Bibliografía Anotada

Carlos Felipe Téllez Castaño

Seminario de Investigación I
Maestría en Ingeniería de Sistemas y Computación
05 de mayo de 2006

Referencias

[1] Anderson Gustave, Leonardo Urbano, Gaurav Naik, David Dorsey, Andrew Mroczkowski, Donovan Artz, Nicholas Morizio, Andrew Burnheimer, Kris Malfetone, Dan Lapadat, Evan Sultanik, Saturnino Garcia, Max Peysakhov, William Regli and Moshe Kam. "***A Secure Wireless Agent-based Testbed***". Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04). Pages=19. 2004.

Este artículo habla sobre la recopilación de algunos algoritmos de enrutamiento en redes MANET (Mobil Ad-Hoc Network) como CLIQUES, Spread, Secure Spread, EMAA, RSA, IPSec y los algoritmos proactivos de enrutamiento, para así determinar las fallas en los nodos nocivos que ocasionan desrutamiento e intrusión a través de un sistema de detección de fallos basado en agentes móviles. Las pruebas para la determinación de este sistema de seguridad MANET, para este paper, se hacen sólo sobre PDAs, un limitante en cuanto a resultados se refiere para los casos más prácticos cotidianos, sin embargo la infraestructura SWAT es muy aplicable para cualquier caso de seguridad wireless así como la determinación del nuevo sistema de enrutamiento que se propone con los agentes.

[2] Artz Donovan and Maxim Peysakhov and William C. Regli. "***Network Meta-Reasoning for Information Assurance in Mobile Agent Systems***". Proceedings of the Eighteenth International Joint Conference on Artificial Intelligence. Publisher: Morgan Kaufmann, pages: 1455-1457. 2003.

Este artículo explica una propuesta sobre detección de intrusos en redes Ad-Hoc, basándose en la teoría de agentes inteligentes para dar alerta a la intrusión. Lo más sobresaliente del artículo, es la formulación para determinar a través de una teoría de conjuntos muy bien explicada, un esquema base de reflejo y predicción de los nodos nocivos en la red, usando un sistema de asociación para determinar cuáles

nodos son pertenecientes a la red y cuáles no lo son. Esto genera algoritmos que usan teoría lógica para llegar a la detección asociando valores y propiedades de la red y de los nodos.

[3] Asokan N. and Philip Ginzboorg. "***Key-Agreement in Ad-hoc Networks***" Computer Communications journal. Volume:23, pages:1627-1637, number:17, 2000.

Este artículo trata un supuesto particular. Teniendo en cuenta un pequeño grupo de personas que se encuentran en una reunión o conferencia en un cuarto, cada uno con un dispositivo móvil (como un computador portátil), desea acceder a la red de la conferencia que está siendo dictada. Lo que se quiere alcanzar es: como acceder a la red inalámbrica, sin que otras personas que se encuentren por fuera del recinto puedan acceder a la conferencia; además, como establecer un intercambio de datos privado dentro del mismo cuarto. La propuesta aunque parece trivial, entrega un enfoque acertado de la asignación de claves a través de un método conocido como Intercambio tolerante de la llave de Diffie-Hellman donde se realizan cálculos matemáticos sencillos por el número de personas que se encuentran vigentes en la red Ad-Hoc (pues no existen puntos de acceso), para la entrega de una clave generada aleatoriamente, donde no exista colisión, ni duplicado de estas llaves.

[4] Blazevic L. and L. Buttyan and S. Capkun and S. Giordano and J. Hubaux and J. Le Boudec. "***Self-organization in mobile ad-hoc networks: the approach of terminodes***". IEEE Communications Magazine. 2001.

Este artículo muestra una organización más especifica en la redes Ad-hoc, en cuanto a enrutamiento y control se refiere. Dentro del artículo se le llaman a los nodos de la red MANET: terminodos o nodos terminales. El propósito es tomar el protocolo de enrutamiento AMRoute, ya que este usa la generación de árboles de usuario o clasificación jerárquica de los nodos según su prioridad. Lo que se pretende es alcanzar una comunicación privada sin tener que arriesgar el flujo de datos por la comunicación de nodos. Es un artículo muy interesante pues presenta un enfoque muy distinto a los distintos tipos de enrutamiento proactivos de las redes Ad-Hoc. Además, el enfoque del nodo terminal, pretende ahorrar recursos en la red.

[5] Boyd Colin and Anish Mathuria. "***Key Establishment Protocols for Secure Mobile Communications: A Selective Survey***". Lecture Notes in Computer Science Journal. Volume:1438, pages:344-350, year:1998.

En este "survey" lo que se hace es cuestionar y diagnosticar los distintos tipos de acceso que se tienen en redes por cable y redes wireless para establecer criterios

de funcionalidad. Básicamente comparan algunos protocolos usados en la actualidad, como el establecimiento de algoritmos de extracción de raíz de datos (MSR) y la aplicación de algoritmos de Beller y Yacobi para la detección de ataques sin frameworks estables. Es un artículo muy pertinente para entender la lógica funcional a la hora de detectar intrusos en redes Ad-hoc.

[6] Bradley K. A. and S. Cheung and N. Puketza and B. Mukherjee and R. A. Olsson. "***Detecting Disruptive Routers: A Distributed Network Monitoring Approach***". Booktitle: Detecting Disruptive Routers: A Distributed Network Monitoring Approach. Pages 115-124. 1997.

Básicamente, el artículo habla de los ataques que sufren las redes por cable y vulnerabilidad existente desde los routers que funcionan como puerta de enlace. Lo que se pretende es controlar dichos ataques siguiendo un monitoreo de los mismos y estableciendo unos parámetros de control, tales como velocidad de enrutamiento, generación de tablas de enrutamiento estables, y procesos de envió de mensajes de acuse de recibo desde el mismo router. Creo que es pertinente pues se puede aplicar para redes Ad-hoc donde todos los nodos se comportan como routers.

[7] Josh Broch and David A. Maltz and David B. Johnson and Yih-Chun Hu and Jorjeta Jetcheva. "***A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols***". In Proc. of the ACM/IEEE MobiCom. Booktitle: Mobile Computing and Networking, pages: 85-97, 1998.

Muy buen artículo que muestra una simulación construida sobre 50 nodos para comparar los distintos protocolos de enrutamiento existentes para redes MANET, con sus distintos algoritmos. Aunque no es especifico con la construcción del simulador, si muestra resultados que pueden ser muy relevantes para el proyecto de investigación. Los protocolos estudiados son DSDV-SQ, TORA, DSR y AODV-LL. Con base en esto, se puede definir sobre que protocolo construir el IDS para redes MANET del tema de investigación personal.

[8] L. Buttyfin and J. Hubaux. "***Report on a Working Session on Security in Wireless Ad Hoc Networks***". Mobile Computing and Communications Review. Volume 6, Number 4. November 2002.

Consiste en una recopilación de artículos sobre seguridad en redes Ad-Hoc, pero para dar a conocer las principales causas de los problemas que surgen en una red MANET o sus respectivas dificultades tales como el constante cambio de canales y nodos así como sus vulnerabilidades, el cambio dinámico en las topologías de la red y un tema muy concreto como lo es la intrusión. Resulta de la recopilación de las muchas técnicas usadas, teniendo en cuenta artículos ya nombrados dentro de

ésta bibliografía anotada pero con la singularidad de relacionar unos con otros con respecto al tema de seguridad inalámbrica para redes móviles. Muy pertinente.

[9] S. Toumpis and A. Goldsmith, "***Capacity Regions for Wireless Ad-Hoc Networks***". International Symposium on Communication Theory and Applications. 2001.

Este completo artículo, da a conocer el desempeño de una red Ad-Hoc con topologías y número de nodos aleatorios. Este desempeño se expresa matemáticamente, para dar a conocer los recursos utilizados en una red Ad-Hoc tales como distribución de energía, radio de comunicación o rango de transmisión, enrutamiento, entre otros. Estas expresiones matemáticas dan un acercamiento a la abstracción de las redes MANET, para conocer más a fondo, las distintas variables que involucran el óptimo funcionamiento de una red móvil.

[10] Z. Haas and B. Liang. "***Ad hoc mobility management with randomized database groups***". Proceedings of IEEE ICC. 1999.

Este artículo muestra como se puede realizar la implementación del establecimiento de grupos de nodos de forma aleatoria para establecer entre el subgrupo una base de datos que proporcione la ubicación entre grupos y determine la capacidad de comunicación entre los mismos. Esto se hace con el fin de capturar la transmisión del grupo que se encuentre más contiguo el uno del otro. La aleatoriedad se establece de acuerdo a la densidad de la ubicación de los nodos en el área ocupada por la red. Lo destacado de este artículo es el enfoque matemático aplicado para tal fin.

[11] E. Royer and P. Melliar-Smith and L. Moser. "***An Analysis of the Optimum Node Density for Ad hoc Mobile Networks***". Submitted for publication, 2000.

Este artículo consiste en un análisis otorgado par determinar los mejores métodos de ahorro de recursos importantes a la hora de establecer una comunicación de nodos inalámbricos como lo es la potencia y la energía de cada nodo de una red MANET. Lo que se hace es determinar la densidad de ubicación de los nodos en una área específica y determinar cual es la mejor ruta de comunicación usando el protocolo de enrutamiento AODV, para así deshabilitar las conexiones que no cumplan con los parámetros para establecer comunicación temporalmente. Muestra muchos resultados pero pocas aplicaciones técnicas, sin embargo, los argumentos teóricos son muy fuertes, que son precisamente los que dan relevancia al artículo.

[12] David Chess and Colin Harrison and Aaron Kershenbaum. "***Mobile Agents: Are They a Good Idea?***". RC 19887 (December 21, 1994 - Reclassified March 16, 1995), address: Yorktown Heights, New York 1994.

Este artículo hace un estudio y diagnóstico de la aplicación de los agentes móviles en la seguridad de las redes computacionales de cualquier tipo. Lo destacado de este artículo es la presentación de los argumentos que hacen mostrar las ventajas en el tema de seguridad con respecto a la aplicación de los agentes móviles, además de las posibles alternativas de solución que pueden aplicarse en vez de este tipo de programas inteligentes y que pueden llegar a cumplir similares funciones. Asimismo presenta las desventajas de estos mismos y como podrían mejorarse en cuanto a la aplicación de sus funciones. Los argumentos son validos, sin embargo no aparecen muchas pruebas técnicas o formas de aplicar las mejoras o las soluciones alternativas de una forma detallada.

[13] C. Cordeiro and D. Agrawal, "***Mobile Ad Hoc Networking***". Brazilian Symposium on Computer Networks. pp. 125-186, May 2002.

Este extenso documento muestra las características propias de una red MANET, así como sus comportamientos y elementos fundamentales. Trata temas como la estructura, el enrutamiento, los tipos de protocolos usados, los sensores, la difusión, la coordinación, la autenticación, el clustering, el manejo de la energía, la potencia, los recursos necesarios para el establecimiento de una red Ad-Hoc incluyendo su Hardware, entre otros temas. Es esencial para tener en cuenta los avances de las redes MANET hasta el año 2002.

[14] X. Hong and M. Gerla and G. Pei and C. Chiang, "***A Group Mobility Model for Ad Hoc Wireless Networks***". Group Mobility Model for Ad Hoc Wireless Networks,In Proceedings of ACM/IEEE MSWiM'99. 1999.

Este artículo es una evaluación para los distintos tipos de modelos de movilidad de los caminos a seguir de nodos en redes inalámbricas en especial para redes MANET y la presentación de un nuevo modelo para la representación de la movilidad de los nodos. Lo que se hace es dar a conocer los distintos modelos probabilísticos de interacción entre los nodos de grupos de movilidad y las rutas que siguen con comportamientos estocásticos. Además se introduce un nuevo modelo llamado Reference Point Group Mobility (RPGM) que consiste en definir en un grupo de movilidad jerárquica de nodos determinado, un centro especifico de nodos por área donde factores como la velocidad, la aceleración y la dirección de los mismos dependen de este punto central o de referencia. Es básicamente la comparación y evaluación de los distintos modelos anteriores con respecto al RPGM.

[15] Y. Hu and A. Perrig and D. Johnson, "***Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks***". Institution: Department of Computer Science, Rice University, month: dec, year:2001.

Este artículo explica en que consiste el ataque wormhole en las redes MANET, la forma de identificarlo, procesarlo y detenerlo, así como la propuesta de un protocolo de autenticación de nombre TIK que usa como correas temporales entre los nodos, para tratar con este tipo de ataques. Wormhole (Hueco de gusano) consiste en un túnel que se forma en una red Ad-Hoc cuando un nodo atacante empieza a recibir paquetes sin pertenecer a la red, realizando captura de información y repite esta operación varias veces desde cualquier punto de la red y en cualquier momento.

[16] Y. Hu and A. Perrig and D. Johnson, "***Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks***". in The 8th ACM International Conference on Mobile Computing and Networking, September 2002.

El propósito de este artículo es mostrar la implementación de un protocolo de enrutamiento seguro para la prevención y corrección de ataques en redes MANET llamado Ariadne. Básicamente es un protocolo basado en primitivas de criptografía que trabaja sobre TESLA, un protocolo de autenticación broadcast que requiere poco tiempo de sincronización en la red. Además se habla del protocolo DSR (Dynamic Source Routing) que es la base para la implementación de Ariadne. Un punto interesante de este artículo, es la explicación de los ataques comunes en la red tales como blackmail, rushing, wormhole, gratuitous detour, entre otros que se encuentran clasificados en ataques de disrupción de enrutamiento o de consumo de recursos. Por otra parte se considera cual es la filosofía o modelo principal de un atacante en una red.

[17] Y. Hu and A. Perrig and D. Johnson. "***SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks***". Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), month: jun, pages:3-13. 2002.

Para este artículo, se realiza la presentación del protocolo SEAD (Secure Efficient Ad hoc Distance vector routing protocol) que consiste en un protocolo seguro de enrutamiento basado a su vez en el protocolo de enrutamiento DSDV (Destination-Sequenced Distance-Vector routing protocol). El propósito es realizar la implementación sobre el protocolo sin usar operaciones asimétricas criptográficas como muchos otros. Aunque no muestra una implementación detallada sobre el SEAD, si muestra una clasificación acertada de los posibles ataques en una red MANET.

[18] Y. Hu and A. Perrig and D. Johnson. "***Efficient Security Mechanisms for Routing Protocols***". In Proceedings of Network and Distributed Systems Security 2003.

En este artículo, se presentan básicamente 4 mecanismos de seguridad en redes computacionales, sustentados en técnicas de criptografía simétrica que pueden ser aplicadas en protocolos vector-distancia y protocolos vector-ruta que a su vez pueden ser incorporados en nuevos diseños de protocolos de enrutamiento seguro. Lo interesante de este artículo es la presentación de la técnica de autenticación de nodos a través de árboles, pues esta representación jerárquica puede ser útil a la hora de implementar un agente detector de intrusos en redes Ad-Hoc.

[19] Jean-Pierre Hubaux and Levente Buttyán and Srdan Capkun. "***The Quest for Security in Mobile Ad Hoc Networks***". Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), year:2001..

Este artículo muestra otro enfoque sobre la seguridad en redes computacionales donde se involucran las redes celulares y las redes multi-hop. Muestra las vulnerabilidades de los mecanismos ya planteados de seguridad y unos nuevos argumentos en mecanismos para aplicar nuevas técnicas de seguridad (Tamper resistance, Routingbased mechanisms, Neighborhood and Service enforcement). Es un artículo más argumentativo pues no abarca muchos detalles técnicos.

[20] Chalermek Intanagonwiwat and Ramesh Govindan and Deborah Estrin. "***Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks.***" Mobile Computing and Networking, pages: 56-67, 2000.

Este artículo consiste en la implementación de comunicación con procesos de difusión dirigida, que tienen como propósito principal el ahorro de recursos de energía en las redes que usan sensores como lo son las redes MANET. Básicamente consiste en determinar transporte de datos apuntando intencionalmente a nodos que hacen parte de la red, para evitar el envío de paquetes por la red sin que estos sean usados. Un tema muy interesante para determinar los caminos más cortos para tal fin.

[21] Markus Jakobsson and Susanne Wetzel. "***Security weaknesses in Bluetooth***.". Lecture Notes in Computer Science Journal, volume: 2020, pages:176, 2001.

Un artículo muy pertinente que muestra los tres puntos más vulnerables del estándar de comunicación Bluetooth. Fundamentalmente son: la revelación de claves de acceso, la localización geográfica de un nodo o victima del ataque en la topología de la red wireless y un tercero que consiste en el cifrado de datos. El artículo muestra las implementaciones necesarias para combatir estos ataques,

aunque en general no muestra muchos detalles técnicos.

[22] Markus Jakobsson and Susanne Wetzel and Bülent Yener. "***Stealth Attacks on Ad-Hoc Wireless Networks***". In Proceedings of VTC, 2003.

Consiste en el estudio de los ataques que son montados en redes MANET para la manipulación de información de enrutamiento y el excesivo consumo de potencia. Se basa en artículos referenciados en esta misma bibliografía anotada pero presentan un enfoque nuevo al convertir en teoría los términos necesarios para generar protocolos de seguridad. No contiene explicaciones puntualmente técnicas.

[23] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang, "***Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks***". To appear in ICNP, 2001.

Centrado en tres razones principales: La vulnerabilidad de intrusión en las redes wireless por parte de atacantes pasivos de incursión en la red y activos de disrupción y detección de información, la demanda de los usuarios móviles para recibir una nueva generación de servicios, y las necesidades de escalabilidad para poder realizar desplazamientos a gran escala, este artículo pretende mostrar las técnicas de seguridad que pretenden lidiar con problemas muy comunes en las redes MANET.

[24] Haiyun Luo, Songwu Lu. "***Ubiquitous And Robust Authentication Services For Ad Hoc Wireless Networks***". Report TR-200030, Dept. of Computer Science, UCLA, 2000.

En este artículo se muestra un conjunto de protocolos de localización, enrutamiento y distribución de nodos para facilitar la tarea de envío de paquetes entre si, estableciendo una comunicación de constante autenticación unos respecto a otros, donde cada nodo tenga la capacidad de brindar servicios de información a cualquiera del resto de los nodos pertenecientes a una red. Lo más destacado del artículo son los argumentos teóricos para la seguridad en las redes MANET.

[25] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang. "***Self-Securing Ad Hoc Wireless Networks***". Seventh IEEE Symposium on Computers and Communications (ISCC '02). 2002.

Este artículo muestra un enfoque de colaboración entre nodos para hacer que cada uno se comporte como un identificador o detector de autenticaciones donde se construye una base propia de datos de autenticación y enrutamiento necesarios para determinar nodos intrusos pasivos, que son aquellos nodos que por error

pueden entrar a la red sin pertenecer a ella. Lo más destacado es el enfoque que se otorga a la autenticación de nodos, sin embargo no tiene muchas explicaciones técnicas auque si muchos y buenos resultados.

[26] Pietro Michiardi And Refik Molva. "***Simulation-Based Analysis Of Security Exposures In Mobile Ad Hoc Networks***". European Wireless Conference, 2002.

El artículo muestra una simulación realizada para determinar conclusiones propias a la hora de aplicar algunos protocolos de enrutamiento sugeridos en artículos anteriores. Básicamente el objetivo es demostrar que los algoritmos de seguridad cooperativa entre nodos resulta la solución más razonable para solucionar problemas de inseguridad en las redes inalámbricas móviles.

[27] Pietro Michiardi And Refik Molva. "***Ad Hoc Networks Security***". Journal of System Research, Volume 4, N1, March 2003.

Este extenso documento, muestra un detallado conjunto de argumentos teóricos para aplicar en las redes MANET sobre seguridad en las mismas. Básicamente muestra los tipos de ataques que aquejan a las redes y las soluciones que se pueden brindar para este tipo de ataques. Resulta como un documento oficial para tener a mano para aplicar alguna solución propia basada en la teoría mostrada, sin embargo la mayoría son propuestas solo para aplicar.

[28] Charles E. Perkins And Elizabeth M. Royer, "***Ad-Hoc On-Demand Distance Vector Routing***". MILCOM '97 panel on Ad Hoc Networks, Nov. 1997.

Consiste en el artículo que explica el protocolo de enrutamiento para redes Ad-Hoc más usado desde hace ya algún tiempo y que genera los mejores resultados en cuanto a enrutamiento se refiere. Este protocolo consiste en la unión de los nodos para realizar una comunicación de desplazamiento entre nodos, haciendo que cada nodo funcione como un enrutador. En cuanto a lo destacado de este artículo se puede describir el hecho de hacer parte del artículo sobre el que se realizará el tema de investigación. Es muy pertinente.

[29] Frank Stajano And Ross Anderson. "***The Resurrecting Duckling: Security Issues For Ad-Hoc wireless Networks***", 7th International Workshop Proceedings, Lecture Notes in Computer science, pages:172-194, 1999.

Es un artículo que describe los mecanismos necesarios para aplicar seguridad a nodos de gran tamaño en redes MANET y que se encuentran a grandes distancias. El propósito es mostrar un termómetro que identifique la disponibilidad de un nodo para establecer comunicación con los otros pertenecientes a la red. Todo esto basado en la constante implementación de autenticación del nodo para evitar

la intrusión.

[30] Koral Ilgun, Richard A. Kemmerer, Fellow, IEEE, And Phillip A. Porras, "***State Transition Analysis: A Rule-Based Intrusion Detection Approach***". Software Engineering journal, volume:21, number:3, pages:181-199, Year=1995.

Aunque es un artículo general sobre Detección de intrusos en computación no propiamente sobre redes MANET, y además, es un poco antiguo, presenta un enfoque muy practico sobre detección en tiempo real de intrusos. Lo que hace el enfoque presentado es realizar una implementación de un sistema experto que ubica las anomalías características de agentes y procesos malévolos dentro de una representación computacional.

[31] Seung Yi And Prasad Naldurg And Robin Kravets, "***Security-aware Ad Hoc Routing For Wireless Networks***", Proceedings of the (ACM) Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), 2001.

Este artículo describe la implementación de un protocolo de seguridad en redes MANET que involucra los distintos atributos de seguridad de enrutamiento como parámetros incluidos en la búsqueda de una ruta entre nodos. El propósito del artículo es mostrar, la relevancia que se le otorga a las aplicaciones que puedan ejecutarse sobre la red mientras el protocolo de enrutamiento SAR (Security-Aware ad hoc routing) propuesto por los autores, realiza enrutamiento seguro y efectivo a la hora de transmitir paquetes distintos a los de difusión. Lo interesante de este artículo es la clasificación de nodos que se aplica en una red Ad-Hoc como lo son privados, públicos y generales que se deben comportar como tal.

[32] Evan Sultanik, Donovan Artz, Gustave Anderson, ,Moshe Kam, ,William Regli,Max Peysakho,Jonathan Sevy,Nadya Belov,Nicholas Morizio, Andrew Mroczkwski, "***Secure Mobile Agents On Ad Hoc Wireless Networks***". Proceedings of the Fifteenth Innovative Applications of Artificial Intelligence Conference, 2003.

Este artículo muestra una nueva aplicación para establecer seguridad en redes Ad-Hoc a través de un protocolo de detección de intrusos basado en agentes móviles llamado SWAT (Secure Wireless Agent Testbed). Consiste en determinar un sofisticado método de encripción soportado sobre una comunicación segura basada en la aplicación de las distintas caspa del modelo OSI. Lo más destacado del artículo es precisamente la seguridad en redes MANET enfocada al modelo y aplicación del modelo OSI.

[33] Maxim Peysakhov, Donovan Artz, Evan Sultanik,William Regli, "***Network Awareness For Mobile Agents On Ad Hoc Networks***". AAMAS '04: Proceedings of the Third International Joint conference on Autonomous Agents and Multiagent Systems, pages: 368-376, 2004.

El enfoque de este artículo es proporcionar herramientas para la detección de intrusos en redes MANET. Lo que se propone es establecer agentes móviles que se comunican entre sí, enviando paquetes de datos de los estados de privacidad y seguridad de una red Ad-Hoc. Lo más destacado es precisamente el enfoque como tal, pues se diferencia muy bien el sistema de agentes de detección de intrusión de la capa de red para establecer las rutas de nodo origen con respecto al nodo destino y también se diferencia de la conectividad de la capa física de la red inalámbrica.

[34] Zygmunt J. Haas, Ben Liang, "***Ad Hoc Mobility Management With Uniform Quorum Systems***". IEEE\slash ACM Transactions on Networking, volume:7, number:2, pages:228-240, 1999.

El propósito de este artículo es mostrar la implementación de un esquema que determina la movilidad de los nodos de una red Ad-Hoc generando una base de datos de las ubicaciones principales de dichos nodos y crear un backbone virtual. Este esquema se denomina UQS (Uniform Quorum Systems) y predice la nueva ubicación de un nodo en movimiento para establecer una comunicación de transmisión nodo a nodo sin interrumpir los enlaces aun cuando los nodos se encuentren distantes uno del otro. Lo mas destacado de este artículo es la matemática aplicada a las redes MANET para cumplir con el objetivo de administración de la red móvil inalámbrica.

[35] Srdjan Capkun And Levente Buttyán And Jean-Pierre Hubaux, "***SECTOR: Secure Tracking Of Node Encounters In Multi-Hop Wireless Networks***". International Conference on Mobile Computing and Networking, 2003.

Este artículo muestra un conjunto de mecanismos para proporcionar la sincronización necesaria y medición del tiempo de encuentro entre los nodos de una red MANET. El propósito es evitar ataques como los "agujeros de gusanos" que pueden ser efectuados en el tiempo en que un nodo abandona la conexión con otro suplantando la conexión y realizando intrusión. La sincronización de tiempos de encuentro se realiza a través de un reloj que debe tener cada nodo para contribuir con la aplicación de tiempos de encuentro y así dar limite a la comunicación para reiniciarla cuando es abandonada por aumento en la distancia de los nodos. Lo destacado de este artículo es la explicación técnica y matemática para llegar a tal fin.

[36] Yongguang Zhang And Wenke Lee, "***Intrusion Detection In Wireless Ad-Hoc Networks***". ACM MobiCom, pages:275-283, 2001.

Este artículo consiste en un pertinente documento que describe las características que hacen a una red Ad-Hoc vulnerable para sufrir intrusión. Dentro del artículo se mencionan los distintos tipos de comportamientos que pueden llegar a tener cada uno de los nodos atacados para argumentar la posibilidad de realizar la detección de los intrusos. Comportamientos tales como anomalías en la tabla de enrutamiento de un nodo, el flujo de desvío de información por causa de mensajes de difusión que capturan las direcciones físicas MAC de los nodos pertenecientes a la red, la disrupción entre otros. Pero lo más destacado de este artículo es la propuesta de IDS (Intrusion Detection System) que se da a conocer, pues se fundamenta en crear un sistema que interprete las anomalías en la red tal que la intrusión sea eliminada reiniciando la comunicación entre los nodos que si hacen parte de la red.

[37] Marco Conti, Enrico Gregori, Giovanni Turi, "***A Cross-Layer Optimization Of Gnutella For Mobile Ad Hoc Networks***". ACM MobiCom, 2005.

Consiste en basar la optimización en los recursos usados por una red MANET en la comunicación que establecen dos equipos por la red Internet con servidores y aplicaciones P2P (peer-to-peer). Esto para establecer canales privados inalámbricos entre los nodos y evitar la comunicación con nodos disruptivos pasivos o activos. Se establece una mejora práctica al protocolo Gnutella que genera comunicación p2p, haciendo que la nueva identificación distinga entre nodos participantes de la comunicación y nodos Super-peer que son los que dan la parada en la comunicación entre nodos estableciendo un orden jerárquico de comunicación.

[38] Douglas M. Blough And Giovanni Resta And Paolo Santi, "***A Statistical Analysis Of The Long-Run Node Spatial Distribution In Mobile Ad Hoc Networks***". ACM MobiCom, 2004.

Consiste en el análisis de la distribución espacial de los nodos de una red Ad-Hoc para determinar el nivel de conectividad de una red MANET. Esto permite aplicar elementos a la red móvil tales como establecimiento de Energía y aumento de frecuencia de la señal de transmisión aplicando recursos para evitar la caída de la red. El artículo es muy completo y descriptivo.

[39] Jennifer E. Walter, Jennifer L. Welch And Nitin H. Vaidya. "***A Mutual Exclusion Algorithm For Ad Hoc Mobile Networks***", ACM MobiCom, 2001.

Este artículo consiste en una muy completa descripción técnica de un algoritmo de exclusión mutua para aumentar la capacidad de conexión entre nodos móviles que se encuentran lejanos unos de otros. Básicamente se analiza la interacción con respectivo a la ubicación y represtación espacial de los nodos de una red MANET. Esto se realiza con una cooperativa comunicación donde la transmisión de un nodo distante de otro, se comunica con el nodo más cercano que encuentre y realiza una operación de transmisión-recepción inmediata sucesiva hasta encontrar el nodo destino. Si el nodo se encuentra muy lejano la comunicación podría hacer que interfieran todos los nodos de la red. Lo más destacado de este artículo es la descripción detallado del algoritmo para realizar la exclusión en cada nodo, así como su implementación para determinar los comportamientos de movimiento de los nodos. Muy descriptivo.

[40] Yongguang Zhang, Wenke Lee, Yi-An Huang "***Intrusion Detection Techniques For Mobile Wireless Networks***". Wireless Networks, Volume 9 Issue 5, Kluwer Academic Publishers. 2003.

Este artículo habla sobre algunas técnicas de detección de intrusos ya mencionadas en el artículo "*Intrusion Detection In Wireless Ad-Hoc Networks*" [36]. Se encuentra escrito por sus mismos autores, sin embargo, muestran un enfoque más acertado al discriminar algunas técnicas de encripción como poco útiles, pues se centran en generar una base de conocimiento en la que los comportamientos de los nodos nocivos lleven a la detección de la intrusión. Aunque nombra muchas de los temas del anterior artículo, se centran por dar un enfoque más moderno a la detección de intrusos en redes Ad-Hoc.

[41] Yi-an Huang, Wenke Lee "***A Cooperative Intrusion Detection System For Ad Hoc Networks***" Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. 2003.

Este artículo describe un método mucho más acertado para realizar detección de intrusos en redes MANET. Consiste en hacer que los nodos de la red Ad-Hoc realicen periódicamente una asignación entre ellos mismos como agentes móviles de detección basando en realizar clustering e identificando cada uno la autenticación de cada uno de los nodos existentes dentro de la red. Este método hace que la manifestación de los nodos intrusos sea mucho más efectivamente, pues en trabajos anteriores de los autores se contaba con que cada nodo fuera un agente de detección, sin embargo este nuevo método es mucho más efectivo pues el intruso no podrá ser agente y será más fácil de detectar.

[42] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt. "***A Specification-Based Intrusion Detection System For Aodv***" Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks. 2003.

Basado en el protocolo de enrutamiento AODV (Ad-Hoc On-Demand Distance Vector Routing) que consiste en el protocolo de enrutamiento más aplicado a redes MANET, este artículo habla de una técnica de detección de intrusos generando un árbol jerárquico entre los nodos para realizar una autenticación que obstaculice el paso a nodos intrusos y disruptivos. Inicialmente habla de la vulnerabilidad en las redes Ad-Hoc y los principales ataques que sufren este tipo de redes y luego se centra en la técnica descrita por los autores. Aunque los argumentos son necesarios para el trabajo de investigación, es muy poca la descripción técnica del estudio.