Impacto de las Configuraciones de Seguridad y el Tipo de Tráfico en Redes WLAN 802.11

Santiago Pérez, Higinio Facchini, Luis Bisaro
GRID TICs (Grupo UTN de Investigación y Desarrollo en TICs
Facultad Regional Mendoza, Universidad Tecnológica Nacional
Rodriguez 273, Mendoza, Argentina
0261-5244576
{santiagocp, higiniofac, lbisaro}@frm.utn.edu.ar

Nora Costa
Facultad de Ingeniería
Universidad de Mendoza
Peatonal Descotte 750, Mendoza, Argentina
0261- 4201872
noraalejandracosta@gmail.com

Resumen

Las redes cableadas LAN, han concentrado mucha atención científico técnica durante lo últimos 30 años. No sucede lo mismo con la relativamente reciente introducción de las redes LAN wireless, a pesar de su despliegue en areas administrativas, comerciales e industriales. Por ello resulta cada vez más importante analizar el comportamiento de estas redes y sus prestaciones.
El tráfico total de estas redes wireless tiene una importante sobrecarga sobre el tráfico de datos real. Independientemente de la sobrecargar al sumar cualquier configuración de seguridad que se le aplique a las mismas. El conjunto puede degradar sensiblemente las prestaciones de las redes WLAN 802.11.
Se sabe, que en general, las comunicaciones wireless tienen un rendimiento real del 50 % de la tasa nominal de velocidad, muy inferior a la tasa en las comunicaciones cableadas. Sin embargo, no hay muchos trabajos y estudios que respalden dicho enunciado empirico, ni el grado de la variabilidad del mismo de acuerdo a las diversas configuraciones, tipos de tráfico, y los contextos de seguridad de los enlaces wireless.
El trabajo propone efectuar diversos estudios y análisis sobre simuladores, y complementariamente, con experimentos piloto de laboratorio, y determinar el grado de influencia en las prestaciones para cada caso.
Palabras claves: WLAN 802.11 Prestaciones Seguridad Simulación

Contexto

La línea de investigación está inserta en el proyecto PID "Análisis Cuantitativo del Impacto de las Configuraciones de Seguridad y de Tipos de Tráfico en las Redes WLAN 802.11", en el ámbito del Grupo UTN GRID TICs (Grupo UTN de Investigación y Desarrollo en TICs), del Departamento Ingeniería en Electrónica, de Facultad Regional Mendoza, de la Universidad Tecnológica Nacional, aprobado por el Consejo Directivo con resolución nº 636/2011, y en trámite de acreditación ante el Programa de Incentivos del Ministerio de Educación, Ciencia y Tecnología, desde enero/2012 hasta la fecha.

Introducción

Las grandes Redes LAN (cableadas y/o wireless) están ampliamente instaladas, y la combinación de ambas propuestas ha ganado rápidamente popularidad.

Además, una parte de lo nodos de red han conmutado a nodos wireless, y en conjunto, crecen proporcionalmente con el número de nodos, su variedad y los requerimientos de los servicios demandados.
En este escenario, la importancia de entender la conducta de los nodos wireless ha aumentado.
Hay bastantes trabajos de investigación dirigidos al objetivo general de entender la conducta de los nodos wireless de red, con focos diferentes y aplicaciones potenciales en mente.
En [1] se presentan resultados de trazas coleccionadas durante 4 semanas en un gran ambiente corporativo, con 177 access points y 1366 usuarios. En él se estudian la distribución de usuarios y carga a través de los access points. Se comparan los resultados con aquellos de estudios previos para extraer y explicar algunas características de usos de la red y la movilidad. Por ejemplo, confirmando aspectos como que la carga está desigualmente distribuida a través de los access points, e influida más por los usuarios que están presentes, que por el número de usuarios. Además, clasifican a las trazas por las duraciones de sesión, y por la frecuencia con que los usuarios visitan varias locaciones, y estableciendo que las distribuciones de probabilidad de ambas medidas siguen las leyes de potencia.
Alternativamente, algunos trabajos utilizan técnicas matemáticas avanzadas para el agrupamiento de las trazas. En [2] se analizan trazas WLAN de tres mayores campus universitarios para entender los aspectos comunes y diferentes, aplicando las técnicas de análisis de componentes principales. Los autores proponen un índice de similitud que es usado para identificar grupos de usuarios wireless con tendencias comunes.
Otro estudio de trazas interesante por su magnitud, que focaliza sobre trazas wireless coleccionadas desde campus universitarios y redes corporativas, se discute en [3]. Se obtuvieron trazas wireless desde 4 fuentes diferentes, incluyendo 12000 usuarios distintos, y más de 1300 APs. Además, se proponen métricas par describir las conductas individuales, y se encontraron hechos significativos, como por ejemplo, que los modelos de movilidad convencionales, aleatorios, generados sintéticamente, no son adecuados para un ambiente heterogéneo, tal como un campus de universidad y corporaciones.
Así, en los trabajos mencionados precedentemente, y en otros [4], [5], [6], [7], [8] se han propuesto diversas definiciones de métricas para entender la conducta individual o grupal del nodo: a) Actividad online de los usuarios, b) Movilidad de largo plazo de los usuarios, c) Movilidad de corto plazo de los usuarios, d) Patrón de asociación repetitivos de los usuarios, ó Patrón de asociación de grupo, e) Tráfico de los usuarios, f) Prevalencia de APs, g) Persistencia de APs, etc.
Y afortunadamente, buena parte de los investigadores y analistas de tráfico de red wireless, dejan disponibles para otros trabajos, sus bases de datos de trazas, ó las reúnen en depósitos comunitarios. Tal es el caso del proyecto CRAWDAD (Community Resource for Archiving Wireless Data at Dartmouth) [9], que actualmente utilizan más de 320 Universidades del mundo.
Por otro lado, en [10] se presenta una modelo de EDCA 802.11e, usando las Redes de Petri como herramienta matemática, para obtener las prestaciones y tiempos medios para varias configuraciones, en aplicaciones de tiempo real.
Y en [11], se plantean las consecuencias negativas en las redes WLAN ad hoc, sobre la capacidad de la misma, debido a los requerimientos de transmisión de paquetes entre los nodos. Y muestran las dificultades de una red ad hoc, bajo ciertos patrones de tráfico, para escalar a grandes redes.
Además, hay muchos trabajos relacionados con el tema de Seguridad Informática, dedicados en forma general o específicos a algunos de los puntos señalados anteriormente. En [12] se estudia y emite un manual básico de Auditoría, Evaluación, Test de Seguridad en una metodología abierta que puede servir como guía gratuita a tomar como referencia para cualquier profesional de

Sistemas que debe hacer o contratar este tipo de trabajo; es decir realizar una auditoría de seguridad en la red informática, correr distintos tests de seguridad y evaluar los posibles riesgos y prestaciones, para luego implementar (o actualizar) una política de seguridad.
En [13], se realiza un informe sobre Recomendaciones Generales de Seguridad a implementar en una organización, considerando aspectos sobre seguridad a nivel de red, a nivel de sistemas, recomendaciones para usuarios finales e información de seguridad sobre Internet.
En [14], se realiza una revisión de seguridad en redes inalámbricas, considerando los estándares de la IEEE 802.11 y 802.16 y las amenazas posibles.

Escenarios Experimentales de Simulación

Para el desarrollo de las simulaciones se utilizará un modelo de nodo wireless 802.11e [10] implementado usando la herramienta Möbius [15], de la Universidad de Illionois, que soporta una extensión de Redes de Petri Estocásticas (SPN), referidas como Redes de Actividad Estocástica (Stochastic Activity Networks - SANs). Ellas proveen una aproximación de modelación jerárquica que se combina con soluciones analíticas de estado del arte y simulación. El formalismo de modelación es completamente similar a las Redes de Petri Estocásticas clásicas con cuatro objetos primitivos: lugares, actividades, compuertas de entrada (input gates) y compuertas de salida (output gates). Las interacciones (flujo de datos) entre estos objetos se describen por medio de arcos.
Además, y desde el punto de vista de la modelación, el modelo también exhibe una importante flexibilidad en los siguientes aspectos:
- Facilidad para incluir modificaciones o refinamientos. El modelo fue construido de forma modular, con cada módulo implementando una funcionalidad específica. Por lo tanto, su topología ayuda a localizar los módulos donde las modificaciones o refinamientos deberían incluirse,
- Pueden obtenerse un gran número de medidas de performance de diferentes tipos, desde el mismo modelo sin modificaciones estructurales,
- El modelo puede ser usado como una estructura base para construir modelos más complejos y de más alto nivel

Una ventaja importante, para evitar el proceso de construir un modelo de red para cada uno de los escenarios de simulación, es que el modelo adoptado representa una simple estación que soporta QoS. Este modelo es luego replicado, para obtener el escenario de simulación requerido. El numero de replicas se parametriza por el usuario y está totalmente automatizado por la herramienta de modelación Möbius. Esto provee una importante flexibilidad en el proceso de evaluación, con la aceleración en el análisis de diferentes escenarios de red. Por ejemplo, en la evaluación de escenarios compuestos por un numero de estaciones crecientes, o variando su proporción relativa, con tráfico diverso, tal como se aspira en la presente proyecto.
Todas las simulaciones experimentales se obtendrán usando el modelo de simulación EDCA, previamente descripto, y con un intervalo de confianza del 95% y una precisión del 5 %.
Las métricas de performance a analizar son: rendimiento absoluto, rendimiento relativo, pérdida de paquetes, retardo de cola promedio y tamaño de cola promedio.

Escenarios Experimentales de Laboratorio

Para el desarrollo de los laboratorios pilotos a implementar para el proyecto, se utilizará equipamiento, software de generacion y analisis de trafico, de los Labs del GRID TICs del Departamento de Electrónica, la UTN Regional Mendoza, a saber:
- AIRPCAP NX: USB 802.11 a/b/g/n Adapter (capture + injection)
- AP CISCO 4410N
- Placas USB Wireless Linksys WUSB600N

- Placas USB Wireless Kozumi K300MWUN
- Placas Routerboard Mikrotik RB433AH
- Placas MiniPCI Wireless Mikrotik R52N
- Wireless Access Point Sp918gk Micronet
- Switch KVM 4 port Trendnet TK-400K
- IP Traffic Test & Measure

En función de estos recursos, se deberán establecer las características de los laboratorios de testing piloto, que incluyan por un lado, los casos de tráfico de enlaces punto a punto, y por otro, los casos de tráfico entre clientes conectados a un AP; ó que resulten de la combinación de estos tipos de configuraciones.

Ademas, con el generador generador de tráfico IP Traffic seleccionado se deberá también recibir, capturar y retransmitir tráfico IP, y medir la performance end-to-end y la QoS sobre la red piloto inalámbrica. Además, se deberá administrar conexiones simultáneas, permitir la selección del ancho de banda, tipo de tráfico (TCP ó UDP, IPv4 ó IPv6), la longitud de los paquetes, etc. y la simulación de ambientes normales y congestionados.

Resultados y Objetivos

El objetivo general es:

Demostrar el grado en que los diversos esquemas de seguridad y tipos de tráfico en Redes WLAN 802.11 generan un impacto diferenciado en las prestaciones del tráfico de datos efectivo.

Los objetivos específicos son:

1) Calcular el efecto cuantitativo y cualitativo sobre las redes WLAN 802.11, de los esquemas de seguridad y tipos de tráfico usando, generadores y/o simuladores de tráfico.

2) Establecer si hay diferencias estadísticas significativas en el estado global de la red WLAN, al cambiar la proporción y diversidad relativa de dispositivos en la red.

3) Comparar cuantitativamente los comportamientos de la red cuando se encuentra o no en estado de saturación

Tareas:

Adicionalmente, se pretende:.

- Identificar las clases o tipos de procedimiento de autenticación, ordenados según su fiabilidad y complejidad, utilizados en los estándares WLAN 802.11
- Identificar las clases o tipos de técnicas de encriptación, ordenados según fiabilidad y complejidad, utilizados en los estándares WLAN 802.11.
- Establecer las características de los laboratorios de testing piloto con uso de simuladores y equipamiento real, que incluyan, por un lado, los casos de tráfico de enlaces punto a punto, y por otro, los casos de tráfico entre clientes conectados a un AP; ó que resulten de la combinación de estos tipos de configuraciones.
- Construir tablas comparativas de las prestaciones para cada caso, según las combinaciones de procedimientos de autenticación, técnicas de encriptación, tamaños de contraseñas, tipo de tráfico (TCP ó UDP, IPv4 ó IPv6), tamaño de paquetes, etc, para cada laboratorio de testing piloto.
- Enunciar y establecer conclusiones de las mejores prácticas sugeridas para cada contexto según la fiabilidad y prestaciones deseadas, considerando:

a) La interacción entre las diferentes capas de seguridad y sus efectos sobre las prestaciones; específicamente, tiempo de respuesta y rendimiento, cuando la red no está congestionado o saturada.

b) Los mismos ensayos anteriores pero cuando la red está congestionada. y

c) El grado de variabilidad ó degradación de las prestaciones:

1. En concordancia con la mejora de la calidad de seguridad deseada,
2. Cuando el número de cliente se incrementa, por ejemplo, debido a los efectos de las colisiones y backoffs,
3. Cuando se utiliza tráfico TCP ó UDP , observando, por ejemplo, los mecanismos de control de congestión de TCP, ó la cantidad de paquetes pérdidos de UDP,
4. Cuando se varía el tamaño de los paquetes

Líneas de investigación y desarrollo

El proyecto está direccionado hacia el Análisis de Tráfico de Red, como eje temático. El énfasis es en el análisis del

comportamiento de las redes Ethernet y Wireless 802.11, para favorecer la mayor exactitud posible en los modelos de simulación de tráfico de red. Los autores experimentan actualmente diversas versiones y escenarios posibles de un modelo de nodo Wireless 802.11e sobre el simulador Möbius, y configuraciones de laboratorio con uso de un generador y analizador de trafico.

Formación de Recursos Humanos

El equipo de trabajo está integrado por docentes investigadores, y becarios graduados y alumnos del Grupo GRID TICs (Grupo UTN de Investigación y Desarrollo en TICs) de la Universidad Tecnológica Nacional, Facultad Regional Mendoza. Entre los integrantes, hay en curso un tesis doctoral, una de magister y una de grado, relacionadas con la línea general de investigación.

Referencias

[1] Balazinska, M. y Castro, P., (2001), Charactirizing Mobility and Network Usage in a Corporate Wireless Local Area Network, Laboratorio para la Ciencia de la Computación MIT, Centro IBM de Investigación Watson.
[2] Hsu, W. y Helmy, A., (2003), Principal Component Analysis of User Association Patterns in Wireless LAN Trace. Department of Electrical Engineering, University of Southern California.
[3] Hsu, W. y Helmy, A., (2004), On Modeling User Associations in Wireless LAN Traces on University Campuses, Department of Electrical Engineering, University of Southern California.
[4] Hsu, W. y Helmy, A., (2006), On Nodal Encounter Patterns in Wireless LAN Traces, Second International Workshop On Wireless Network Measurement.
[5]. Taduce, C. y Gross, T., (2003), A Mobility Model Based on WLAN Traces and its Validation, Proceedings of IEEE INFOCOM.
[6] Papadopouli, M., Shen, H. y Spankis, M., (2005), Characterizing the Duration and Association Patterns of Wireless Access in a Campus, 11º European Wireless Conferences 2005, Nicosia, Cyprus.
[7] Henderson, T. y Kotz, D., (2004), The Changing Usage of a Mature Campus-wide, Proceedings of ACM MobiCom 2004.
[8] Meng, X., Wong, S., Yuan Y. y Lu, S., (2004), Characterizing Flows in Large Data Networks, Proceedings of ACM MobiCom.
[9] CRAWDAD project
http://au.crawdad.org/
[10] Wireless Real-Time Communication for Industrial Environments using the IEEE 802.11e Communication protocol
http://paginas.fe.up.pt/~vasques/ieee80211e/
[11] Jinyang, L, Blake, C., Douglas, S. Lee, H. y Morris, R., Capacity of Ad Hoc Wireless Networks, M.I.T. Laboratory for Computer Sience.
[12] Alejandro Corletti Estrada , 2005, Auditoría, Evaluación, Test de Seguridad - metodología abierta OSSTMM, Universidad Politécnica de Madrid.
[13] Chelo Malagón Poyato, Francisco Monserrat Coll, David Martinez Moreno, 2000, Recomendaciones de Seguridad, Red IRIS, España
[14] Abdel-Karim R. Al Tamimi, 2006, Security in Wireless Data Networks : A Survey Paper, Washington University in St.Louis
[15] https://www.mobius.illinois.edu