end{cases}$$

A partir de las funciones de membresía se obtiene la siguiente gráfica Fig. 6.5 variable nivel de confianza.

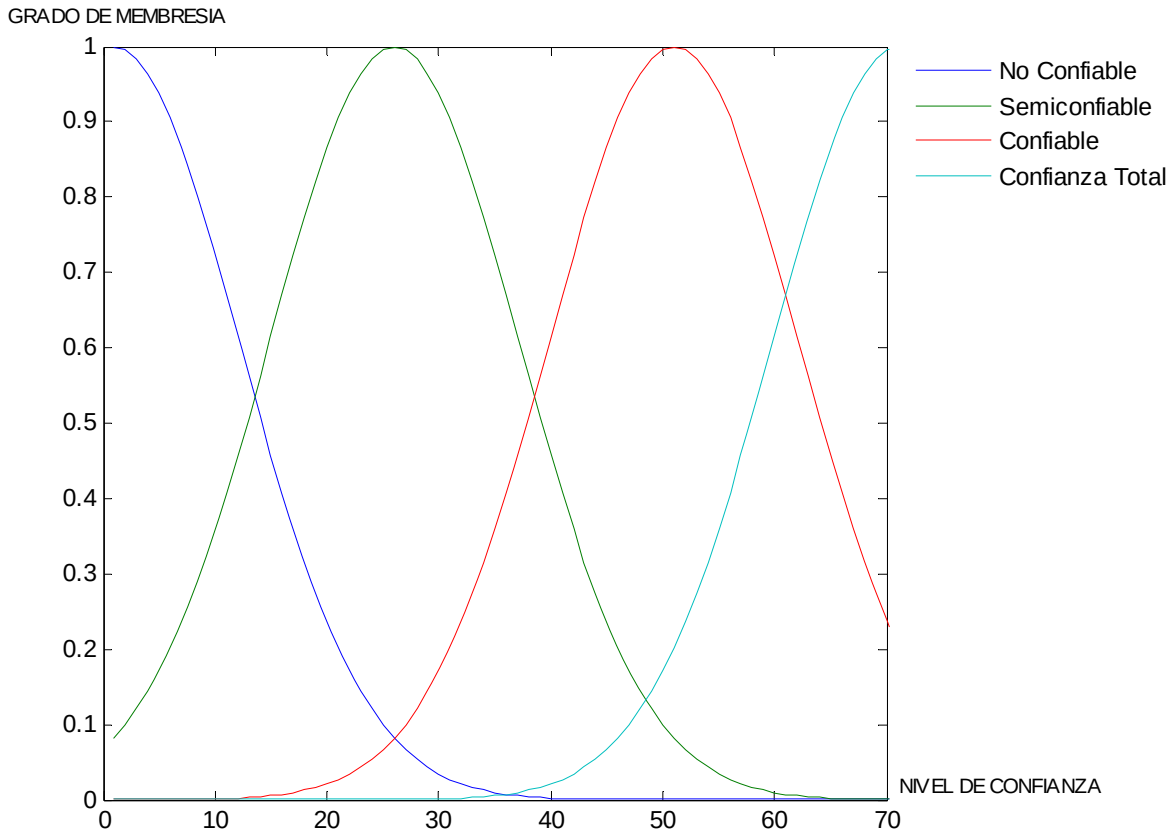

Fig. 6.5 Gráfica nivel de confianza (Original en colores).

Para poder observar de mejor manera la gráfica tiene una escala de 10 a 1.

6.2 OPERACIÓN DEL MODELO.

6.2.1 OBTENCIÓN DEL NIVEL DE CONFIANZA.

Una vez que hemos revisado los elementos que intervienen en el modelo la operación se da de la siguiente manera, las tres variables de entrada se difusifican para convertirse en grados de membresía para cada uno de los conjuntos, se evalúan con el mecanismo de inferencia difusa que tiene cargada la base de conocimientos y se obtiene como resultado un conjunto difuso resultante del nivel de confianza este a su vez pasa por la defusificación y obtenemos el valor nítido de la variable nivel de confianza por cada sesión.

El nivel de confianza nos ayuda a establecer los servicios que se pueden asignar a los nodos vecinos una vez que fueron evaluados, hasta este momento el nivel de confianza podría ser tan variable que se comportar de una manera extremosa, en la sección de resultados podremos observar este comportamiento.

Para controlar estas variaciones se adhirieron dos funciones: ventana estándar y largo plazo, estas funciones sirven para administrar el modelo en la variable de confianza que se ocupa para definir el grado de autenticación y generar un conocimiento a largo plazo logrando una dinámica temporal.

6.2.2 VENTANA ESTÁNDAR.

Ventana estándar: Inicialmente la variable nivel de confianza se retroalimenta como comportamiento durante las iteraciones definidas dentro de la ventana, cuando se llega al límite definido de sesiones se lleva a cabo el cálculo promedio de las iteraciones previas del comportamiento, en nuestras pruebas se definió que la ventana se calculara cada 7 sesiones, el valor obtenido se compara con el nivel de confianza previo para determinar si de acuerdo al comportamiento observado en la ventan puede subir de nivel de confianza el nodo evaluado, quedar con el mismo grado o decrecer el nivel. Este procedimiento es muy importante dado que nos va a dar como resultado el nivel de confianza que se va a aplicar para el nodo evaluado hasta que se cuente con una nueva evaluación estándar.

6.2.3 LARGO PLAZO.

Largo plazo: Esta función tiene como objetivo generar un conocimiento del nivel de confianza durante un periodo de tiempo mayor que la ventana estándar su objetivo es poder identificar a un largo plazo el comportamiento que se observa del nodo evaluado, este procedimiento entra en funcionamiento cuando se llega al limite definido dentro del largo plazo, para las pruebas se definió el valor del limite como 35, la forma de obtenerlo es mediante la formula:

$$\text{Largo Plazo} = w_1 \quad m_1 + w_2 \quad m_2$$

En donde m_1 es el cálculo promedio del comportamiento de los últimos registros definidos en el límite, m_2 es el valor obtenido de la ventana estándar, w_1 es el peso referencial que se le da al cálculo a largo plazo, para nuestras pruebas se definió como 0.6 y w_2 es el peso referencial que se le dio al calculo de la ventana estándar, para el modelo se definió como 0.4, al aplicar la formula se obtiene el valor del nivel de confianza a largo plazo y se actualiza también el valor obtenido de la ventana estándar.

6.2.4 APLICACIÓN DEL NIVEL DE CONFIANZA.

Una vez definidos los componentes del modelo, observamos que el nivel de confianza puede variar de acuerdo a los valores que en ese momento se inyectan al sistema, por lo que la obtención del nivel de confianza proviene del cálculo de la ventana estándar. Con este dato podemos autenticar a los demás nodos asignándoles un grado de autenticación variable que nos va a permitir tener el control de acceso a los servicios que puedo proporcionar al nodo evaluado de la siguiente manera:

Tenemos al nodo A y el nodo B Fig. 6.6.

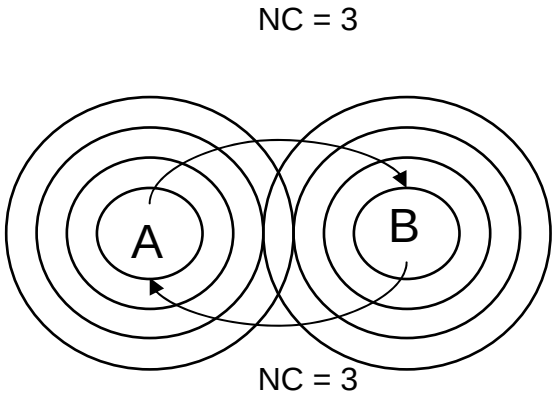

Fig. 6.6 Red ad hoc inicial.

Ambos nodos acaban de crear una red ad hoc, y cada uno evalúa en su sistema de inferencia difusa el nivel de confianza con el que van a ocupar esa sesión guardando el registro del nodo con el cual tiene contacto. Como es la primera vez que se conocen el nivel de confianza utilizado es igual a 3 de acuerdo a lo explicado en los componentes del modelo. Con el paso de las sesiones en el tiempo, el tráfico generado entre los nodos y el comportamiento evaluado en el sistema de inferencia difusa entre el nodo A y B, la ventana estándar pueden subir o bajar su nivel de confianza, para este ejemplo suponemos que ambos nodos se portaron de forma correcta y que ambos aumentaron mutuamente su nivel de confianza a 4.

En ese momento entra el nodo C a la red ad hoc que tenían generada los nodos A y B, los niveles de confianza que tienen especificados cada uno de ellos entre sí sería de la siguiente manera:

Tabla 6.4 Evaluación de nivel de confianza entre nodos.

NODO EVALUADOR	NODO EVALUADO	NIVEL DE CONFIANZA GENERADO
A	B	4
A	C	3
B	A	4
B	C	3
C	A	3
C	B	3

La red ad hoc con sus respectivos niveles de confianza sería de la siguiente manera Fig. 6.7.

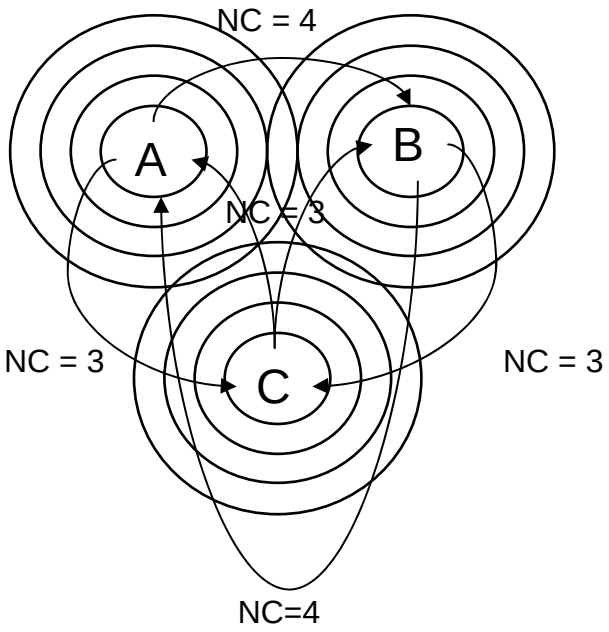

Fig. 6.7. Red ad hoc con tres nodos y sus niveles de confianza.

Como podemos observar nuestro modelo de autenticación por niveles de confianza nos permite identificar a los nodos dentro de la red y establecer distintos niveles de confianza entre los nodos que conforman la red. Con la autenticación generada por el modelo podemos controlar el acceso a servicios apoyándonos de una matriz que define los accesos que podemos utilizar de acuerdo al nivel de confianza que se tiene evaluado en el sistema de inferencia difusa.

Cuando un usuario es autenticado en una red con infraestructura se revisan las políticas de seguridad para determinar los permisos y servicios a los cuales el usuario puede entrar, como podemos ver en nuestro modelo cada uno de los nodos puede generar sus propias políticas de seguridad para cada nivel de confianza.

La siguiente tabla muestra un ejemplo de configuración de políticas de seguridad y los servicios que proporciona el nodo de acuerdo al nivel de confianza adquirido.

Tabla 6.5 Matriz de políticas de seguridad de acuerdo al nivel de confianza.

		Servicios						
	Nivel de confianza	Servicio de ruteo	Servidor de Impresión	Acceso a Internet	Servidor de archivos.	Servicios de FTP	Entidad Certificadora	Servicios especiales.
Política	0							
	1							
	2	X						
	3	X	X					
	4	X	X	X				
	5	X	X	X	X	X		
	6	X	X	X	X	X	X	
	7	X	X	X	X	X	X	X

Entre los servicios tenemos:

- Servicio de ruteo: Actúa como ruteador del nodo autenticado cuando éste lo solicita.
- Servidor de impresión: Da el servicio de servidor de impresión del nodo autenticado.
- Acceso a Internet: Permite al nodo autenticado utilizar el servicio de Internet cuando se encuentre conectado a una red con infraestructura.
- Servidor de archivos: Permite al nodo autenticado utilizar una parte del disco para guardar archivos.
- Servicios de FTP: Permite utilizar al nodo autenticado una sesión de FTP.
- Entidad certificadora: Puede utilizar al nodo autenticado como entidad certificadora cuando se requiera de un canal encriptado con algún otro nodo de la red, para ello este último también debe confiar en el nodo autenticado.
- Servicios especiales: Base de datos, servidor web entre otros.

Como podemos observar en la matriz, a mayor nivel de confianza es mayor la cantidad de servicios que el nodo ofrece al nodo autenticado.

6.3 DINAMISMO DEL MODELO.

Durante la explicación del modelo se revisaron los valores propuestos para nuestras pruebas, dentro de ellos hablamos de la sesión, en nuestro caso la sesión se genera por día de transmisión con el nodo evaluado sin embargo podrían generarse varios esquemas dependiendo de cómo queremos que se comporte nuestro nodo, podemos configurar las variables de entrada para que se evalúen en tiempos más cortos o más largos, redefinir los límites de los conjuntos, aumentar o disminuir los niveles de confianza para generar un mayor número de políticas de seguridad.

6.4 DEFINICIÓN DEL TAMAÑO DE LA MUESTRA.

Una vez definido el modelo y su funcionamiento vamos a revisar el tamaño de las pruebas ya que si tratáramos de generar un estudio total nos veríamos en un gran problema ya que la población de nuestro modelo son todos los números enteros positivos Z^+, por ello necesitamos definir una muestra, para las pruebas de nuestro modelo no requerimos de una cuenta absolutamente exacta de la población.

Tradicionalmente existen 2 tipos de muestras:

- El Muestreo aleatorio o probabilístico.
- Muestreo no aleatorio o no probabilístico.

Muestreo aleatorio.

Como su nombre indica está basados en el azar, se caracteriza porque todos los elementos tienen siempre la misma probabilidad de resultar elegidos, en principio pensar en un procedimiento es bueno pero en la práctica para ser representativo se utilizan los números aleatorios.

Muestreo no aleatorio.

El muestreo no aleatorio, consiste en la elección de una muestra según el juicio del equipo investigador y depende de los criterios utilizados para escoger los componentes de la muestra.

Tamaño de la muestra.

El tamaño de una muestra depende del error estándar de la media que queremos tener, si incluimos el total de la población entonces el error estándar tiende a cero aunque este es un caso extremo que no se encuentra en la práctica, dado un nivel de confianza y un error fijo de estimación se puede escoger un tamaño de muestra

La muestra es el número de elementos, elegidos o no al azar, que hay que tomar de un universo para que los resultados puedan extrapolarse al mismo, y con la condición de que sean representativos de la población. El tamaño de la muestra depende de tres aspectos:

- Error permitido.
- Nivel de confianza con el que se desea el error.
- Carácter finito o infinito de la población.

La fórmula general para determinar el tamaño de una muestra es la siguiente:

$$n = \frac{Z^2 P/Q}{E^2}$$

En donde:

n = Número de elementos de la muestra.

P/Q = Probabilidades con las que se presenta el fenómeno.
Z^2 = Valor crítico correspondiente al nivel de confianza elegido.
E = Margen de error permitido.

Estos métodos son útiles para realizar estudios de mercado o determinar la cantidad de elementos de un estudio en una población sin embargo de la forma dinámica que se construyo el modelo y las pruebas realizadas optamos por definir de manera aleatoria la cantidad de iteraciones para cada uno de los modelos, iniciamos con 50 iteraciones y fuimos haciendo crecer la cantidad hasta llegar a 1000, sin embargo al obtener los resultados nos dimos cuenta que los comportamientos seguian siendo muy parecidos aun variando la cantidad de pruebas por ello se decidió reducir la cantidad de iteraciones a 400..

6.5 RESULTADOS OBTENIDOS DEL PROGRAMA.

Para comprobar el funcionamiento del modelo construimos un ambiente de pruebas con tres nodos los cuales se detallaron previamente en este capítulo, se conectaron en una red ad hoc y definimos cinco diferentes tipos de pruebas en donde vamos a analizar cada una de las variables de entrada y la salida así como el resultado de la ventana estándar y a largo plazo, para cada prueba se tomaron en cuenta doscientas sesiones obteniendo los siguientes resultados:

6.5.1 AMBIENTE IDEAL.

En esta configuración todos los nodos enviaban y recibían la información de forma correcta.

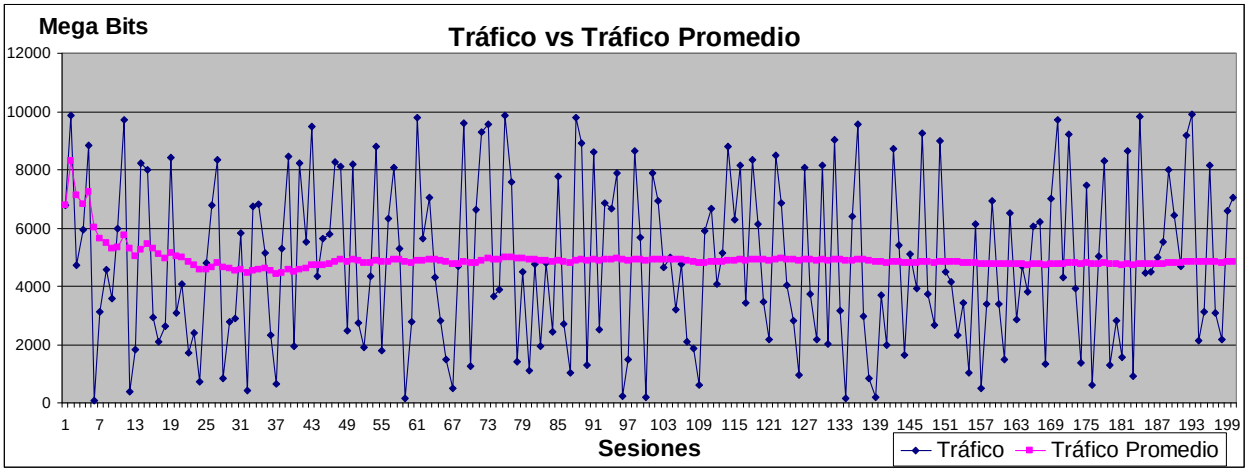

Fig. 6.8 Gráfica de tráfico contra tráfico promedio de transmisión en ambiente ideal (Original en colores).

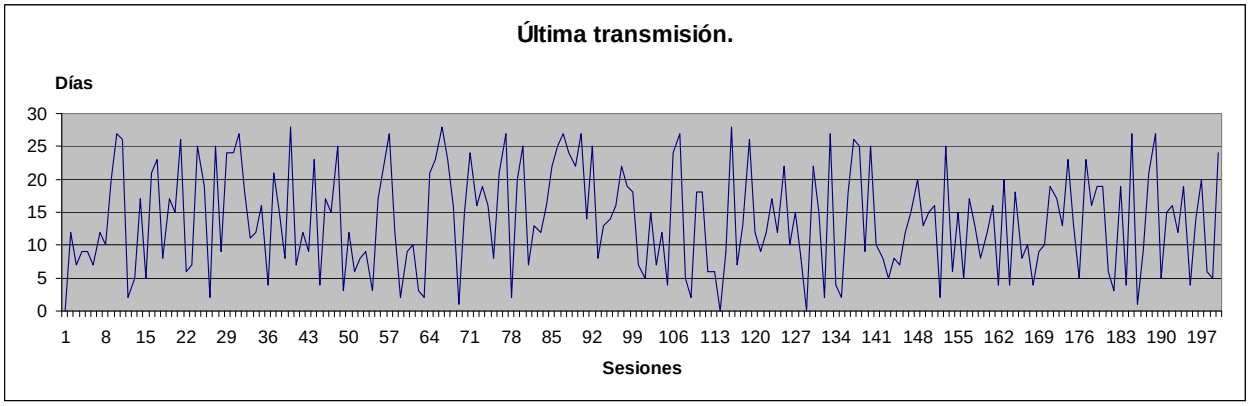

Fig. 6.9 Gráfica de última transmisión en ambiente ideal (Original en colores).

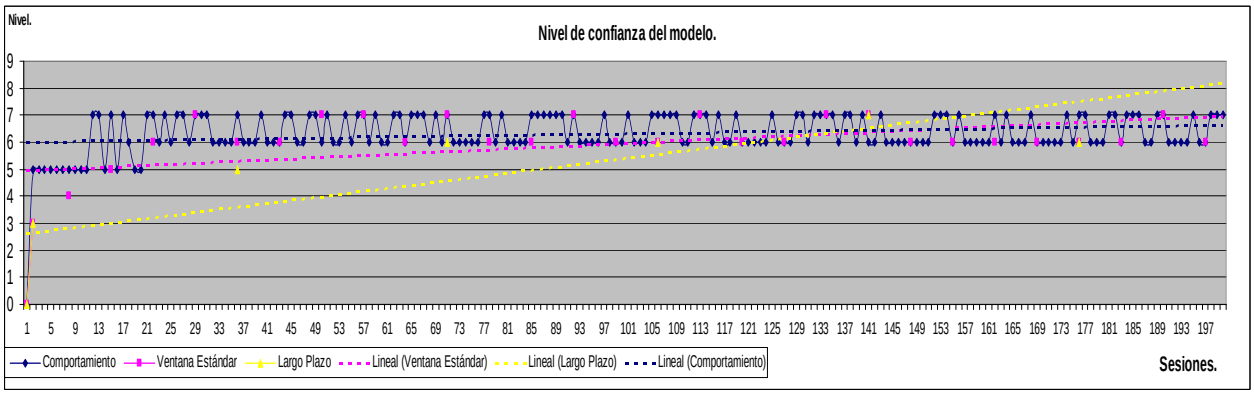

Fig. 6.10 Gráfica del nivel de confianza del modelo en ambiente ideal (Original en colores).

6.5.2 NODOS MALICIOSOS.

En esta configuración todos los nodos se portaron de manera maliciosa, la información no fluía en la red.

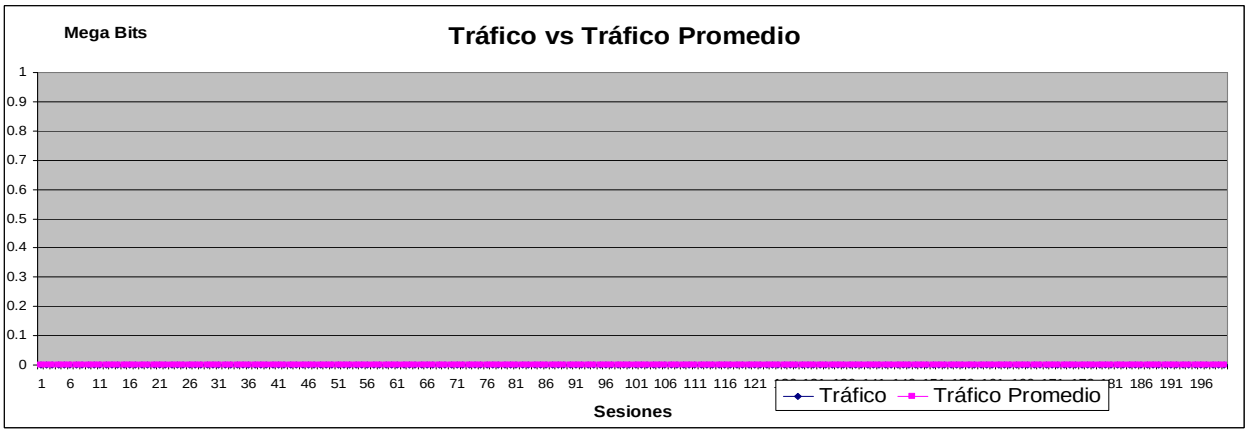

Fig. 6.11 Gráfica de tráfico contra tráfico promedio de transmisión en nodo malicioso (Original en colores).

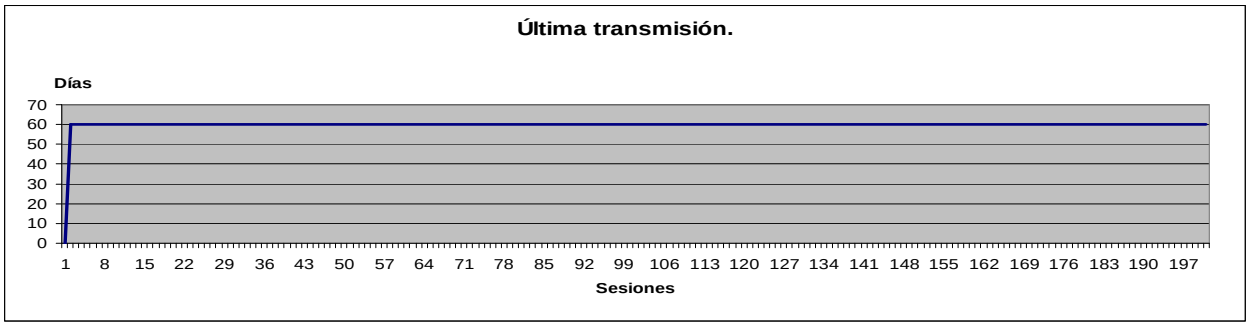

Fig. 6.12 Gráfica de última transmisión en nodo malicioso (Original en colores).

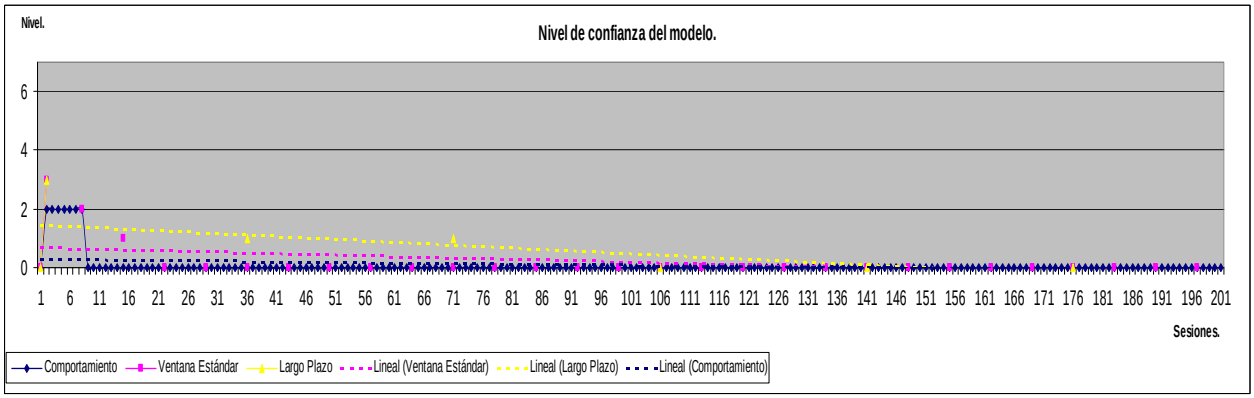

Fig. 6.13 Gráfica del nivel de confianza del modelo en nodo malicioso (Original en colores).

6.5.3 NODOS INTERMITENTES.

En esta configuración los nodos en ocasiones enviaban la información y en otras dejaban de hacerlo.

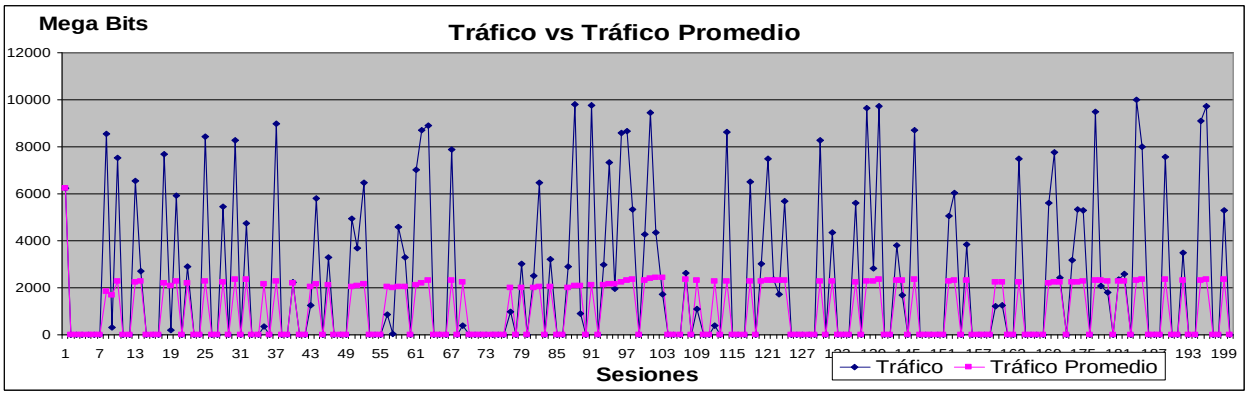

Fig. 6.14 Gráfica de tráfico contra tráfico promedio de transmisión en nodo intermitente (Original en colores).

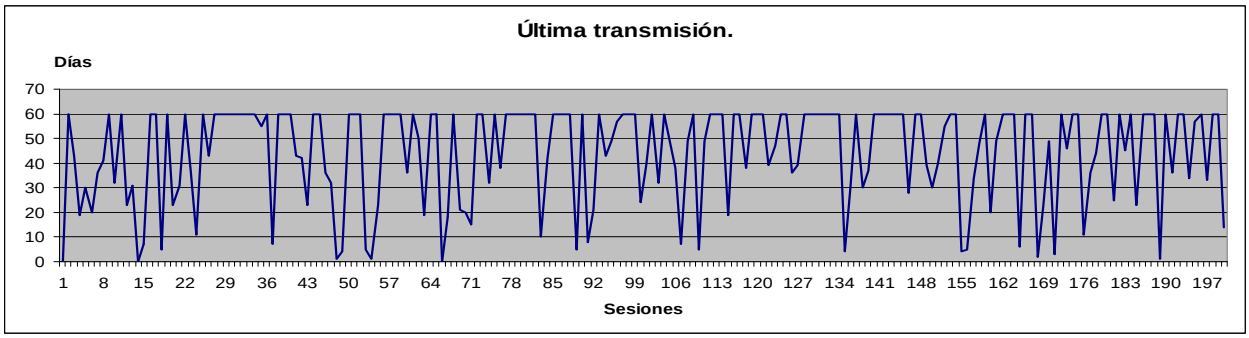

Fig. 6.15 Gráfica de última transmisión en nodo intermitente (Original en colores).

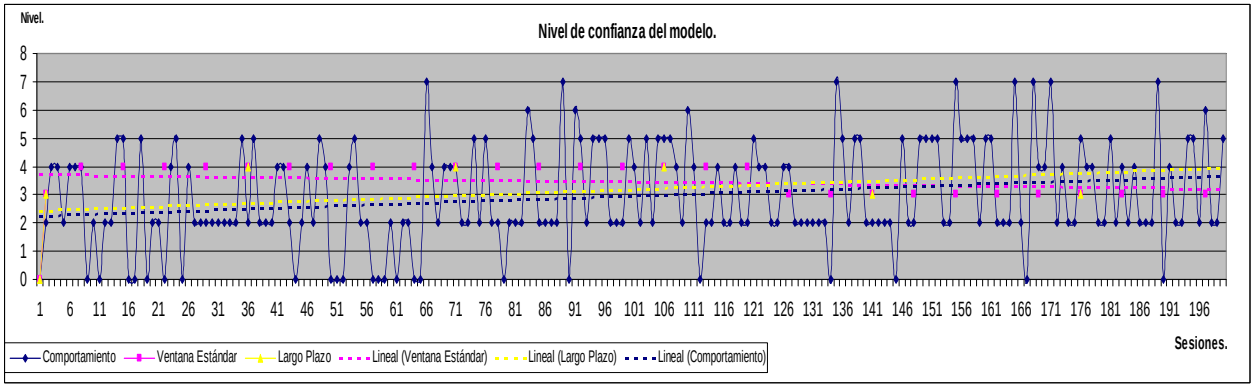

Fig. 6.16 Gráfica del nivel de confianza del modelo en nodo intermitente (Original en colores).

6.5.4 NODOS INTERMITENTES MALICIOSOS.

En esta configuración los nodos por un periodo de tiempo se comportaban de manera intermitente y en otro periodo eran completamente malicioso impidiendo la transmisión de la información.

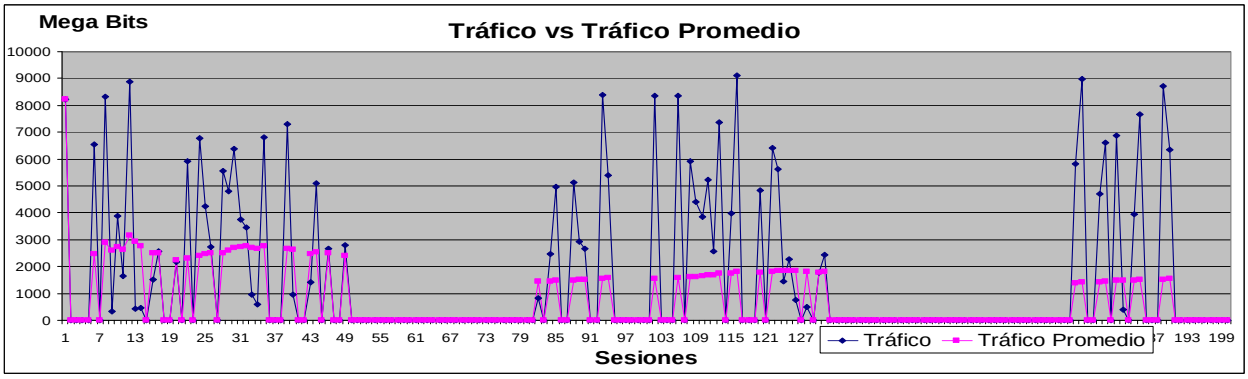

Fig. 6.17 Gráfica de tráfico contra tráfico promedio de transmisión en nodo intermitente malicioso (Original en colores).

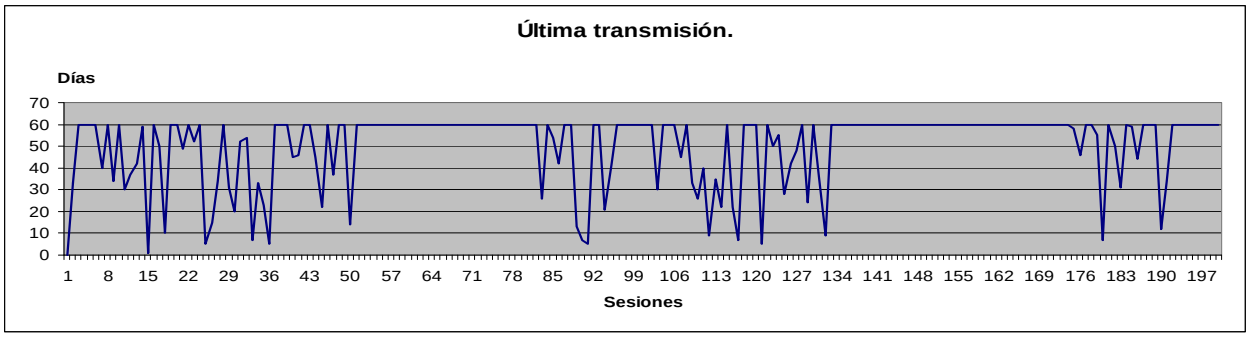

Fig. 6.18 Gráfica de última transmisión en nodo intermitente malicioso (Original en colores).

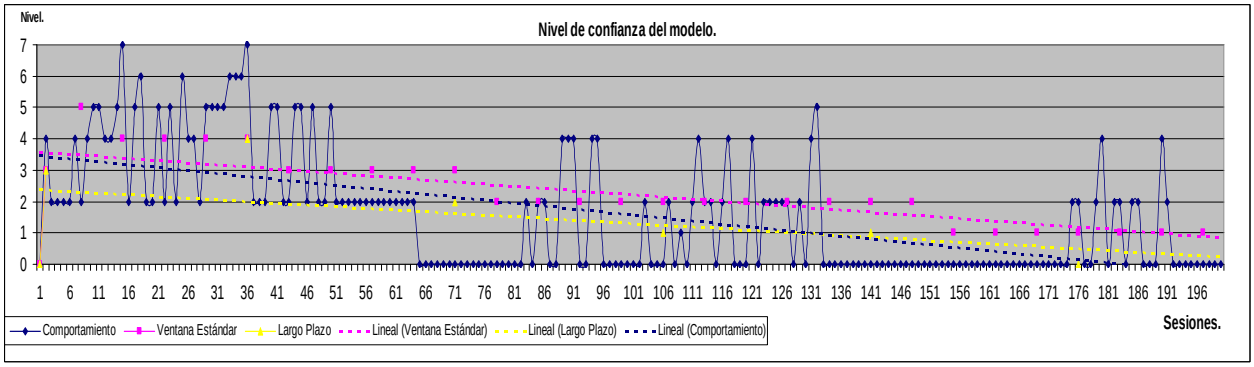

Fig. 6.19 Gráfica del nivel de confianza del modelo en nodo intermitente malicioso (Original en colores).

6.5.5 NODOS INTERMITENTES IDEALES.

En esta configuración los nodos enviaban se comportaban de manera intermitente en un periodo de tiempo y después se convertían en transmisores ideales.

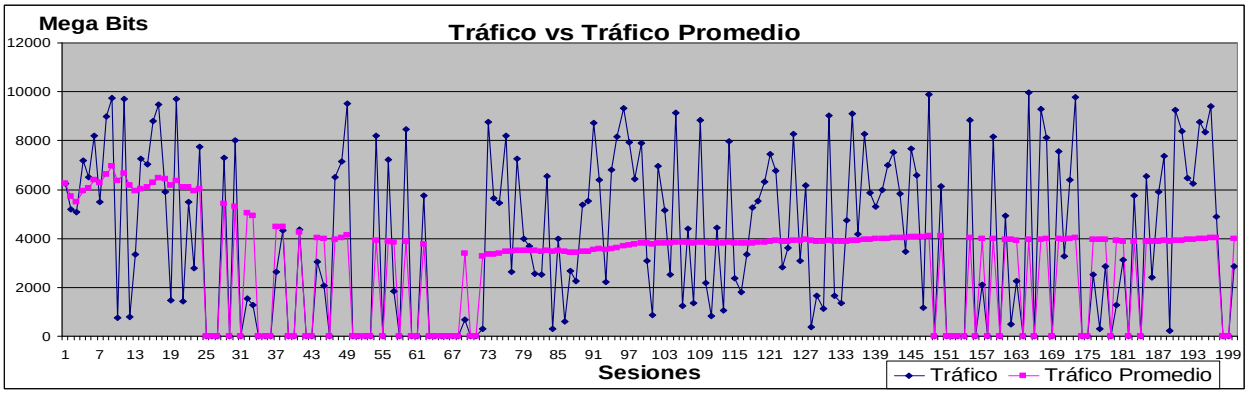

Fig. 6.20 Gráfica de tráfico contra tráfico promedio de transmisión en nodo intermitente normal (Original en colores).

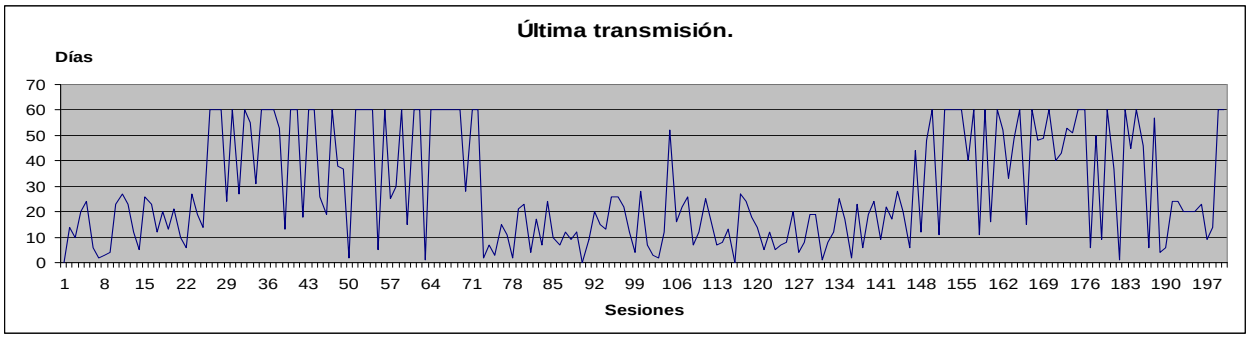

Fig. 6.21 Gráfica de última transmisión en nodo intermitente normal (Original en colores).

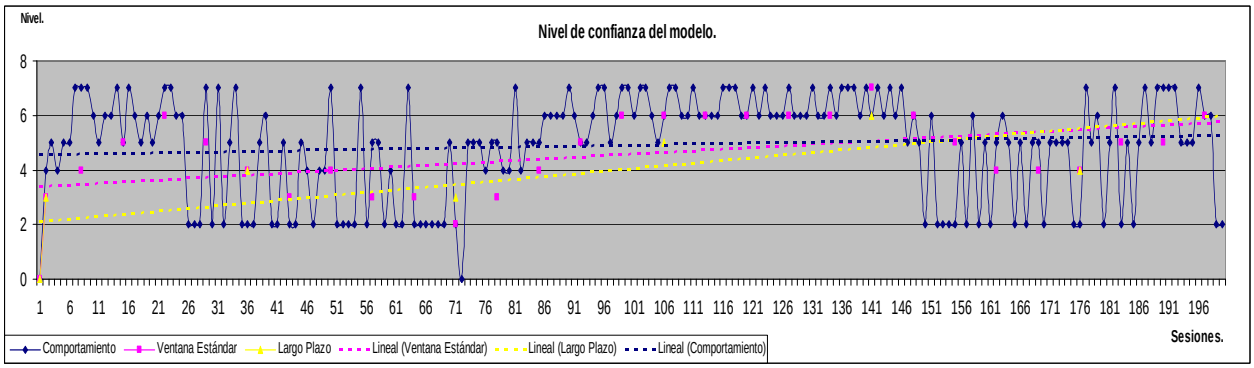

Fig. 6.22 Gráfica del nivel de confianza del modelo en nodo intermitente normal (Original en colores).

6.5.6 ANÁLISIS DE LOS RESULTADOS OBTENIDOS.

En la Tabla 6.6 podemos observar un análisis de los resultados obtenidos con 400 sesiones, dependiendo del comportamiento en el nodo evaluado se distribuye la evaluación del modelo de distintas maneras.

Tabla 6.6 Análisis de resultados por tipo de nodo.

Tipo de Nodo	Nivel de confianza			Distribución del nivel							
Tipo	Mínimo	Máximo	Promedio	0	1	2	3	4	5	6	7
Malicioso	0	3	0.04	98%	0%	2%	0%	0%	0%	0%	0%
Normal	3	7	6.42	0%	0%	0%	0%	0%	4%	51%	45%
Intermitente	0	7	3.05	9%	12%	36%	0%	16%	21%	2%	4%
Intermitente Malicioso	0	7	1.26	45%	15%	22%	0%	11%	5%	1%	1%
Intermitente Normal	0	7	5.01	0%	6%	17%	0%	3%	22%	29%	23%

7 CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES.

A lo largo de este trabajo de tesis pudimos construir un modelo de autenticación dinámico para redes ad hoc; En él pudimos observar como las máquinas podrían generar confianza entre ellas para proporcionar servicios a través del tiempo sin necesidad de tener una entidad certificadora, con la base de inferencia propuesta logramos incrementar la confianza entre los nodos así como aislar los que presentaban comportamientos malicioso.

Los comportamientos observados dentro de los distintos escenarios nos mostraron como el modelo puede variar a lo largo del tiempo dando entrada a una configuración automática en la cual el control de acceso a cada servicio dependía del nivel de confianza observado en la ventana estándar, cuando el nodo tenia un comportamiento ideal el nivel de confianza tiende a aumentar, sin embargo cuando se comportaba de manera maliciosa disminuía al grado de dejar de prestarle servicios.

Al construir el modelo sobre un mecanismo de inferencia difusa logramos generar que fuera dinámico y configurable. Definimos los conjuntos y matriz de inferencia base que pueden llegar a evolucionar en cada uno de los nodos y adoptar sus propios modelos.

Aunque por su naturaleza las redes ad hoc requieren interconectarse libremente podemos aplicar políticas de seguridad a los nodos de acuerdo a la confianza generada, los resultados que obtuvimos muestran como se distribuyen en los distintos niveles de acuerdo al tipo de nodo configurado en la red siendo el nodo normal el que alcanzó los más altos niveles de confianza por mayor tiempo y siendo el nodo malicioso el que se mantuvo aislado de la red durante casi todo el tiempo registrado.

7.2 TRABAJO FUTURO.

Las redes ad hoc tienen grandes oportunidades de investigación, en este trabajo de tesis propusimos un modelo para la autenticación basado en lógica difusa y dan pie a distintas investigaciones como:

Evolución del modelo: Actualmente el modelo esta acotado a tres variables de entrada y una de salida con conjuntos definidos, podemos utilizar sistemas expertos para generar conocimiento

sobre los distintos comportamientos de los nodos y poder aplicar no sólo un modelo sino dependiendo del entorno en el que nos encontremos ajustar los valores del modelo, este conocimiento nos permitiría conectarnos a distintas redes ad hoc y variar de una manera más rápida o lenta el nivel de confianza es decir el modelo puede proporcionar más servicios cuando detecta que se encuentra en una red de tu salón de clases en donde los nodos vecinos son más confiables que cuando te encuentras una red en un sitio público.

Políticas de Seguridad: Aunque el modelo propone una serie de servicios que proporciona de acuerdo al nivel de confianza, las políticas de seguridad son más que eso, podríamos pensar en un esquema en el cual los nodos en una red ad hoc puedan homologar las políticas o generar excepciones de acuerdo a los niveles de confianza que se logren en la red.

8 REFERENCIAS

[1] Rappaport, T. S. *Wireless Communications*. Prentice Hall, 1996.

[2] Donald C. Cox (1995) Wireles Personal Comunications: What Is It? IEEE Pers. comm. pp. 20-30.

[3] Tanenbaum, A. S. *Computer Networks*. Prentice Hall, 1996.

[4] C-K Toh Ad hoc Movile Wireless Networks Protocols and System, Primera edición, Prentice Hall, 2002, 302 p.

[5] Stalling William. Wireless Comunications and Networks, Primera edición Prentice Hall, 2002, 584 p.

[6] Kazantzidis Manthos, Kapoor Rohit, Gerla Mario. Bluetooth: An Enabler for Personal Area Networking. IEEE Network September/October 2001 pág. 28-37.

[7] WWRF/WG4 Subgroup on Ad hoc Networking, Contribution to the 6th WWRF meeting London UK. June 2002. White paper.

[8] Konrad Wrona. Distributed Security: Ad hoc Networks & Beyond. Pampas workshop September 16-17 2002.

[9] Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic. Routing and Security in Mobile Ad hoc Networks. Computer Magazine IEEE February 2004 pág 61-65.

[10] IETF Manet http://www.ietf.org.com/manets Liga oficial de la Fuerza de tarea de ingenieros en Internet para el estudio de Manets.

[11] T. Larsson y N. Hedman: ``Routing Protocols in Wireless Ad hoc Networks - A simulation Study", master's thesis, Lulea University of Technology, Estocolmo, 1998.

[12] C. E. Perkins y P. Bhagwat: ``Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of the SIGCOMM '94, Conference on Communications Architectures, Protocols and Applications, Agosto 1994, pp. 234-244.

[13] C. E. Perkins y E. M. Royer: ``Ad hoc On-Demand Distance Vector Routing", Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, Febrero 1999.

[14] David B. Johnson y David A. Maltz: ``Dynamic Source Routing in Ad hoc Wireless Networks", Mobile Computing, editado por Tomasz Imielinski y Hank Korth, capítulo 5, pp. 153-181. Kluwer Academic Publishers, 1996

[15] V. D. Park y M. Scott Corson: ``A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", Proceedings of INFOCOM '97, Abril 1997, pp. 1405-1413.

[16] http://www.iec.csic.es/criptonomicon/acceso/

[17] “Computer System and Network Security” capítulo 4 G.B. White, E.A. Fisch, U.W.Pooch CRC Press 1996

[18] Criptografía y Seguridad en Computadores, 3º Edición – 2002 - Manuel J. Lucena López

[19] http://www.lasalle.edu.co/csi_cursos/informatica/termino/seguridad_informatica.htm

[20] R. Subiela y Gonzalez-Mendoza, M., Titli, A. León.: ``SIMULACIÓN DE PROTOCOLOS DE ENCAMINAMIENTO EN REDES MÓVILES AD HOC CON NS-2", 2005.and Hernandez-Gress, N.. *SVM clustering for identification of Takagi-Sugeno fuzzy models*. 5th IFAC International symposium of Intelligent Components and Instruments for Control Applications, SICICA. July 9-11 2003, Aveiro, Portugal

[21] Gonzalez-Mendoza, M.. *Surveillance temps–réel des systèmes Homme–Machine. Application à l’assistance à la conduite automobile*. Thèse LAAS-INSAT, Toulouse France, July 2004.

[22] Zadeh, L. A.. *Fuzzy sets*. Information and Control, volume 8, pp. 338-353, 1965.