Escuela Politécnica Superior
Departamento de Tecnología Electrónica y de las Comunicaciones

CONTRIBUCIÓN AL ANÁLISIS DEL TRÁFICO DE INTERNET

TESIS DOCTORAL

Antonio Cuadra Sánchez

Madrid, Abril de 2017

TESIS DOCTORAL: Contribución al análisis del tráfico de Internet

AUTOR: Antonio Cuadra Sánchez

DIRECTOR: Prof. Dr. Javier Aracil Rico

El comité para la defensa de la presente tesis doctoral está compuesto por:

PRESIDENTE: Prof. Dr. Sergio López Buedo

MIEMBROS: Vocal 1: Prof. Dr. Eduardo Magaña Lizarrondo

Vocal 2: Prof. Dr. Carlos García Rubio

Vocal 3: Prof. Dr. Daniel Morató Osés

Suplente 1: Prof. Dr. Luis Sánchez Fernández

Suplente 2: Prof. Dr. Narciso García Santos

SECRETARIO: Prof. Dr. Jorge Enrique López de Vergara Méndez

Esta tesis se presenta como un compendio de aplicaciones cumpliendo con los requisitos artículo 8 del "Procedimiento relativo al tribunal, defensa y evaluación de la tesis doctoral en la Universidad Autónoma de Madrid", aprobado por Consejo de Gobierno de 1 de junio de 2012 y modificado por Consejo de Gobierno de 6 de febrero de 2015, por Consejo de Gobierno de 24 de abril de 2015, por Consejo de Gobierno de 16 de julio de 2015, y por Consejo de Gobierno de 11 de diciembre de 2015:

Articulo 8.- Tesis presentadas como un compendio de publicaciones.

8.1 El doctorando, con la autorización expresa del director/es de la tesis y de la Comisión académica responsable del programa de doctorado, puede optar por presentar la tesis doctoral como un compendio de publicaciones. Para ello se requiere que tenga publicados o admitidos para su publicación un mínimo de 3 contribuciones que deberán ser artículos en revistas científicas de reconocido prestigio o en libros editados de importancia justificada, o monografías publicadas por editoriales de relevancia.

La fecha de las publicaciones debe ser posterior a la aprobación de su proyecto de tesis doctoral/Plan de Investigación y anterior a la presentación de la tesis.

8.2 En este caso, el ejemplar de la tesis ha de cumplir los siguientes requisitos:

a) Incluir una introducción general que presente los trabajos compendiados, que justifique la temática y que explique la aportación original del autor.

b) Incluir un resumen global de los resultados obtenidos, de la discusión de estos resultados y de las conclusiones finales.

c) Se ha de incluir en un anexo una copia completa de los trabajos publicados o admitidos para su publicación, haciendo constar el nombre de todos los coautores de los trabajos y la referencia completa de la revista en que los trabajos estén publicados o admitidos para su publicación.

Agradecimientos

A mi familia: a los que se han ido y a los que han llegado mientras preparaba mi tesis: Rosa Mari, Antonio y Alejandro; y Susana, Valvanuz, Yurde y Maribel.

Y por supuesto, a mi director de tesis, Javier, por todo.

Mil gracias.

Resumen

En esta tesis se ha desarrollado una serie de técnicas avanzadas de análisis de tráfico que cubren nuevas necesidades en el ámbito de la monitorización de redes y servicios. Las técnicas tradicionales se basan en el mero análisis de los protocolos y su evolución en el tiempo, en lugar considerar los perfiles y las características del tráfico como se propone en esta tesis, lo que posibilita su aplicación a distintas disciplinas, como la detección de anomalías en la red, la supervisión de la calidad o la gestión de la seguridad. Se ha desarrollado una metodología novedosa para analizar el tráfico denominada "análisis del perfil de día típico", que permite caracterizar el comportamiento del tráfico para los diferentes periodos del día. Además, se ha desarrollado un algoritmo que analiza desviaciones de tráfico con respecto al comportamiento normal, utilizando de manera combinada las principales técnicas estadísticas para determinar posibles anomalías en la red en función del periodo del día, detectar eventos inesperados que surjan en la red, y descartar falsos comportamientos que podrían parecer anómalos, con mayor precisión que utilizando una sola técnica. Esta metodología se ha aplicado con éxito al campo de la seguridad contextual para detectar posibles ataques, y a entornos SDN (Software-Defined Networks), utilizando un año completo de tráfico de 2000 hogares de Suecia. Finalmente, se ha desarrollado una técnica inédita para detectar llamadas de VoIP (Voz sobre IP) en WhatsApp, ya que las técnicas tradicionales no pueden aplicarse porque el tráfico está ofuscado. Esta técnica analiza la sostenibilidad del tráfico en el tiempo para discernir llamadas de voz de otros servicios dentro de una misma sesión de WhatsApp. Los resultados indican que los algoritmos desarrollados detectan correctamente los distintos escenarios planteados, sin dar lugar a falsos positivos ni falsos negativos. Como resultado de esta tesis, se han publicado 5 contribuciones en revistas (mas otra en revisión), un libro y una conferencia de referencia.

Esta tesis se presenta como un compendio de aplicaciones cumpliendo con los requisitos artículo 8 del "Procedimiento relativo al tribunal, defensa y evaluación de la tesis doctoral en la Universidad Autónoma de Madrid", aprobado por Consejo de Gobierno de 1 de junio de 2012 y modificado por Consejo de Gobierno de 6 de febrero de 2015, por Consejo de Gobierno de 24 de abril de 2015, por Consejo de Gobierno de 16 de julio de 2015, y por Consejo de Gobierno de 11 de diciembre de 2015.

La presente tesis se ha realizado mientras el doctorando estaba empleado a tiempo completo en la empresa Indra Sistemas, S.A.

Glosario

CUSUM	Cumulative Sum
DDoS	Distributed Denial of Service
DoS	Denial of Service
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
χ^2	Test de bondad de ajuste χ^2 (Ji cuadrado) de Pearson
K-S	Test de bondad de ajuste de Kolmogorov-Smirnov
Kbps	Kilobits por segundo
MI	Mutual Information
OTT	Over-the-top
QoS	Quality of Service
QoE	Quality of Experience
SDN	Software-Defined Networks
SYN	Bit de control del segmento TCP para sincronizar una conexión
TADI	Traffic Anomaly Detection Indicator
TCP	Transmission Control Protocol
TIC	Tecnologías de la Información y Comunicación
VoIP	Voice over IP

INDICE DE CONTENIDOS

1 Introducción general

En este capítulo se introducen los trabajos compendiados, incluyendo la justificación de la temática con respecto a la tesis, y explicando la aportación original del doctorando. Para ello, se incluyen secciones explícitas que exponen la aportación original del autor para cada una de las publicaciones incluidas en el capítulo "3.- Copia completa de los trabajos publicados".

En la tesis doctoral "Contribución al análisis del tráfico de internet" se han abordado las nuevas necesidades de monitorización de redes y servicios de siguiente generación, que están originando el desarrollo de técnicas avanzadas de análisis de tráfico de redes IP. Las técnicas tradicionales de monitorización de redes y servicios se basan en el mero procesamiento de protocolos en lugar considerar los perfiles y características de tráfico. Las técnicas avanzadas de análisis de tráfico permitirán gestionar la red y los servicios de manera más exhaustiva, haciendo posible extender su ámbito de aplicación a otras disciplinas, como la detección de anomalías en la red, la supervisión de la calidad o la gestión de la seguridad. Se ha realizado un estudio exhaustivo de las principales técnicas de análisis de tráfico de Internet con el fin de realizar investigaciones que evidencien el comportamiento de Internet y el uso que de él hacen los usuarios, que posibilitarán desarrollar análisis de tendencias más fiables. Los estudios del tráfico son una fuente de información fundamental para conocer no sólo el estado actual, sino una evolución del tráfico de Internet.

Con todo, se ha ahondado en el estudio de las técnicas actuales de análisis de tráfico en Internet, y se ha concluido que esta línea de investigación no ha sido suficientemente cubierta por el estado del arte. Las técnicas actuales se basan en observar el tráfico de manera longitudinal en el tiempo, esto es, su evolución temporal sin considerar las características propias de los diferentes periodos a lo largo del día. Por ello, en esta tesis se ha desarrollado una nueva metodología denominada "análisis del perfil de día típico" o "typical day profile analysis", que permite analizar el comportamiento del tráfico a lo largo de las 24 horas del día, y cuya principal ventaja es caracterizar el tráfico para los diferentes periodos concreto del día. De esta forma, para determinar las características del tráfico, se analizan los mismos periodos a lo largo del día (por ejemplo horas) para la serie completa de los días. Es decir, para cada periodo del día, se considera la contribución de todos los días de la muestra, de

manera que puede obtenerse un perfil de día típico que refleje el comportamiento habitual del tráfico, que puede servir de indicio, por ejemplo, para detectar comportamientos anómalos de tráfico. Dado que el consumo de tráfico varía a lo largo del día, pueden establecerse periodos bien definidos dentro del perfil de día típico, como por ejemplo perfiles diurnos, nocturnos, horario de oficina, hora cargada o distinción con respecto a fines de semana.

En este sentido, las técnicas actuales para detectar anomalías de tráfico utilizan la teoría de detección de puntos cambiantes o "change point detection" que permiten identificar cambios abruptos de tráfico, pero no tienen en cuenta el comportamiento de tráfico habitual. En esta tesis se ha propuesto utilizar la técnica de análisis del perfil del día típico mencionada anteriormente para detectar situaciones cambiantes en la red. Como resultado, se ha desarrollado una nueva metodología de análisis de tráfico para la detección de anomalías en Internet y otras redes de comunicaciones, denominada "análisis de desviaciones de tráfico con respecto al comportamiento normal" o "traffic baseline deviation analysis", que utiliza simultáneamente diferentes técnicas estadísticas, y que se basa en analizar la desviación del comportamiento de tráfico con respecto al perfil de día típico, en lugar de detectar picos repentinos de tráfico.

Con ello no sólo se consigue determinar posibles anomalías en la red en función del periodo del día, sino también detectar eventos inesperados que surjan en la red, como aplicaciones emergentes de internet que respondan a variaciones con respecto al comportamiento habitual. También permite descartar comportamientos que a priori puedan parecer anómalos, pero que sin embargo no lo son: un pico de tráfico puede suceder periódicamente en determinado instante del día, pero no implica que pueda considerarse como anómalo. Además, la metodología desarrollada utiliza por vez primera diferentes técnicas estadísticas de manera combinada, que obtiene como resultado un algoritmo que proporciona resultados más precisos. Las técnicas consideradas son tres: tests de bondad de ajuste (χ^2 de Pearson y Kolmogorov-Smirnov), gráficas de control (suma cumulativa) y basados en la entropía (información mutua).

El algoritmo resultado de esta metodología fue aplicado con éxito a varias semanas de tráfico capturado en un campus universitario. Los resultados preliminares se publicaron por primera vez en [cuadra2014], y posteriormente se elaboró una versión extendida como artículo invitado para una edición especial de un journal [cuadra2015a]. Como resultado de

este trabajo se ha editado un libro monográfico sobre detección de anomalías de tráfico publicado por la editorial Elsevier [cuadra2015b]. Las principales conclusiones han sido que el algoritmo desarrollado proporciona mejores resultados que una única técnica, y que además permite detectar anomalías de tráfico asociadas al periodo del día en el que ocurran. En función del perfil de tráfico, se determina qué combinación de técnicas estadísticas es la más idónea, y qué umbrales son los que determinan que puede existir una anomalía en un instante concreto del día.

En **[cuadra2014]** se presenta por primera vez la propuesta de una nueva técnica de análisis de tráfico basada en la teoría de la información, denominada análisis de perfil de día típico, y su aplicación a la detección de anomalías.

[cuadra2014] Cuadra-Sánchez, Antonio, Javier Aracil, and Javier Ramos de Santiago. "Proposal of a new information-theory based technique and analysis of traffic anomaly detection." IEEE International Conference on Smart Communications in Network Technologies (SaCoNeT), 2014.

- Justificación: La teoría de la detección de cambios se utiliza para identificar cambios abruptos en el tráfico de la red. La literatura se ha centrado en el análisis del tráfico longitudinal, es decir, detectar cambios bruscos de pico, en lugar de analizar el patrón de tráfico en un día típico de 24h. Dado que el tráfico varía a lo largo del día, es esencial considerar el período de tráfico concreto en el que se produce la anomalía, algo que no es posible con las técnicas tradicionales de detección de cambios repentinos.

- Aportación original: En este trabajo se presenta esta nueva técnica para la detección de anomalías, y se analiza cómo se comportan los diferentes métodos considerados en la detección de puntos de cambio dentro del perfil de día típico. Concluimos que una combinación de métodos proporciona mejores resultados que el uso de uno solo. En los períodos de bajo tráfico, las pruebas de bondad de ajuste detectan mejor las condiciones cambiantes, mientras que en los períodos normales de tráfico (durante el día) los métodos basados en entropía detectan mejor los aumentos de tráfico. Además, las gráficas de control estadístico complementan a ambas al detectar cambios muy abruptos sin importar la carga de tráfico. Ningún autor hasta la fecha ha propuesto detectar puntos cambiantes

dentro de un típico patrón de tráfico diario, lo que constituye una innovadora técnica basada en la teoría de la información.

En **[cuadra2015a]** se desarrolló una versión extendida del artículo anterior como paper invitado para una edición especial del International Journal of Parallel, Emergent and Distributed Systems sobre Smart Communications in Network Technologies.

[cuadra2015a] Cuadra-Sanchez, A., Aracil, J., & Ramos de Santiago, J. "Proposal of a new information theory-based technique based on traffic anomaly detection analysis". International Journal of Parallel, Emergent and Distributed Systems, 30(6), 464-477. doi:10.1080/17445760.2015.1044002 (2015).

- Justificación: Se trata de una versión extendida de [cuadra2014], en la que se amplían las diferentes secciones del artículo: se extienden considerablemente las referencias del estado del arte, se detalla el análisis del perfil de día típico, se desarrollan las conclusiones, y se anexan las técnicas estadísticas utilizadas en el algoritmo desarrollado.

- Aportación original: En este artículo se ha realizado un análisis exhaustivo de los trabajos y técnicas empleadas para la detección de anomalías, y se ha detallado el perfil de tráfico de todos los días monitorizados. Por otro lado, se ha realizado una clasificación de las técnicas estadísticas óptimas en función del tipo de problema y su anomalía asociada. Se establece que las variaciones repentinas de tráfico están asociadas a cambios abruptos, y la metodología de suma acumulativa (CUSUM) las detecta con mayor precisión. Los descensos de tráfico están determinadas por una caída en el tráfico que detecta el test χ^2 de Pearson. Los incrementos de tráfico son detectados por el método de Información mutua con mayor precisión para periodos de poco tráfico, y por el test χ^2 de Pearson en periodos de mucho tráfico.

En **[cuadra2015b]** se publica un libro monográfico sobre detección de anomalías de tráfico publicado por la editorial Elsevier titulado "Introduction to Traffic Anomaly Detection Methods", cuyo principal editor y contribuidor a todos los capítulos es el doctorando.

[cuadra2015b] Cuadra-Sanchez, Antonio, and Javier Aracil. "Traffic Anomaly Detection". Elsevier, 2015. ISBN 978-1-78548-012-6 http://store.elsevier.com/Traffic-Anomaly-Detection/Antonio-CuadraS%C3%A1nchez/isbn-9781785480126/

- Justificación: Se ha editado un libro monográfico sobre los métodos para la detección de anomalías de tráfico tomando como base las publicaciones anteriores [cuadra2014] [cuadra2015a], en el que se ha descrito con rigor científico las diferentes técnicas estadísticas empleadas, se ha desarrollado en detalle la metodología utilizada, y se han expuesto minuciosamente los resultados obtenidos.

- Aportación original: En este libro constituye un monográfico de referencia para la detección de anomalías, del que se ha publicado una crítica favorable en el en el Journal Network Security, Volume 2016, Issue 6[1], que concluye con la frase: "Está destinado a ser de interés para los desarrolladores de soluciones de seguridad". En primer lugar, se han detallado las diferentes técnicas de detección de anomalías: tests de bondad de ajuste (χ^2 de Pearson y Kolmogorov-Smirnov), gráficas de control (suma cumulativa) y basadas en la entropía (información mutua). También se ha detallado la técnica empleada para determinar el periodo óptimo de agregación, que es la base de la metodología que permite llevar a cabo un análisis de perfil de día típico. Además, se ha realizado un análisis comparativo de los resultados obtenidos a partir de los métodos estadísticos de detección de anomalías, y su aplicación al perfil de tráfico de día típico.

Por otro lado, esta metodología se ha aplicado también al campo de la seguridad contextual. A partir del algoritmo desarrollado para la detección de anomalías basado en el perfil de día típico, se ha implementado un indicador denominado TADI (Traffic Anomaly Detection Indicator) que permite identificar posibles brechas en la seguridad [cuadra2016]. En primer lugar, se analiza el historial de tráfico para determinar el comportamiento normal del tráfico, y se establece qué combinación de técnicas estadísticas proporciona mejores resultados para cada periodo del día. A partir de la información contextual (periodo del día y perfil del tráfico) se calcula el TADI como indicación de un posible ataque o brecha de la seguridad. Los ataques pueden suceder en cualquier momento del día, y conocer qué

[1] http://www.sciencedirect.com/science/article/pii/S1353485816300551

combinación de técnicas es la más precisa dependiendo del momento del día constituye una mayor ventaja frente a los actuales métodos, que no consideran el perfil de día típico como contexto.

[cuadra2016] Cuadra-Sanchez, A. & Aracil, J. "Context-aware security framework based on Traffic Anomaly Detection Indicator". Journal of Telecommunication Systems, ISSN: 1018-4864, doi:10.1007/s11235-016-0233-8 (2016).

- Justificación: La seguridad contextual es una nueva tendencia que tiene en cuenta información adicional para enriquecer los criterios de seguridad. Esta información complementaria (contexto) se utiliza para mejorar las decisiones de seguridad, y se compone de datos heterogéneos, como el tiempo, ubicación, condiciones de tráfico, información del usuario, etc. Diferentes expertos tecnológicos defienden que la próxima generación de seguridad de las TIC se basará en el contexto, y consideran que las infraestructuras de seguridad deben ser lo suficientemente flexibles y adaptables como para permitir incorporar información de contexto cada vez que se tome una decisión de seguridad. Por otro lado, los sistemas de detección de anomalías de tráfico son capaces de identificar situaciones anormales que pueden constituir amenazas o intrusiones en la red y, por lo tanto, son las principales fuentes de datos de tráfico de red de los sistemas de gestión de seguridad.

- Aportación original: En este artículo presentamos un marco de seguridad basado en el contexto que utiliza un Indicador de Detección de Anomalías de Tráfico (TADI) que indica cuándo puede ocurrir una amenaza. La principal novedad de nuestro enfoque es que utilizamos como contexto la información basada en el tiempo derivada del análisis de perfil de un día típico para determinar con mayor precisión la presencia de una anomalía en función del momento del día en que se produce. Este análisis de las 24 horas de un día típico nos ayuda a considerar el intervalo de tiempo (nocturno, horas de trabajo, etc.) en el que se produce una amenaza potencial, en contraposición con las técnicas tradicionales de detección de cambios bruscos de tráfico. En primer lugar, un análisis preliminar basado en datos históricos muestra cómo se comporta el tráfico típicamente en cada período particular del día. Posteriormente, calibramos nuestro procedimiento comprobando la efectividad de diferentes métodos para determinar cuáles son los

que proporcionan mayor precisión en cada período del día. Finalmente, el TADI se calcula a partir de la información contextual basada en el tiempo. También presentamos los resultados basados en trazas reales de tráfico recogidas en una universidad, que muestran la efectividad del método propuesto. Hemos evaluado el Indicador de Detección de Anomalías de Tráfico (TADI) utilizando 8 semanas de tráfico, a las que hemos añadido tráfico contaminado para simular amenazas (inundaciones y ausencia de tráfico) en tres intervalos de tiempo específicos: poco tráfico (4AM, noche), hora cargada (12AM, mediodía) y tráfico medio (5PM, tarde). Los resultados muestran que nuestro TADI detecta correctamente los diferentes periodos con tráfico asociados a potenciales amenazas.

Además, se ha verificado la aplicabilidad del algoritmo desarrollado para la detección de anomalías en entornos SDN (Software-Defined Networks), utilizando un año completo de tráfico de 2000 hogares de Suecia. Se ha propuesto aprovechar las capacidades adicionales de procesamiento de la tecnología SDN para incorporar en ellas el algoritmo desarrollado en esta tesis. Los resultados obtenidos anteriormente son completamente extrapolables a este tráfico, y aunque el perfil de día típico es diferente, la metodología empleada permite ajustar los parámetros del modelo en base a nuevos umbrales ajustados en función de toda la muestra de tráfico. En concreto, el algoritmo desarrollado ha sido capaz de detectar diversas situaciones anómalas reales que sucedieron en la muestra de tráfico, sin dar lugar a falsos positivos ni falsos negativos. Los resultados se han enviado a una edición especial del Communications Magazine sobre avances en la cadena de servicios de red **[cuadra2017b]**, y se está a la espera de la aceptación. El feedback preliminar por parte del editor ha sido bueno.

[cuadra2017b] Cuadra-Sanchez, A. & Aracil, J. "Detecting traffic anomalies at the SDN edge: a case of one-year traffic sample in Sweden". Submitted to IEEE Communications Magazine, Special Issue on Advances in Network Services Chain (January 2017), en revisión.

- Justificación: En este artículo presentamos un caso de uso del análisis de desviaciones de la línea base del tráfico que se basa en la nueva técnica que hemos desarrollado anteriormente en [cuadra2014], [cuadra2015a] y [cuadra2015b], aplicado en este caso a tecnologías SDN utilizando el tráfico de Internet de un año en Suecia. Nuestra técnica se basa en analizar los patrones de tráfico en un

día típico de 24h para tener en cuenta el período de tiempo en el que se produce una anomalía de tráfico (cualquier cambio significativo del comportamiento normal del tráfico), en contraste con las técnicas tradicionales de cambios repentinos (análisis longitudinal del tráfico). Nuestra metodología se basa en analizar desviaciones de la línea de base, y utiliza un conjunto de algoritmos que se basan en diferentes modelos estadísticos. Estos algoritmos se combinan eficientemente para determinar si ha ocurrido una anomalía.

- Aportación original: Con el fin de validar nuestro enfoque, en este artículo presentamos un caso de uso con el tráfico de todo el año 2015 en el extremo SDN, procedente de 2.000 hogares en Suecia. Los resultados son muy convincentes ya que nuestra técnica ha sido capaz de detectar todas las anomalías reales que ocurrieron durante el período de observación.

Finalmente, dentro de esta tesis se ha desarrollado una técnica inédita para detectar llamadas de voz sobre IP (VoIP) en WhatsApp a partir del análisis del tráfico **[cuadra2017a]**. Dado que las técnicas tradicionales de detección de VoIP no pueden aplicarse a las llamadas de WhatsApp porque el tráfico está ofuscado, es necesario desarrollar nuevas técnicas de análisis que consideren otros parámetros del tráfico, en lugar de intentar desencriptarlo y descodificarlo. La técnica desarrollada analiza las características estadísticas del tráfico para discernir llamadas de VoIP dentro de las sesiones de WhatsApp, lo que se ha denominado "análisis ciego de tráfico". En primer lugar, se discrimina el tráfico de WhatsApp del resto de tráfico, y posteriormente se analizan determinados parámetros del tráfico (como el nivel de transporte empleado) para distinguir si ha existido una llamada, y diferenciar el tráfico propio de voz del de la señalización de las llamadas analizando su sostenibilidad en el tiempo. Se analizaron más de 100 sesiones reales de WhatsApp en diferentes entornos, incluyendo simultáneamente llamadas e intercambio de contenidos multimedia entre lugares remotos, y utilizando una veintena de terminales móviles distintos con diferentes sistemas operativos y versiones de WhatsApp. En todos los casos se detectó correctamente cuándo había ocurrido una llamada de VoIP dentro de una sesión de WhatsApp, no dando como lugar ni falsos positivos ni falsos negativos.

[cuadra2017a] Cuadra-Sanchez A, & Aracil J. "A novel blind traffic analysis technique for detection of WhatsApp VoIP calls", International Journal of Network Management (2017), 1968. https://doi.org/10.1002/nem.1968

- Justificación: Hoy en día las redes sociales desempeñan un papel clave en la comunicación interpersonal. Las aplicaciones de mensajería instantánea, como WhatsApp, son utilizadas a diario por miles de millones de usuarios. Esta aplicación se ha actualizado recientemente para soportar llamadas de voz, cuyo tráfico se transporta por encima (OTT, Over-the-top) de los operadores de red, como muchos otros servicios de Voz sobre IP (VoIP). Sin embargo, las técnicas tradicionales de detección de VoIP no pueden aplicarse a las llamadas de WhatsApp porque el tráfico está ofuscado, y es necesario desarrollar nuevas técnicas de análisis que consideren otros parámetros del tráfico.

- Aportación original: En este trabajo hemos caracterizado las llamadas de voz de WhatsApp mediante la detección ciega de tráfico, lo que permite diferenciar las llamadas de WhatsApp de otras aplicaciones, como compartir video, fotos o mensajes. Nuestra propuesta sólo tiene en cuenta las características estadísticas del flujo de tráfico de WhatsApp y no el contenido del paquete. Desde el punto de vista de los operadores, los beneficios de una herramienta de este tipo son múltiples: desde la priorización del tráfico hasta las campañas de marketing a medida para los usuarios que producen en gran medida llamadas de voz de WhatsApp.

1.1 Organización de la tesis

La tesis consta de los siguientes capítulos:

- Introducción general
- Resumen de los resultados obtenidos
- Trabajos publicados
- Anexo I: Otros trabajos publicados por el doctorando
- Anexo II: Copia completa de los trabajos publicados relacionados con la tesis.

2 Resumen de los resultados obtenidos

En este capítulo se realiza un resumen global de los resultados obtenidos, de la discusión de estos resultados y de las conclusiones finales.

En esta tesis se ha presentado la técnica de "perfil de día típico" y su aplicación al campo de detección de anomalías en la red, que constituye una nueva técnica basada en la teoría de la información, que analiza el patrón de tráfico a lo largo de las 24 horas del día. Después de realizar un análisis exhaustivo del tráfico para determinar el comportamiento normal del tráfico, ajustamos nuestro procedimiento considerando qué combinación de métodos estadísticos obtiene un mejor rendimiento en cada período del día. Además, hemos analizado los principales métodos de detección de cambios para determinar cuál obtiene los mejores resultados a lo largo de las 24h de un día típico. Determinar el período de tráfico concreto en el que se produce la anomalía es una labor esencial, ya que el tráfico se comporta de manera diferente a lo largo del día. Hemos probado cuatro técnicas estadísticas (test $\chi 2$ de Pearson, Kolmogorov-Smirnov, Información Mutua-MI y Suma acumulativa-CUSUM) con tráfico real e inyectando tráfico contaminado para determinar qué algoritmo detecta mejor las diferencias.

Por otra parte, hemos evaluado el procedimiento utilizando ocho semanas de tráfico de una universidad, en la que hemos añadido un día de amenazas al incluir el tráfico contaminado (inundaciones y ausencia de tráfico) en tres períodos específicos: tráfico bajo (4AM, noche), hora cargada (12AM, mediodía) y tráfico alto (5PM, tarde). Los resultados muestran que tres técnicas son las más precisas, pero su comportamiento depende de la carga de tráfico y la cantidad de contaminación introducida. La conclusión es que el algoritmo $\chi 2$ es el mejor para detectar caídas repentinas de tráfico, independientemente de la tasa de tráfico; MI es el algoritmo que detecta mejor el aumento repentino del tráfico independientemente de la tasa de tráfico, y también cuando el tráfico cae en períodos de alto tráfico; y finalmente CUSUM es el mejor en la detección de cambios cuando son muy abruptos, independientemente de la carga de tráfico.

De igual forma, hemos analizado cómo funcionan los diferentes métodos de detección de anomalías de tráfico para detectar puntos de cambio dentro de un perfil de día típico, y como resultado hemos desarrollado un algoritmo que propone qué combinación de técnicas estadísticas es más precisa en cada momento del día. Llegamos a la conclusión de que no hay un solo método que tenga mejor comportamiento, sino una combinación de técnicas estadísticas proporciona mejores resultados que una sola. Los resultados muestran que MI se comporta mejor en los intervalos de tráfico medio y alto, mientras que $\chi 2$ detecta mejor las variaciones en los períodos con menor tráfico, a diferencia de CUSUM, que detecta mejor cambios súbitos repentinos en el tráfico y complementa a ambos algoritmos. Los algoritmos no produjeron falsos positivos ni falsos negativos. Este enfoque es más útil que los cambios bruscos de pico basados en el análisis tradicional del tráfico, ya que consideramos el período de tráfico concreto en el que se produce la anomalía, porque es evidente que el tráfico se comporta de manera diferente a lo largo del día.

Además, hemos probado nuestro algoritmo utilizando una cantidad considerable de tráfico: el tráfico de 2.000 líneas fijas de banda ancha en Suecia de todo el año 2015. Hemos identificado cuatro días anómalos reales entre la traza de tráfico de todo el año, y hemos verificado la exactitud de nuestra técnica al detectar el período exacto de tiempo en el que ocurrió la anomalía. Los resultados son muy convincentes: se detectaron los diferentes períodos anómalos y no se notificó de ningún comportamiento anormal durante los períodos normales de tráfico: no dio lugar a falsos positivos ni falsos negativos. Por lo tanto, nuestro algoritmo de detección de anomalías, basado en desviaciones de la línea de base de tráfico, fue capaz de detectar todas las anomalías reales en un año de tráfico en una zona residencial en Suecia. Además, también hemos determinado que el algoritmo propuesto tiene unos requisitos computacionales muy bajos, y es adecuado para ejecutarse en routers SDN de gama baja en la red de acceso.

También, a partir de esta línea de investigación, hemos desarrollado un marco de seguridad basado en el contexto que utiliza un Indicador de Detección de Anomalías de Tráfico (TADI) que alerta de cuándo puede ocurrir una amenaza. Como contexto, utilizamos información basada en el tiempo que se encuentra en el análisis de perfil de un día típico para determinar con mayor precisión la presencia de una anomalía en función de la hora del día en que ocurre. En primer lugar, hemos categorizado el día típico en tres períodos principales diferentes (nocturno, diurno, hora ocupada), aunque este método también puede aplicarse a otros períodos de tiempo, como horas. A continuación se calcula el TADI a partir de la

información contextual basada en el tiempo. Nuestra propuesta es capaz de detectar cualquier ataque malicioso que altere el tráfico en la red, como inundaciones de tráfico o disminución del tráfico. Por ejemplo, el ataque de denegación de servicio (Denial of Service, DoS) se utiliza para interrumpir los servicios al inundar un nodo con una gran cantidad de tráfico. Cuando varios elementos inundan simultáneamente un único nodo con tráfico, el ataque se denomina Denegación de servicio distribuida (DDoS). Los tipos de ataque DoS y DDoS más comunes son el ataque de inundación ICMP, y el ataque de inundación SYN, donde el atacante envía peticiones de ping ICMP masivas al host de la víctima sin esperar una respuesta, o tramas TCP SYN, solicitando una conexión que nunca se establece. Además, el objetivo principal de los ataques es hacer caer un nodo o un enlace, o disminuir el rendimiento global de la red, lo que supone una reducción del tráfico. De esta manera podemos detectar ataques en dos etapas: de forma proactiva, al comienzo del ataque, cuando detectamos que hay un aumento de tráfico en curso; y también de forma reactiva, una vez concluido el ataque, cuando detectamos una disminución del tráfico como consecuencia de una caída producida en algún elemento de la red.

Asimismo, hemos caracterizado las llamadas de voz de WhatsApp para distinguirlas de otras funcionalidades de WhatsApp, como compartir video, fotos o enviar mensajes. En primer lugar, hemos estudiado el comportamiento de las llamadas de voz a través de WhatsApp, analizando el tráfico real intercambiado entre los usuarios. Luego lo hemos probado con usuarios reales bajo diferentes condiciones reales: llamadas locales, regionales, nacionales e internacionales, con distinta duración y en diferentes períodos del día, y coexistiendo con el tráfico de mensajería, y compartiendo imágenes y videos. De acuerdo con el estado de la técnica, no se ha desarrollado aún ningún mecanismo para detectar llamadas de WhatsApp.

Los beneficios para los operadores son múltiples, pero el principal es determinar cuántos usuarios están haciendo llamadas a través de WhatsApp, distinguiéndolos de otros servicios utilizados, lo que no es posible actualmente. Por una parte, de manera reactiva, el operador puede decidir gestionar este tipo de tráfico de diferentes maneras dependiendo del perfil del cliente, como priorizarlo o no entre otros servicios, limitar el tráfico de red mediante técnicas de modelado de tráfico o incluso rechazar llamadas de WhatsApp dependiendo del tipo de contrato. Por otra parte, ya que nuestra solución es capaz de identificar a los clientes que realizan llamadas de WhatsApp, el operador puede ofrecer productos adaptados al usuario

para consumo de voz (servicios VoIP alternativos, tarifas planas individualizadas, actualización de contratos de primas, etc.).

Cabe destacar que la utilización del tráfico de los usuarios plantea problemas de privacidad y está sujeto a las leyes de protección de datos, aunque sea con fines de marketing o para medir la calidad del servicio. En la actualidad, los contratos de los proveedores de servicios incluyen cláusulas diferentes para permitir el acceso a este tipo de información, muchas veces de manera agregada y / o anónima, para consentir el manejo de esta información con fines comerciales. Además, los reguladores nacionales de telecomunicaciones suelen instar a los proveedores de servicios a que pongan a disposición pública la información de las llamadas y los datos que se realicen en sus redes. Actualmente también se está considerando la publicación de las llamadas de VoIP también, por lo que es previsible que en un futuro cercano también soliciten información sobre llamadas de WhatsApp, y nuestra propuesta permite a los operadores cumplir con estos requisitos.

Finalmente cabe añadir que como resultado de las actividades de esta tesis se han publicado un total de 5 contribuciones en publicaciones de referencia: tres artículos como autor principal en revistas de reconocido prestigio (una de las cuales con clasificación T2 e indexado en JCR), y un artículo más en proceso de evaluación (con un primer feedback favorable por parte del editor del journal); un libro que ha sido publicado la editorial de referencia Elsevier, del que el autor es el editor y autor principal de todos los capítulos; y finalmente, un artículo como autor principal publicado en una conferencia internacional. Con todo, esta tesis doctoral se presenta como compendio de aplicaciones.

3 Trabajos publicados

En este capítulo se enumeran los trabajos publicados o admitidos para su publicación, haciendo constar el nombre de todos los coautores de los trabajos y la referencia completa de la revista en que los trabajos estén publicados o admitidos para su publicación.

En el anexo I de la presente tesis se enumeran otras publicaciones realizadas del doctorando.

En el anexo II de la presente tesis se incluye una copia completa de los trabajos publicados relacionados con la tesis.

3.1 Journals y revistas

[cuadra2015a] Cuadra-Sanchez, A., Aracil, J., & Ramos de Santiago, J. "Proposal of a new information theory-based technique based on traffic anomaly detection analysis". International Journal of Parallel, Emergent and Distributed Systems, 30(6), 464-477. doi:10.1080/17445760.2015.1044002 (2015)[2].

Clasificación: T2 – Q2 (indexado en SJR)

[cuadra2016] Cuadra-Sanchez, A. & Aracil, J. "Context-aware security framework based on Traffic Anomaly Detection Indicator". Journal of Telecommunication Systems, ISSN: 1018-4864, doi:10.1007/s11235-016-0233-8 (2016)[3].

Clasificación: T2 – Q3 (indexado en JCR)

[2] http://www.tandfonline.com/doi/abs/10.1080/17445760.2015.1044002

[3] http://link.springer.com/article/10.1007/s11235-016-0233-8

[cuadra2017a] Cuadra-Sanchez A, & Aracil J. “A novel blind traffic analysis technique for detection of WhatsApp VoIP calls”, International Journal of Network Management (2017), 1968[4].

Clasificación: T3 – Q4 (indexado en JCR)

[cuadra2017b] Cuadra-Sanchez, A. & Aracil, J. "Detecting traffic anomalies at the SDN edge: a case of one-year traffic sample in Sweden". Submitted to IEEE Communications Magazine, Special Issue on Advances in Network Services Chain (January 2017), en revisión.

Clasificación: T1 – Q1 (indexado en JCR)

3.2 Libro editado

[cuadra2015b] Cuadra-Sanchez, Antonio, and Javier Aracil. “Traffic Anomaly Detection”. Elsevier, 2015. ISBN 978-1-78548-012-6[5].

3.3 Artículo en conferencia

[cuadra2014] Cuadra-Sánchez, Antonio, Javier Aracil, and Javier Ramos de Santiago. "Proposal of a new information-theory based technique and analysis of traffic anomaly detection." IEEE International Conference on Smart Communications in Network Technologies (SaCoNeT), 2014.

[4]https://doi.org/10.1002/nem.1968

[5]http://store.elsevier.com/Traffic-Anomaly-Detection/Antonio-CuadraS%C3%A1nchez/isbn-9781785480126/

Anexo I: Otras publicaciones del doctorando

[fuentes2015] Fuentes-Lorenzo, D., Sánchez, L., Cuadra, A., & Cutanda, M. (2015). A RESTful and semantic framework for data integration. Journal of Software: Practice and Experience, 45(9), 1161-1188 (2015). doi: 10.1002/spe.2267

http://onlinelibrary.wiley.com/doi/10.1002/spe.2267/abstract

[mellouk2014] Mellouk, Abdelhamid, and Antonio Cuadra-Sanchez, editors. "Quality of experience engineering for customer added value services: from evaluation to monitoring". John Wiley & Sons, 2014. ISBN: 978-1-84821-672-3

http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1848216726.html

[cuadra2014a] Cuadra, A., Cutanda, M., Aurelius, A., Brunnström, K., de Vergara, J. L., Varela, M, Laulajainen, J.P., Morais, A., Cavalli, A., Mellouk, A., Agistin. B and Perez I. "An ecosystem for quality of experience management", Quality of Experience Engineering for Customer Added Value Services, 11-30.

[cuadra2014b] Cuadra, A., Cutanda, M., Perez, A., Rogles, E., Gutierrez, J. and Jauregizar, F."IPTV multiservice QoE management system", Quality of Experience Engineering for Customer Added Value Services, 31-52.

[guyard2014c] Guyard, F., Varela, M., Skorin-Kapov, L., Cuadra-Sanchez, A., & Sevilla-Ramos, P. J. (2014). Quality of experience estimators in networks. Quality of Experience Engineering for Customer Added Value Services, 225-243.

[cuadra2013a] Cuadra, A., Cutanda, M., Aurelius, A., Brunnström, K., de Vergara, J. L., Varela, M., & Augustin, B. (2013, June). Ecosystem for customer experience assurance. In Smart Communications in Network Technologies (SaCoNeT), 2013 International Conference on (Vol. 3, pp. 1-5). IEEE.

[cuadra2013b] Cuadra, A., Cutanda, M., Perez, A., Rogles, E., Gutiérrez, J., & Jaureguizar, F. (2013, June). SAVAGE: IPTV multiservice QoE management system. In Smart Communications in Network Technologies (SaCoNeT), 2013 International Conference on (Vol. 3, pp. 1-5). IEEE.

[cuadra2012] Cuadra-Sánchez, Antonio; Cutanda-Rodríguez, Mar; Pérez-Mateos, Ismael; Aurelius, Andreas; Brunnström, Kjell; Laulajainen, Jukka-Pekka; Varela, Martín; De Vergara, Jorge E López; "A global customer experience management architecture", Future Network & Mobile Summit (FutureNetw), 2012,1-8, 2012, IEEE.

[morais2012] Morais, Anderson; CAVALLI, Ana; Tran, Hai Anh; Mellouk, Abdelhamid; Augustin, Brice; Hoceini, Said; Cuadra-Sánchez, Antonio; Brunnström, Kjell; Aurelius, Andreas; "Managing customer experience through service quality monitoring", Conference Proceedings of Future Network and Mobile Summit,2012

[menkovski2012] Menkovski, Vlado; Exarchakos, Georgios; Liotta, Antonio; Sánchez, Antonio Cuadra; "Quality of experience models for multimedia streaming", Advancing the Next-Generation of Mobile Computing: Emerging Technologies, 112,2012,IGI Global, ISBN: 9781466601192.

[cuadra2011a] Cuadra-Sanchez, Antonio; del Mar Cutanda-Rodriguez, Maria; Martinez, Rosa Maria; Fernandez, Olga; Prieto, Silvia; Serrano, Salvador; Barbadillo, Jose Carlos; "OMEGA-Q: A platform for measuring, troubleshooting and monitoring the quality of IPTV services", Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on", 882-895,2011,IEEE

[cuadra2011b] Cuadra, Antonio; Cutanda, Ma Mar; Fuentes-Lorenzo, Damaris; Sánchez, Luis; "A semantic web-based integration framework", Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on", 93-98,2011 ,IEEE

[cuadra2011c] Cuadra, A; Mata, Felipe; García-Dorado, José Luis; Aracil, Javier; De Vergara, J López; Cortés, FJ; Beltrán, P; De Mingo, E; Ferreiro, A; "Traffic monitoring for assuring quality of advanced services in Future Internet", International Conference on Wired/Wireless Internet Communications IFIP WWIC 2011,186-196,2011,Springer Berlin

[cuadra2011d] Antonio Cuadra-Sanchez; Maria del Mar Cutanda-Rodriguez "Evaluación del aprendizaje electrónico a través de la monitorización de plataformas de eLearning / Evaluation of learning through the monitoring of e-learning platforms", XXI Jornadas Telecom I+D, Septiembre de 2011.

[cuadra2011e] Antonio Cuadra-Sanchez; Maria del Mar Cutanda-Rodriguez "El papel de la Calidad de la Experiencia en la Interacción Persona-Ordenador / The role of the Quality of

Experience in Human-Computer Interaction", XXI Jornadas Telecom I+D, Septiembre de 2011.

[cuadra2011f] Antonio Cuadra-Sanchez; Javier Aracil; Maria del Mar Cutanda-Rodriguez; Pedro, María Santiago Del Río; Javier Ramos; José Luis García-Dorado; Francisco Garcés García, "Tecnologías para la inspección de aplicaciones basadas en monitorización pasiva de paquetes con análisis ciego de tráfico / Technologies for applications inspection based on passive monitoring and traffic blind analysis", XXI Jornadas Telecom I+D, Septiembre de 2011.

[fuentes2011] Fuentes-Lorenzo, Damaris; Sánchez, Luis; Cuadra-Sánchez, Antonio; del Mar Cutanda-Rodríguez, María; "Managing Legacy Telco Data Using RESTful Web Services,REST: From Research to Practice", 303-317, 2011, Springer New York.

[delrio2011] Del Rio, PM Santiago; Ramos, Javier; García-Dorado, José Luis; Aracil, Javier; Cuadra-Sánchez, A; Cutanda-Rodríguez, M; "On the processing time for detection of Skype traffic", Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International", 1784-1788,2011,IEEE

[menkovski2011a] Menkovski, Vlado; Exarchakos, Georgios; Liotta, Antonio; Cuadra-Sánchez, Antonio; "A quality of experience management module", International Journal on Advances in Intelligent Systems Volume 4, Number 1 & 2, 2011.

[menkovski2011b] Menkovski, Vlado; Exarchakos, Georgios; Liotta, Antonio; Cuadra-Sánchez, Antonio; ,"Managing quality of experience on a commercial mobile TV platform", International Journal on Advances in Telecommunications Volume 4, Number 1 & 2, 2011", 2011.

[cuadra2010a] Cuadra Sánchez, A; del Mar Cutanda Rodríguez, M; Liotta, A; Menkovski, V; "Method for calculating perception of the user experience of the quality of monitored integrated telecommunications operator services." Patente ES WO2011141586, U.S. Patent Application No. 13/697,891, Patent date Issued Dec 28, 2010.

[cuadra2010b] Cuadra Sánchez, A; del Mar Cutanda Rodríguez, M; "Dispositivo y método para monitorizar tráfico de extremo a extremo y medir la calidad entregada a los clientes en redes opticas pasiva.", Patente ES2390546 A1 ES2390546 B1 H04Q11/00, Patent date Issued Dec 28, 2010

[cuadra2010c] Cuadra-Sanchez, Antonio; Casas-Caballero, Clara; “A generic monitoring architecture for assuring the QoS in mobile TV platforms”, MELECON 2010-2010 15th IEEE Mediterranean Electrotechnical Conference, 1227-1231,2010,IEEE.

[cuadra2010d] Cuadra Sanchez Antonio, Angel Ferreiro Olivo, "Gestión de la Calidad de la Experiencia de Usuarios de Servicios de Telecomunicaciones", XX Jornadas Telecom I+D 2010.

[cuadra2010e] Cuadra Sanchez, Antonio; M. Del Mar Cutanda Rodriguez, Eduardo Martín, Damaris Fuentes-Lorenzo, Luis Sánchez, David Muñoz-Díaz "Integración de Bases de datos basada en Web Semántica", XX Jornadas Telecom I+D 2010, Valladolid

[delrio2010] del Río, Pedro M Santiago; Ramos, Javier; Salvador, Alfredo; de Vergara, Jorge E López; Aracil, Javier; Cuadra, Antonio; Cutanda, Mar; “Application of internet traffic characterization to all-optical networks”, Transparent Optical Networks (ICTON), 2010 12th International Conference on",1-4,2010,IEEE

[menkovski2010a] Menkovski, Vlado; Exarchakos, Georgios; Liotta, Antonio; Sánchez, Antonio Cuadra; “Estimations and remedies for quality of experience in multimedia streaming", Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services (CENTRIC), 2010 Third International Conference on", 11-15,2010,IEEE

[menkovski2010b] Menkovski, Vlado; Exarchakos, Georgios; Liotta, Antonio; Sánchez, Antonio Cuadra; “Measuring quality of experience on a commercial mobile TV platform", Advances in Multimedia (MMEDIA), 2010 Second International Conferences on", 33-38,2010,IEEE.

[cuadra2009a] Cuadra, A; Garces, F; del Sol, JA; Nieto, G; “A generic end-to-end monitoring architecture for multimedia services", Integrated Network Management, 2009. IM'09. IFIP/IEEE International Symposium on", 129-132,2009,IEEE

[cuadra2009b] Cuadra-Sanchez, Antonio; Casas-Caballero, Clara; “End-to-end quality of service monitoring in convergent IPTV platforms”, Next Generation Mobile Applications, Services and Technologies, 2009. NGMAST'09. Third International Conference on",303-308,2009,IEEE

[cuadra2009c] Cuadra Sánchez, Antonio, M. Del Mar Cutanda Rodriguez, Francisco Garces Garcia, J.L. García-Dorado, V. Lucas, J. Aracil, J.E. López de Vergara "Caracterización

avanzada de uso de servicios y aplicaciones en redes de datos mediante el análisis detallado de tráfico", XIX Jornadas Telecom I+D 2009

[cuadra2009d] Cuadra Sánchez, Antonio, Angel Ferreiro Olivo, Nuria Gomez Rojo, F. Mata Marcos, J. Ramos, "Monitorización de tráfico IP para el control de calidad de servicio en entornos convergentes" XIX Jornadas Telecom I+D 2009

[cuadra2009e] Cuadra Sánchez, Antonio, M. Del Mar Cutanda Rodriguez, Francisco Garces Garcia, "Network tomography applied to surveillance of QoS", 48th FITCE Congress 2009.

[cuadra2009f] Cuadra Sánchez, Antonio, Mar Cutanda Rodriguez, Marcos Reyes Ureña, Jose Manuel Cantera Fonseca, Francisco Garces Garcia, Luis Sanchez Fernandez, Damaris Fuentes Lorenzo "Service monitoring platform based on advanced web technologies" 48th FITCE Congress, 2009.

[menkovski2009a] Menkovski, Vlado; Oredope, Adetola; Liotta, Antonio; Sánchez, Antonio Cuadra; "Predicting quality of experience in multimedia streaming", Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia,52-59,2009,ACM.

[menkovski209b] Menkovski, Vlado; Oredope, Adetola; Liotta, Antonio; Sánchez, A Cuadra; "Optimized online learning for QoE prediction", Proc. of the 21st Benelux conference on artificial intelligence, 2009.

[cuadra2008a] Cuadra, Antonio; Garcés, Francisco; Reyes, Marcos; Fuentes-Lorenzo, Damaris; Sánchez, Luis; Cantera, José M; "Tecnologías Web Avanzadas para el Aseguramiento de la Calidad de Servicio", IV Jornadas Científico-Técnicas en Servicios Web y SOA, Sevilla, 2008.

[cuadra2008b] Cuadra Sánchez, Antonio, Francisco Garces Garcia, Jose Manuel Cantera Fonseca, Antonio Cuadra Sanchez, Marcos Reyes Ureña, Luis Sánchez, Damaris Fuentes "Plataforma de monitorización avanzada basada en tecnologías web", XVIII Jornadas Telecom I+D 2008

[ansorena2008] Ansorena Campuzano, Maria Reyes, Cuadra Sánchez, Antonio Francisco Garces Garcia, Antonio Cuadra Sanchez, Nuria Gomez Rojo, Pedro Jose Sevilla Ramos, "How to face convergence to guarantee end-to-end quality of service", ICT-MOBILE SUMMIT 2008.

[cuadra2007a] Cuadra Sánchez, Antonio; “Supervisión de la calidad percibida en plataformas de IPTV“, Jornadas Telecom I+D, 2007.

[cuadra2007b] Cuadra Sánchez, Antonio Cuadra; García, Francisco Garcés; “Tomografía en los sistemas de gestión”, Jornadas Telecom I+D ,2007.

[cuadra2007c] Cuadra Sánchez, Antonio, Francisco Garces Garcia, Pedro Jose Sevilla Ramos, "Convergencia en la supervisión de redes y servicios", XVII Jornadas Telecom I+D, 2007.

[cuadra2007d] Cuadra Sanchez, Antonio, Alfonso Castro Escudero, Begoña Costales Piñera, "Normalización del modelo de información del subsistema IMS", XVII Jornadas Telecom I+D, 2007.

[cuadra2007e] Cuadra Sanchez, Antonio, Francisco Garces Garcia, Rosa Maria Martinez Martin, Pablo Merino Moro, Maria Reyes Ansorena Campuzano, "Tecnologías para auditorías de calidad de servicios triple play en redes internet de nueva generación", Primer premio de "Nuevas aplicaciones para internet", concedido por la cátedra telefónica de la UPM, 2007.

[cuadra2005a] Cuadra Sanchez, Antonio, Alfonso Castro Escudero, Begoña Costales Piñera, Hector Garces Mencia, "Sistema de caracterización de uso de red", Jornadas Telecom I+D 2005

[cuadra2005b] Cuadra Sanchez, Antonio, "Supervisión del fraude en redes NGN (de nueva generación)" Jornadas Telecom I+D 2005.

[cuadra2004a] Cuadra Sánchez, Antonio, Manuel Diaz Cayetano, Alfonso Castro Escudero, Victoria Lorenzana, "gestión dinámica de tráfico de usuarios en redes GPRS", XIV Jornadas Telecom I+D 2004.

[cuadra2004b] Cuadra Sánchez, Antonio, "Supervisión de redes y servicios en NGN", XIV Jornadas Telecom I+D 2004.

[cuadra2004c] Cuadra Sánchez, Antonio; “Gestión de redes de voz sobre IP”, Comunicaciones de Telefónica I+ D, 33,33-42,2004,Telefónica I+ D.

[cuadra2003] Cuadra Sánchez, Antonio “Supervisión de la calidad de servicio en redes VoIP”, Jornadas Telecom I+D 2003.

[cuadra2002a] Cuadra Sánchez, Antonio “Sistema de gestión de redes IP basado en sondas”, Jornadas Telecom I+D 2002.

[cuadra2002b] Cuadra Sánchez, Antonio; Merinero, Diana López; “La gestión de la señalización en Latinoamérica”, Comunicaciones de Telefónica I+ D, 28,59-70,2002, Telefónica I+D.

Anexo II: Copia completa de los trabajos publicados

[cuadra2014] Cuadra-Sánchez, Antonio, Javier Aracil, and Javier Ramos de Santiago. "Proposal of a new information-theory based technique and analysis of traffic anomaly detection." IEEE International Conference on Smart Communications in Network Technologies (SaCoNeT), 2014.

[cuadra2015a] Cuadra-Sanchez, A., Aracil, J., & Ramos de Santiago, J. "Proposal of a new information theory-based technique based on traffic anomaly detection analysis". International Journal of Parallel, Emergent and Distributed Systems, 30(6), 464-477. doi:10.1080/17445760.2015.1044002 (2015). Clasificación: T2 – Q2 (indexado en SJR)

[cuadra2015b] Cuadra-Sanchez, Antonio, and Javier Aracil. "Traffic Anomaly Detection". Elsevier, 2015. ISBN 978-1-78548-012-6.

[cuadra2016] Cuadra-Sanchez, A. & Aracil, J. "Context-aware security framework based on Traffic Anomaly Detection Indicator". Journal of Telecommunication Systems, ISSN: 1018-4864, doi:10.1007/s11235-016-0233-8 (2016). Clasificación: T2 – Q3 (indexado en JCR)

[cuadra2017a] Cuadra-Sanchez A, & Aracil J. "A novel blind traffic analysis technique for detection of WhatsApp VoIP calls", International Journal of Network Management (2017), 1968. Clasificación: T3 – Q4 (indexado en JCR)

[cuadra2017b] Cuadra-Sanchez, A. & Aracil, J. "Detecting traffic anomalies at the SDN edge: a case of one-year traffic sample in Sweden". Submitted to IEEE Communications Magazine, Special Issue on Advances in Network Services Chain (January 2017), en revisión. Clasificación: T1 – Q1 (indexado en JCR)