Estado del arte en redes 4G (Umts) y 3G-wlan (Pbnm) para terminales móviles como medida de control en el sistema penitenciario colombiano

Por:

Gustavo Adolfo Marún Suárez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

TECNOLOGÍA EN SISTEMAS / INGENIERIA DE SISTEMAS

BUCARAMANGA

2016

Estado del arte en redes 4G (Umts) y 3G-wlan (Pbnm) para terminales móviles como medida de control en el sistema penitenciario colombiano

Por:

Gustavo Adolfo Marún Suárez

Proyecto de grado para optar el título de Ingeniero de Sistemas

Asesor:

Ing. Martín Camilo Cancelado Ruiz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

TECNOLOGÍA EN SISTEMAS / INGENIERIA DE SISTEMAS

BUCARAMANGA

2016

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

1 INTRODUCCION

En las cárceles y centros penitenciarios de nuestro país, desafortunadamente no se consigue en muchas ocasiones resocializar a los delincuentes que ingresan a pagar una condena, es más un sitio donde pueden y llegan a perfeccionar sus actos criminales o incluso a adquirir nuevas habilidades para cometer otros tipos de delitos, generando ingresos mediante la extorsión, la estafa usando como canal los dispositivos móviles. Esto no debería ocurrir si existiera un sistema penitenciario organizado y libre de corrupción pero esta no es la realidad de Colombia, es por ello que se hace necesario mitigar de alguna este flagelo que afecta a miles de ciudadanos de bien, y genera pérdidas por millonarias sumas al año, la mejor forma de poder lograr evitar esta problemática es mediante la aplicación de tecnologías que ya existen y que el gobierno debe exigir a las empresas de telecomunicaciones a implementar lo antes posible, ya que nuestra legislación actual en materia de comunicaciones lo exige y lo permite hacer, vemos una gran oportunidad en la redes 4G la posibilidad de combatir esta problemática de forma eficaz dando resultados en contra del crimen organizado.

2 JUSTIFICACION

Las estadísticas hablan por sí solas en el año 2014 se recibieron 4848 denuncias de extorsiones, de las cuales el 8.3 % provinieron de las cárceles tanto llamadas como mensajes de texto, sin contar con las que nunca se llegaron a denunciar.

Los delincuentes con ayuda de otra persona que se encuentra fuera de la cárcel, se hacen a información y al número telefónico para luego proceder a realizar la extorsión haciéndose pasar por comandantes de las bandas criminales como los Rastrojos, Urabeños y frentes de la guerrilla, logrando engañar y embaucando a sus víctimas y así ejecutando la estafa o la extorsión en cuestión de minutos.

Otra forma con la cual los delincuentes consiguen información de primera mano, es ingresando con el mismo teléfono a las redes Sociales donde las personas escriben información de alta confidencialidad y de allí logran ubicar a la víctima para posteriormente extorsionarla.

Aunque los terminales móviles sin duda son importantes a la hora de registrar algún tipo de emergencia o ayuda al interior de los penales ya que son un medio eficaz de comunicación, es también cierto que deben ser usados únicamente por personal autorizado, como administrativos y guardianes en un lugar propicio para que no se genere la posibilidad del robo de los mismos por parte de los reclusos de un penal.

3 RESUMEN

El presente trabajo busca hacer un análisis de la situación actual que se vive al interior de las penitenciarías colombianas, a nivel de delitos como la extorsión y la estafa usando dispositivos móviles, así como un estado del arte de las tecnologías móviles disponibles para poder mitigar este flagelo que azota diariamente a la ciudadanía en general, y de la aplicación de esta tecnología que está disponible siendo aplicable por la legislación colombiana en materia de telecomunicaciones, para que sea el mismo gobierno el encargado de ordenar a la compañías de telefónica móvil a empezar a usar esta tecnología sin importar solo el beneficio económico que les trae usar la tecnología actual sin importar el beneficio de los usuarios del sistema.

3.1 PALABRAS CLAVES

Cárcel, Sistema Penitenciario, delito, networks, cellular, hacker, mobile divices, imsi, catcher, downgrade, denial of service, 3G, 4G, UMTS, WLAN, SIP, NAS, NAT.

4 PLANTEAMIENTO DEL PROBLEMA

Según el mundo.com (Agosto 30 de 2014) solo con el uso de un teléfono móvil desde una cárcel es suficiente para que un delincuente usando engaños y amenazas pueda llenarse los bolsillos en cuestión de minutos, en nuestro país las cárceles no son solo un lugar para recluir a las personas que cometieron algún o algunos delitos y resocializarse para luego salir de allí como un ciudadano nuevo útil que le aporte a la sociedad, en cambio se convierte en el lugar perfecto para planear el crimen y es donde se prolifera la semilla del delito.

Según Héctor Javier Barrera Palacio 80 de cada 100 delitos que se cometen en las ciudades se planean y se ordenan desde las prisiones, según fuentes consultadas.

El espectador.com en su edición del (5 Febrero de 2015) público que una muestra de ello son las cifras de extorsión y estafa que se producen desde centros penitenciarios. De 4.848 casos en 2014, desde un establecimiento carcelario se realizaron 407. Para las autoridades, en más del 50% de los casos hay involucrada una persona cercana a la víctima.

En el año 2014 se evitó que llegaran a los bolsillo de los delincuentes 706 millones a través de extorsiones.

El secuestro ha disminuido considerablemente en los últimos años en el año 2000 denunciaron 3.572 secuestros y en el año 2014 la cifra cayó a 283 secuestros, la extorsión y la estafa son dos delitos que han subido de posición y ahora se ubican dentro de la lista de los más combatidos.

Esta cifra se ha incrementado debido a la desmovilización de grupos alzados en armas como los paramilitares y guerrilleros que siguen practicando esta modalidad de delito desde las cárceles y centros penitenciarios.

Es más fácil extorsionar o estafar que realizar un secuestro, además si se puede hacer por un teléfono móvil sin necesidad de salir de la cárcel y muchos menos de exponer la vida en la ejecución del delito ¿por qué no?

La denuncia es para las autoridades la mejor estrategia para poder acabar con este flagelo, sin embargo son muchas las extorsiones y estafas que no se denuncian así que la mejor forma de evitar este delito es atacando técnicamente a los delincuentes en las mismas cárceles con técnicas y métodos que ni siquiera ellos sepan cómo evitarlo.

¿Cuáles son las tecnologías en la actualidad en materia de telecomunicaciones que permitan eliminar los delitos desde las cárceles de Colombia?

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Estructurar un estado del arte de las redes 3G Y 4G así como la comunicación entre ellas para poder gestionar de una manera más eficiente la red basada en políticas específicas logrando identificar y bloquear los teléfonos móviles al interior de los penales que están siendo usados para actividades criminales.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar análisis de las diferentes vulnerabilidades o forma de gestionar que presentan las redes 3G (UMTS) y 4G para poder aprovecharlas y combatir el crimen organizado desde las penitenciarías del país.

- Demostrar que las redes 4G son más administrables que las 3G logrando tener un mayor control y monitoreo sobre los abonados de los operadores celulares en nuestro país.

- Identificar los diferentes dispositivos y elementos necesarios para configurar una red 4G.

- Reconocer la importancia de la seguridad informática en la protección de redes de datos y voz tanto wifi como UMTS.

.

6 RESULTADOS ESPERADOS

A continuación se relacionan los resultados esperados con el desarrollo del proyecto de grado propuesto:

El objetivo central de esta investigación es la elaboración del estado del arte de las diferentes formas de gestionar las redes 3G y 4G de telefonía celular y la combinación entre ellas, que se podría aprovechar para poder administrar en el tema de seguridad redes en el país y así evitar que se sigan cometiendo delitos desde las cárceles y centros penitenciarios a nivel nacional.

Analizaremos temas técnicos, y estudios tanto a nivel nacional como internacional en el tema de seguridad en redes UMTS (3G) y la famosa red 4G basada completamente en el protocolo de comunicación de internet IP (Internet protocol) así como la infraestructura tecnológica necesaria para que puedan operar estas tecnologías de comunicación, de tal manera que podremos identificar puntualmente sus vulnerabilidades para poder aprovechar estas para beneficio de la seguridad de la comunidad

- Estado del arte acerca de las redes 3G y 4G y su comunicación entre sí.
- Estado del arte del sistema penitenciario Colombiano en la actualidad
- Documentación de los sistemas y modelos implementados para estos fines.

7 MARCO TEÓRICO

El desarrollo de este trabajo de investigación se basa teniendo en cuenta la problemática social que existe en nuestro país y las falencias técnicas de las redes 2G (GSM), 3G (UMTS) se hace necesario implementar y usar la tecnología 4G que no es otra cosa que la conexión de una red 3G a la WLAN debemos saber específicamente su arquitectura y elementos centrales que las componen así como su forma de operar para aplicar los conocimientos técnicos y de esta forma poder dar solución a la problemática social originada dentro de las cárceles del país, como son estafas y extorciones por ello los tipos de arquitectura y forma de comunicación entre una red 3G y la WLAN que finalmente conforma una 4G.

En la actualidad en la comunidad tecnológica se conocen los siguientes ataques en las redes 3G (UTMS) y 4G que por ende también se dieron en su momento en las redes 2G (GSM):

- Ataques DDoS a nivel de red [1]
- Ataques DDoS Reflectantes
- Ataques DDoS Salientes
- Ataques distribuidos
- Ataques DDoS a nivel de aplicación

DDoS es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. [2]

Los ataques distribuidos son iguales a los DDos comunes pero la diferencia es que no tienen una sola fuente de ataque si no cientos o miles. En este ataque se infectan los ordenadores inseguros que se encuentran conectados constantemente a internet ADSL, con una dirección IP estática, a estos a partir del ataque se les denomina “Zombies” o agentes del ataque. Esta infección cosiste en un troyano o en un programa de ataque que se instala en los agentes que es un programa que no hace daño pero los convierte en soldados a la espera de órdenes del atacante, existen además dos tipos de “colaboradores” los “handlers”, que son los que se encargar de infectar a los agentes y los agentes desde los cuales de ataca.[3]

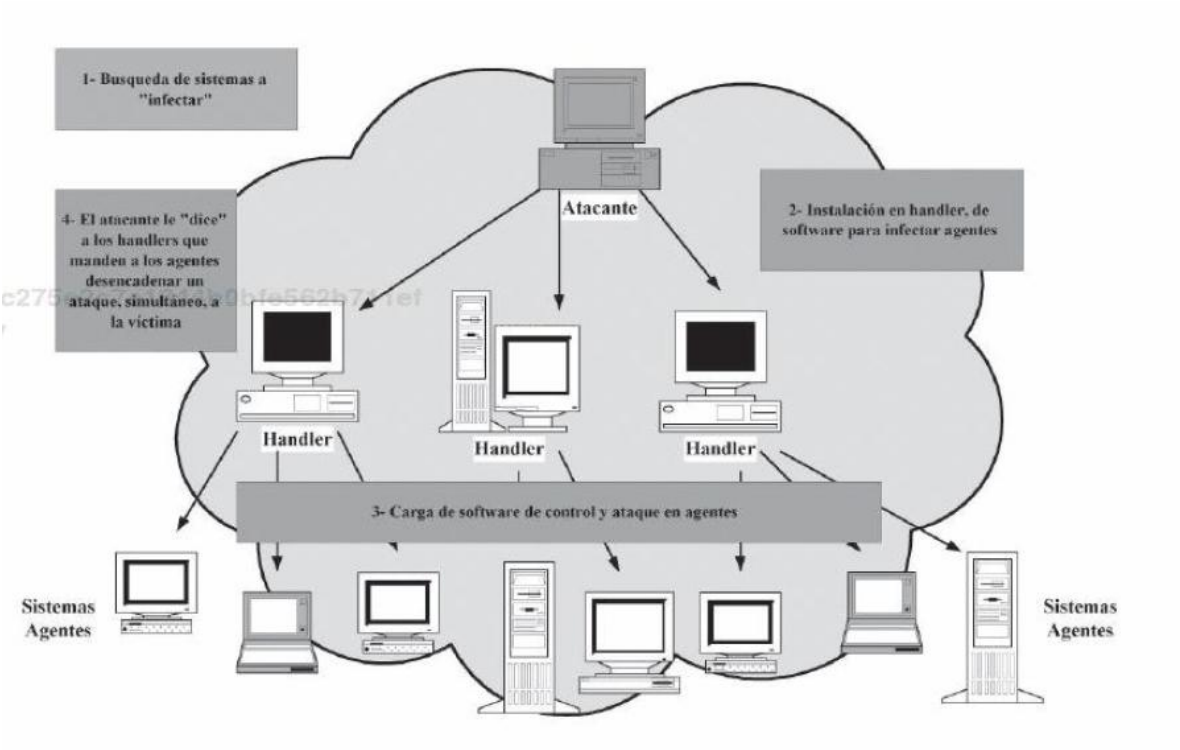
[1] (Distributed Denial of Service) - Ataque de denegación de servicios en la capa de red del Modelo OSI.

[2] https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio

[3] Procesos y herramientas para la seguridad de redes. : UNED - Universidad Nacional de Educación a Distancia, 2000

ATAQUE DOS DISTRIBUIDO

Figura 1: Esquema de ataque DDoS Distribuido



Fuente: Procesos y herramientas para la seguridad de redes. : UNED - Universidad Nacional de Educación a Distancia, 2000. ProQuest ebrary. Web. 5 May 2016.

DDOS reflectante: (Ataque a nivel de red) Ataque TCP DDoS a nivel de red los atacantes cambian su dirección IP origen (spoofing) para que tenga el origen de la red a atacar. Posteriormente empiezan a realizar una inundación masiva de tipo SYN flood contra servidores en internet que contestarán contra su objetivo. El resultado es una inundación del Firewall con los SYN-ACKs entrantes y la CPU de los reverse proxies y Firewalls sube hasta que no pueda tratar las peticiones de usuarios legítimos.[4]

DDOS de Salida: (Ataque a nivel de red y de aplicación) Un ataque DDoS a nivel de red visto desde otro punto de vista este ataque DDoS involucra hosts dentro del perímetro de defensa del cliente, habitualmente PC's infectados por Malware, integrados en una red de botnet y controlados remotamente para participar en

[4] Fuente: http://www.cioal.com/2012/03/15/la-proteccion-real-frente-a-ataques-ddos/

ataques DDoS Como consecuencia, el ISP puede detectar un tráfico saliente de ataque desde la red del cliente y hacer un blackholing para proteger “Internet” del tráfico de ataque DDoS proviniendo de la red afectada. A parte del problema de reputación, la conexión a Internet puede ser bloqueada por el ISP.[5]

DDOS en la capa de aplicación: (Ataque a nivel de aplicación) Es una variante más reciente e inteligente de ataque DDoS. Estos ataques se basan en tráfico legítimo y conexiones TCP completadas. Una vez que la conexión TCP se establece, los atacantes realizan varias peticiones repetidas a la aplicación en un intento de agotar los recursos de los servidores y Bases de Datos.

Es difícil defenderse porque estos ataques crean una condición de denegación de servicio sin afectar el consumo de ancho de banda, uno de los más usados es Slow Loris. Como se puede observar, hay cada vez más tipos de ataques DDoS y son cada vez más complejos de detectar. En su momento fueron necesarios los Firewalls, luego los IPS, hoy en día, cualquier cliente que publica servicios Web, DNS o dispone de VoIP es susceptible de ser víctima de un ataque DDoS. Corero propone a través de su red de partners una tecnología fiable, validada por más de 2000 clientes y capaz de defender ante todos los tipos de ataques DDoS existentes.[6]

La tecnología celular UMTS (Universal MobileTelecommunications System) es el sistema de telecomunicaciones móviles de tercera generación (3G) que proporciona a usuarios móviles dos tipos de servicios de comunicaciones: servicios de paquetes (PS - Packet Switched) para aplicaciones de datos y servicios de conmutación de circuitos (CS - Circuit Switched) para aplicaciones de voz y telefonía.[7]

El ambiente de la red 4G está diseñado para garantizar una red de acceso generalizado con la inclusión de las nuevas interfaces radioeléctricas, basada en una infraestructura común completamente IP, flexible y sin fisuras, que soporte la escalabilidad y la movilidad. En ese sentido el usuario es el centro de atención en el cual gira la tecnología por lo que las alternativas inalámbricas y móviles deben estar enfocadas a cubrir sus necesidades y todo debe estar vinculado a un mecanismo de gestión y administración único centralizado que garantice e integre

[5] Fuente: http://www.cioal.com/2012/03/15/la-proteccion-real-frente-a-ataques-ddos/

[6] Fuente: http://www.cioal.com/2012/03/15/la-proteccion-real-frente-a-ataques-ddos/

[7] Fuente: http://bibliotecavirtual.unad.edu.co/ - (IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008)

cada uno de los servicios que preste la red y así mejorar la calidad de todos los servicio ofertados.

La tecnología en los campos de la telemática, la ingeniería de las telecomunicaciones y las redes wifi como celulares han avanzado sustancialmente en aspectos claves como la seguridad, implementando diferentes técnicas de ataque DDoS y de gestión basada en políticas aprovechando en muchas ocasiones el mal manejo de la información por parte del usuario y en ocasiones usando ingeniería social para poder obtener información clave la cual es susceptible de ser usada para fines criminales como la extorsión, el chantaje entre otros.

Actualmente, la mayor parte de los ataques DDoS tienen como meta sacar ventaja monetaria y son financiados por criminales cibernéticos organizados. También hay ofensivas en la infraestructura y en las aplicaciones, con una variedad de técnicas utilizadas: volumétricas, multivectoriales, de fragmentación, protocolo de recursos y conociendo el IMSI (*Identidad Internacional del Abonado a un Móvil*). Es posible realizar un ataque selectivo ya que este código de identificación es único para cada dispositivo de telefonía móvil integrado en la tarjeta SIM y permite su identificación en redes GSM y UMTS, etc. [8]

En un modelo basado en políticas de gestión y administración al aplicar las políticas en cada uno de los elementos gestionados deben ser seleccionados por un elemento intermediario conocido como Punto de Decisión de Política (PDP – Policy Decisión Point), el cual se comunica con el PR[9] mediante algún protocolo Ligero/Simplificado de Acceso a Directorios y es responsable de Interpretar las políticas almacenadas en el PR y proporcionar respuesta a las peticiones realizadas por el PEP[10].

La integración de las redes celulares con las redes Wi-Fi ha sido un punto de investigación en los últimos años. Algunos esfuerzos han sido dirigidos a solucionar el problema de la interconexión de las dos arquitecturas, para lo cual han propuesto modelos de interconexión dependiendo de los diferentes dominios de gestión disponibles. Con respecto al uso de la gestión basada en políticas dentro del entorno integrado 3G-WLAN se han hecho esfuerzos por resolver problemas específicos como son: control de la movilidad y traspasos, los cuales basan sus decisiones en políticas que evalúan las preferencias del usuario y condiciones de la red. Sin embargo, desde el punto de vista del entorno, los requerimientos de servicio deben ser evaluados para un mejor control de selección de traspaso. Con respecto al control de acceso, la gestión basada en políticas ha sido implementada para una gestión de control de acceso más flexible. Uno de los

8 MIGUEL ÁLVAREZ CALVO, MARÍA TERESA APARICIO PEÑA (1ª EDICIÓN: FEBRERO DE 2005.)

9 Punto de Aplicación de Políticas

10 Repositorio de política

problemas de la gestión de entornos integrados en los que se ha propuesto con mayor auge el uso de la gestión basada en políticas es el control de la calidad de servicio (QoS) extremo a extremo. La que debe mostrar una arquitectura de gestión basada en políticas para proveer un control QoS consistente sobre un sistema integrado UMTS-WLAN, pero solamente se enfoca a la ubicación adecuada de las entidades de gestión basada en políticas y los flujos de comunicación de las entidades y no en la definición de las clases de políticas a ser implementadas. [11]

Al existir esta infraestructura tecnológica instalada en nuestro país hace que exista la posibilidad de aplicar estas técnicas y metodologías de "gestión" a los que promueven y viven del crimen aplicando ingeniería inversa para lograr finalmente detener estas actuaciones que deja cada año una cifra significativa de victimas a lo largo y ancho del país.

[11]Fuente: http://bibliotecavirtual.unad.edu.co/- (IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008)

8 METODOLOGIA

El proyecto se desarrollará considerando la metodología de análisis, distribuidas en 2 etapas:

El Método analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

¿Qué significa Analizar?

Analizar significa desintegrar, descomponer un todo en sus partes para estudiar en forma intensiva cada uno de sus elementos, así como las relaciones entre sí y con el todo. La importancia del análisis reside en que para comprender la esencia de un todo hay que conocer la naturaleza de sus partes, como son las que vamos a analizar en este trabajo que son:

- El sistema carcelario en Colombia
- La elaboración del plan de trabajo
- El Análisis del estado del arte de las tecnologías disponibles para realizar mayor control sobre la red de abonados.
- El Desarrollo y presentación de la propuesta con su análisis y conclusiones del estado del arte

9 CRONOGRAMA DE ACTIVIDADES

De acuerdo con las etapas y actividades planteadas, a continuación se presenta el cronograma a desarrollar:

Tabla 1: Cronograma del Proyecto

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4
Conocimiento del sistema carcelario en Colombia y su problemática.				
Elaboración del plan de trabajo presupuesto y recursos necesarios.				
Estado del arte tecnologías disponibles para hacer control mediante DDoS a terminales móviles de abonado de la red, así como la legislación actual en nuestro país en el tema de telecomunicaciones móviles.				
Análisis y conclusiones del estado del arte de las tecnologías disponibles para realizar Gestión y denegación de servicios a terminales móviles.				

Fuente: Autor

10 PLAN DE TRABAJO Y RECURSOS NECESARIOS:

10.1 PRESUPUESTO

El siguiente cuadro contiene el presupuesto establecido para el proyecto de grado:

Tabla 2 Presupuesto del proyecto

RECURSO	DESCRIPCION	PRESUPUESTO ($)
Equipo Humano (Honorarios)	Ingeniero de sistemas	1.500.000
Equipos y Software	Computador de escritorio/portátil/impresora/office/Visio	4.000.000
Viajes y Salidas de Campo	Visita a distintos centros penitenciarios	300.000
Materiales y suministros	Papel, tinta	200.000
Otros	----	500.000
Bibliografía	----	320.000
TOTAL		6.820.000

Fuente: Autor

10.2 RECURSOS NECESARIOS

Acorde con el presupuesto anterior se presentan los diversos recursos necesarios para desarrollar el estado del arte del proyecto:

Tabla 3 Personal

Participante	Formación	Función	Dedicación (horas)	Dedicación (meses)	Recursos	Total
Martin Camilo Cancelado Ruiz	Ingeniero	Asesor	2 horas/semana	4	UNAD	$6.600.000
Gustavo Marun Suarez	Pregrado	Autor Proyecto	40 horas/semana	4	Propios	$4.800.000
					TOTAL	$11.400.000

Fuente: Autor

Tabla 4 Equipos a adquirir

Equipo	Justificación	Recursos	Total
PC Portátil	Desarrollar pruebas en la red	Propios	$1.800.000
Otros		Propios	$500.000
		TOTAL	$2.300.000

Fuente: Autor

Tabla 5 Equipos a utilizar

Equipo	Justificación	Recursos	Horas Asignación al Proyecto	Total
PC Escritorio	Equipo para realizar consultas	Privados	8 horas / semana	1.280.000
Bases de datos	Bases de datos especializadas	Privados	8 horas /semana	320.000
			TOTAL	1.600.000

Fuente: Autor

Para cada una de las etapas planteadas se detalla el conjunto de actividades a realizar:

10.3 ETAPA 1. EVALUACIÓN DEL ESTADO DEL ARTE ACTUAL DEL SISTEMA CARCELARIO EN COLOMBIA Y ELABORACIÓN DEL PLAN DE TRABAJO.

10.3.1 Metodología: Evaluación de la situación actual de estado de cosas inconstitucional de las prisiones a partir de las sentencias de la Corte Constitucional

Acá podemos ver reflejado el descuido del estado en muchos de los sistemas que hacen parte de su estructura y que se analiza en el marco de las políticas de estado a partir de las sentencias de la Corte Constitucional.

“El estado de cosas inconstitucional decretado por la Corte Constitucional ha tenido varios antecedentes en razón de la vulneración de derechos humanos en Colombia, como es el caso de la población desplazada, concurso de méritos público y abierto para nombrar notarios en propiedad, omisión en el pago de pensiones, y la grave vulneración de derechos de los internos en los establecimientos carcelarios del país. Para ello, ha tenido en cuenta los siguientes factores:

1. La vulneración masiva y generalizada de varios derechos constitucionales que afecta a un número significativo de personas; como el caso de la población interna.

2. La prolongada omisión de las autoridades en el cumplimiento de sus obligaciones para garantizar los derechos.

3. La adopción de prácticas inconstitucionales, como la incorporación de la acción de tutela como parte del procedimiento para garantizar el derecho conculcado.

4. La no expedición de medidas legislativas, administrativas o presupuestales necesarias para evitar la vulneración de los derechos.

5. La existencia de un problema social cuya solución compromete la intervención de varias entidades, requiere la adopción de un conjunto complejo y coordinado de acciones y exige un nivel de recursos que demanda un esfuerzo presupuestal adicional importante.

6. Si todas las personas afectadas por el mismo problema acudieran a la acción de tutela para obtener la protección de sus derechos, se produciría una mayor congestión judicial.

Según el Instituto Rosarista de Acción Social –SERES–, Universidad del Rosario durante muchos años, la sociedad y el Estado se han cruzado de brazos frente a esta situación, observando con indiferencia la tragedia diaria de las cárceles, a pesar de que ella representaba día a día la transgresión de la Constitución y de las leyes. Las circunstancias en las que transcurre la vida en las cárceles exigen una pronta solución. En realidad, el problema carcelario representa no sólo un delicado asunto de orden público, como se percibe actualmente, sino una situación de extrema gravedad social que no puede dejarse desatendida. Pero el remedio de los males que azotan al sistema penitenciario no está únicamente en las manos del INPEC o del Ministerio de Justicia. Por eso, la Corte tiene que pasar a requerir a distintas ramas y órganos del Poder Público para que tomen las medidas adecuadas en dirección a la solución de este problema.

En efecto, tanto el derecho a la dignidad como el de no recibir tratos o penas crueles, inhumanos o degradantes se ven quebrantados por el hacinamiento y las malas condiciones de la estructura física y de servicios públicos que se encuentra en los centros de reclusión; los derechos a la vida y la integridad física son vulnerados o amenazados de manera inminente por el mismo hacinamiento, por la mixtura de todas las categorías de reclusos y por la carencia de los efectivos de guardia requeridos; el derecho a la familia es quebrantado por la sobrepoblación carcelaria y las deficiencias administrativas, condiciones éstas que implican que los visitantes de los reclusos han de soportar prolongadas esperas, bajo las inclemencias del clima, para poder ingresar al centro, y que dificultan en grado extremo las visitas conyugales y familiares; el derecho la salud se conculca dadas las carencias infraestructurales de las áreas sanitarias, la congestión carcelaria, la deficiencia de los servicios de agua y alcantarillado y la escasez de guardia para cumplir con las remisiones a los centros hospitalarios; los derechos al trabajo y a la educación son violados, como quiera que un altísimo porcentaje de los reclusos no obtiene oportunidades de trabajo o de educación y que ***el acceso a éstos derechos está condicionado por la extorsión y la corrupción***; el derecho a la presunción de inocencia se quebranta en la medida en que se mezcla a los sindicados con los condenados y en que no se establecen condiciones especiales, más benévolas, para la reclusión de los primeros.

Colombia, según el WJP, también se situó a la zaga de las garantías de orden y seguridad y el respeto a los derechos fundamentales, y tuvo bajas puntuaciones

entre sus pares regionales en la protección de abusos de agentes estatales y por el caso de las “chuzadas” promovido desde la Casa de Nariño contra periodistas y

líderes políticos […] los sistemas penales de la mayoría de los países de América Latina figuraron entre los peores del mundo. Están afectados por la corrupción.

En materia de política se afirma que: “en el país no ha existido una política penitenciaria y carcelaria dirigida hacia la administración formal de la pena, el tratamiento resocializador, el manejo del hábitat y el control de la seguridad”, enfatizando que la política criminal debe acoger los componentes de prevención, represión y resocialización, y que la política carcelaria se debe orientar hacia el régimen, el fin de la pena, el trato y el hábitat.

Según el documento, para que una política penitenciaria sea efectiva debe contemplar, entre otros, los siguientes aspectos:

• Registro único de detenidos.
• Racionalización de recursos.
• Control de la administración de los centros penitenciarios.
• Mejoramiento de los mecanismos de control y seguridad.
• Capacitación y profesionalización del personal penitenciario.
• Política anticorrupción.

Un punto muy importante que aborda este Conpes es la preocupación por el perfil del funcionario penitenciario, que suele asociarse con la corrupción y el bajo profesionalismo, sumado a la ineficiencia del sistema en materia de seguridad.”[12]

[12] Desarrollo del sistema penitenciario y carcelario colombiano entre 1995 y 2010, en el marco de las políticas de Estado a partir de las sentencias de la Corte Constitucional. Instituto Rosarista de Acción Social –SERES–, Universidad del Rosario. – Bogotá: Editorial Universidad del Rosario, 2011. 322 p.

11 ARTICULOS PERIODISTICOS

11.1 Las modalidades más usadas de extorsión desde las cárceles.

Conocer las modalidades más utilizadas para extorsionar en Colombia Tras la ofensiva de las autoridades contra la extorsión en tres departamentos del país, donde fueron capturadas 55 personas, el Gaula socializó 17 nuevas modalidades que usan los delincuentes para extorsionar a los ciudadanos.

Figura 2: Modalidades más usadas de extorsión

Fuente: Vanguardia liberal Febrero 25 de 2016 las modalidades más usadas de extorsión desde las cárceles. Recuperado de http://www.vanguardia.com

Buenas, para un servicio

Esta extorsión la cometen a empresas de domicilios, de ambulancias o grúas a las que llaman a solicitar un servicio en determinado punto.

Cuando el mensajero sale al servicio recibe otra llamada a decirle que lo están siguiendo, que debe apagar su celular por varios minutos.

Ese tiempo es aprovechado para llamar a la empresa, asegurarle que el empleado ha sido secuestrado y exigir dinero para consignar o entregar de forma exprés.

Feliz ganador

En esta forma de estafa llaman a los celulares o a las casas de las personas para decirles que se han ganado un premio, sea un carro o dinero por el buen uso de una tarjeta de un banco o de un celular.

Muchas veces tienen datos adicionales de la persona -que han recopilado en falsas llamadas de bancos o encuestas- para ganarse su confianza. Entonces, le piden que debe consignar un dinero para el SOAT del carro o impuestos.

Llamada carcelaria

En este caso se identifican como el jefe de un frente guerrillero o banda criminal que está en la cárcel. Citan a su víctima en determinado sitio.

Pero luego de unas horas, antes de la reunión, llaman de nuevo a decirle a su víctima que no pueden asistir a esa cita por combates en esa zona.

Entonces, amenazan a la persona y le piden una colaboración de una determinada cifra de dinero, a cambio de no hacerle daño a ella o a su familia.

Falso alquiler

Crean una página para alquilar inmuebles y utilizan fotografías de sitios que realmente están siendo alquilados en clasificados reales.

En la página falsa anuncian precios especiales y cuando los contactan le piden una consignación de un porcentaje del arriendo de adelanto.

Generalmente, ofrecen apartamentos o casas para vacaciones. Cuando la persona consigna y llama ya no contestan o cambian los números.

Mensajes de whatsapp

Tienen varios tipos de mensajes. En unos se hacen pasar por emisoras o medios de comunicación que anuncian premios.

Para acceder a los premios piden consignar dinero en una cuenta. En el otro caso,

se hacen pasar por bandas sicariales que envían amenazas.

Luego de un tiempo de las intimidaciones, dicen que les pagaron por asesinarlo, pero que pueden negociar y ellos no cometen el crimen.

Redes sociales

Las redes sociales, especialmente Facebook, son una de las herramientas de los extorsionistas para recabar información.
Muchas veces crean perfiles falsos, usando el nombre y la foto de otra persona y le piden a sus contactos ser agregados, de nuevo.

Una vez admitidos ya tienen acceso a las fotografías e información de las personas. En ese momento, aparte de tener los datos, les suben mensajes amenazantes y les exigen dinero.

Investigación judicial

En este caso se hacen pasar por un funcionario judicial, sea policía o fiscal. Le aseguran a su víctima que está a punto de emitirse una orden de captura en su contra, pero que ellos tienen el poder de parar ese proceso.
El extorsionista ha conseguido datos de su víctima y le da detalles puntuales. Además, en ocasiones le dice que lo están siguiendo para generarle terror.
De esta forma, la víctima atemorizada accede a darle dinero.

11.2 Desde cárcel de Santander están extorsionando a profesores de la costa

Figura 3: Cárcel de Palogordo

Fuente: Vanguardia liberal Febrero 29 de 2016 desde cárcel de Santander están extorsionando a profesores de la costa. Recuperado de http://www.vanguardia.com

Según vanguardia (Febrero 29 de 2016) Menciono que desde cárcel de Santander están extorsionando a profesores de la Costa una red de extorsionistas que opera desde la cárcel de Palo Gordo, de Girón, Santander, tenía azotado a los profesores y a los rectores de diferentes instituciones educativas en el departamento de Córdoba, a quienes llamaban a exigir medianas sumas de dinero, aduciendo que de lo contrario atentarían contra sus familias.

Uno de los casos fue denunciado ante las autoridades por la rectora de una institución educativa en Cereté y ello permitió iniciar una investigación que terminó con la captura de una persona que reclamaba el dinero, producto de la extorsión, en el barrio Café Madrid, de Bucaramanga, Santander, cuando recibía la suma de dos millones de pesos.

Se trata de Orlando Calderón Ortiz, quien según la Policía sería la persona encargada de recibir el dinero, producto de la extorsión, mediante llamadas telefónicas que realizaba un interno desde la cárcel. “Una vez se generaba por medio de estas llamadas el temor y la intimidación en la víctima, el capturado procedía a reclamar los giros que enviaban desde el municipio de Cereté como pago de la extorsión”, indicaron los voceros policiales.

El comandante de la Policía Metropolitana de Montería, coronel Jesús Rodolfo Díaz Sezon, señaló que queda una vez más demostrada la efectividad cuando se confía en las autoridades y por ello invitó a la ciudadanía para que en vez de pagar denuncie. “Recordamos que para este tipo de casos se encuentra disponible la línea gratuita de emergencias 165, donde recibirán todo el apoyo y orientación necesaria”, puntualizó.

12 ETAPA 2: ESTADO DEL ARTE DE LAS TECNOLOGÍAS DISPONIBLES, ANÁLISIS Y CONCLUSIONES.

12.1 Estado del arte de las tecnologías 3G y 4G:

12.2 Artículos:

12.2.1 Revista IEEE:

Modelado de carga útil, y la detección de anomalías. Un modelo de carga de seguridad impulsada por los ataques de inundación en las redes activas. (2009)

Los autores P.Jayashreel, K.S.Easwarakumar 2, D.Radhakrishnan, N.Lakshmanan, P.Dinakaran

Este articulo trata sobre la comparación del crecimiento de internet en el mundo entero y a su vez el crecimiento de los ataques de denegación de servicios Ddos a nivel mundial, tanto así que los investigadores se han puesto en la tarea de desarrollar formas de mitigar estos ataques. Un número de dispositivos de seguimiento y de filtrado se han desarrollado para verificar la autenticidad de los paquetes basados en los datos de carga útil de paquetes en sistemas de detección de intrusiones (IDS).

Actualmente, la mayor parte de los ataques DDoS tienen como meta sacar ventaja monetaria y son financiados por criminales cibernéticos organizados. También hay ofensivas en la infraestructura y en las aplicaciones, con una variedad de técnicas utilizadas: volumétricas, multivectoriales, de fragmentación, protocolo de recursos y conociendo el IMSI (*Identidad Internacional del Abonado a un Móvil*). Es posible realizar un ataque selectivo ya que este código de identificación es único para cada dispositivo de telefonía móvil integrado en la tarjeta SIM y permite su identificación en redes GSM y UMTS, etc.

Capacidad de carga en base a detección de anomalías:

El cuerpo de un paquete contiene un conjunto de caracteres. Es diferente de la cabecera del paquete, la carga útil de un paquete de red no tiene un formato uniforme. Cualquier personaje puede aparecer en la carga útil en cualquier posición en la carga útil. Incluso entonces, modelando el algoritmo de formación de la matriz de carga útil en un ataque DDoS asume importancia como la carga útil del paquete de ataque tendrá algunos patrones de carga útil en común con los hechos por las de los paquetes de ataque conocidos y de la misma manera, la

carga útil del paquete legítimo coincidirá con los de los conocidos paquetes legítimos.

También en el campo de la piratería informática de hoy en día, se convierten en los contenidos de cabecera altamente falsificados y, por tanto, no se puede creer por completo.

Por lo tanto el modelado de la carga útil se convierte en inevitable. Al encontrar el patrón (s) específico de la carga útil en una pequeña la duración, la detección de anomalías del éxito puede ser llevada a cabo.

La detección de anomalías llevado a cabo aquí consta de dos pasos.

1) la búsqueda de los patrones

2) Realización de patrones en comparación.

12.2.2 **Revista Técnica de la Empresa de Telecomunicaciones de Cuba Gestión de redes y servicios NGN/4G. (2012)**

En su artículo Guzmán Quintero, Yoandi. *Tono* trata sobre la seguridad de la información y la seguridad de la red que entre las dos juegan un papel muy importante en cuanto a la integridad de las comunicaciones la transferencia de los datos y la inmunidad de los recursos, incluidas las redes y los servidores que proporcionan los servicios. El ambiente de la red 4G está diseñado para garantizar una red de acceso generalizado con la inclusión de las nuevas interfaces radioeléctricas, basada en una infraestructura común completamente IP, flexible y sin fisuras, que soporte la escalabilidad y la Movilidad.

En ese sentido es prioritario que el usuario sea el centro de atención sobre el cual girará la tecnología, por lo que las alterativas móviles e inalámbricas deberán estar centradas en los servicios destinados a cubrir sus necesidades.

Gestión de rastreo del terminal: la gestión de trazas del terminal es importante para detectar y rastrear los terminales robados o falsificados, que son actualmente uno de los problemas más grandes que experimentan los proveedores de servicio. Cuando los terminales son utilizados ilegalmente por alguien, a excepción del dueño, se puede emplear esta característica para rastrearlos.

La gestión de rastreo del terminal se puede utilizar también para medir el funcionamiento entre un terminal y un servidor de prueba dentro de la red. Estos datos son una fuente adicional a la información de supervisión del rendimiento de la infraestructura y permiten entrar a un nivel más detallado en operaciones de supervisión y optimización.

Camino a la cuarta generación:

Aun cuando está empezando el lanzamiento comercial de las redes móviles de tercera generación, basadas en la tecnología UMTS—Universal Mobile Telecommunications System—, ya se vislúmbrala próxima generación, cuyas principales características podrían resumirse en núcleo IP, ubicuidad y servicios. En primer lugar, se basan en un núcleo IP encargado de ofrecer el transporte en la red y sobre esta base se edificarán los servicios tradicionales, así como los nuevos, para los que tendrán que ser implementados conceptos novedosos como QoS y AAA. Finalmente, el acceso heterogéneo a través de cualquier medio, ya sea fijo o móvil, con un único terminal ofrecerá una mayor conectividad al usuario 4G no es un estándar ni una tecnología definida como las anteriores, sino una colección de tecnologías y protocolos para permitir el máximo rendimiento de procesamiento de la red inalámbrica adecuada en cada momento. La convergencia de dichas tecnologías surge de la necesidad de agrupar los diferentes estándares en uso con el objetivo de delimitar el ámbito de funcionamiento de cada uno de ellos y, también, de integrar todas las posibilidades de comunicación en un solo dispositivo de forma transparente al usuario. El WWRF -Wireless World Research Forum- define 4G como una red que funciona con la tecnología de Internet, combinándola con otros usos y tecnologías como Wi-Fi -Wireless Fidelity- y WiMAX. Cuando el sistema utilice una red móvil como UMTS, la comu- nicacion alcanzara una velocidad de OOMbps que puede aumentar hasta I Gbps en aquellas situaciones en las que sea posible utilizar una red de área local como Wi-Fi para establecer dicha comunicación. En resumen, el sistema 4G debe ser capaz de compartir dinamicarnente y utilizar los recursos de red que economicen los requerimientos del usuario 4G.

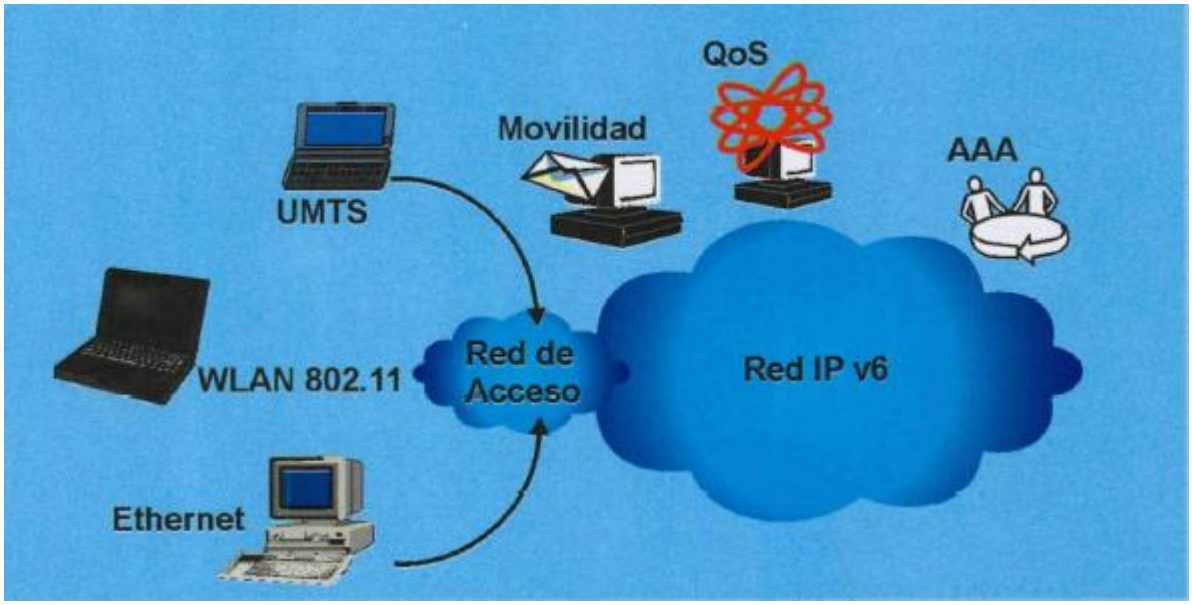
A todo lo dicho hasta el momento se puede afeador que, de acuerdo con los grupos 4G, las infraestructuras y los terminales deberán implementar al menos todos los estándares desde el 2G hasta el 3G, aunque la estructura se basara solo en paquetes IP. Algunos de los estándares fundamentales para 4G son WiMAX, WiBro -Wireless Broadband- y 3GPP LTE -Long Term Evolution. Para poder hacer realidad esta red 4G es necesario no solo integrar las tecnologías existentes, también hacer uso de nuevos esquemas de modulación o sistemas de antenas que permitan la convergencia de los sistemas inalámbricos.

El punto más atractivo de la 4G es la integración de las redes, con lo que desaparecería la frontera entre una red y otra, lo cual beneficia a los usuarios ya que tendrán una conexi6n permanente *-always on-,* sin notar que durante su movilidad cambian constantemente las tecnologías de acceso, y adoptan la que le brinda mayor QoS en el momento. De este modo, el usuario tendrá servicios en cualquier sitio a cualquier hora y se espera que a un costo accesible que permita el progreso a estas tecnologías.

Elementos funcionales de una red 4G

En un escenario 4G aparecen diferentes tecnologías de acceso, las cuales serán complementarias de manera que todas puedan coexistir y, en funci6n de sus necesidades, el cliente podrá optar por alguna de ellas. Por ejemplo, UMTS, CDMA.

Figura 4: Arquitectura de la red 4G



Fuente: Revista Técnica de la Empresa de Telecomunicaciones de Cuba

2000, IEEE 802.11, 802.16 y Ethernet. En la siguiente figura se representan los elementos funcionales que integran una red 4G.

Los elementos más representativos de esta red son la calidad del servicio, la autentificación, la autorización, la contabilidad y la movilidad: QoS: La tecnología IP como se concibió originalmente no ofrece garantías de calidad. Sin embargo, existen servicios, entre ellos el telefónico, con rigurosos requisitos de retardo y variación del retardo (Jitter), lo que hace necesario añadir funcionalidad a IP para que las redes basadas en dicho protocolo sean capaces de soportar este tipo de

servicios [5]. Para lograrlo, el modelo se basa en el uso de un elemento encargado de la gestión de calidad de servicio, llamado QoS Broker, que es el corazón del sistema de prestación de calidad de servicio en el entorno. Su principal función consiste en tomar las decisiones relativas al control de admisión, además de realizar las funciones de configuración de los dispositivos de la red, como routers de acceso y los AAAC. AAAC: Las nuevas redes deberán contar con un sistema de autenticación y autorización para ofrecer formas seguras de identificación y acceso de usuarios. En este sentido, el sistema AAAC está encargado de comprobar la identidad de los usuarios, de controlar los servicios que se usan y facturarles por ello. Estos sistemas utilizan las redes IP para transportar la información de señalización necesaria.

Movilidad: Las redes de 4G deberán soportar mecanismos eficientes que permitan la movilidad de usuarios que, aunque utilicen el mismo o distinto terminal, se conecten a la red mediante diferentes redes de acceso —WCDMA, WLAN, Ethernet, etc. operadas por distintas entidades. Esto requiere mecanismos que soporten traspasos (handovers) entre subredes con igual o desigual tecnología traspaso horizontal y vertical— de forma eficiente y que tengan como elemento Común el transporte IP. La base del soporte de movilidad en redes IPv6 es el protocolo Mobile IPv6

Gestión del terminal

Las terminales gestionadas requieren dos subzonas, una nombrada gestion de localizaci6n de! terminal y, la otra, gestión de negocio del terminal. La gestión de! terminal existe en las redes 3G y esta característica continuara siendo necesaria, quizás con mayor énfasis, en las redes 4G.

Desde el punto de vista del terminal, el proceso de integraci6n requiere considerar aspectos de desafío como:

Terminal multimodo: el terminal necesita soportar distintas interfaces, una para cada tecnología de red de acceso.

Terminal adaptable y reconfigurable: este debe implementar técnicas de radio definido por software -Software Defined Radio (SDR), el soporte de mecanismos de transmisi6n adaptables, etc.

Además debe considerar los siguientes requisitos:

Soporte de múltiples modos de conexión: la conectividad a diferentes tipos de redes de acceso debe ser posible desde un único terminal.

Adaptabilidad y reconfiguración: la modificación expedita de las 16 gigas de las distintas capas de la arquitectura del terminal debe ser posible para facilitar la reacción apropiada ante violaciones de la QoS concertada para las sesiones activas. Descubrimiento de redes de acceso y asociación: esta funcionalidad es indispensable en un entono heterogéneo de redes inalámbricas. La difusión periódica de servicios de conexi6n realizada por los puntos de acceso de las redes móviles actuales puede ser poco eficiente en este escenario. Se propone el uso de canales para anuncio inalámbrico Wireless Billboard Channels a través de los cuales el terminal puede detectar, seleccionar y registrarse a las distintas redes de acceso disponibles independientemente de su tecnología de radio.

También se puede decir que se evidencian dos zonas específicas descritas a continuaci6n.

La gestión de localización del terminal: la información de localización del terminal puede ser utilizada para tomar las decisiones relacionadas con la QoS

Por las operaciones y el sistema de gestión, cuando un usuario desea utilizar un servicio y cierto requisito de QoS ha sido solicitado. Puede también ser utilizado cuando un traspaso es necesario y cuando se desea proporcionar un servicio de valor afligido.

Gestión de rastreo del terminal: la gestión de trazas del terminal es importante para detectar y rastrear los terminales robados o falsificados, que son actualmente uno de los problemas más grandes que experimentan los proveedores de servicio. Cuando los terminales son utilizados ilegalmente por alguien, a excepción del dueño, se puede emplear esta característica para rastrearlos. La gestión de rastreo del terminal se puede utilizar también para medir el funcionamiento entre un ter- minal y un servidor de prueba dentro de la red. Estos datos son una fuente adicional a la información de supervisión del rendimiento de la infraestructura y permiten entrar a un nivel más de- tallado en operaciones de supervisión y optimización. Las trazas, además, pueden desempeñar un papel clave en actividades como la determinación de las causas de! mal funcionamiento de un terminal, la investigación de averías avanzadas, la optimización de! uso del recurso y su calidad, la mejora de la capacidad, y el análisis de la caída de una Hamada. En Cuba esta implementa- do un mecanismo de lista negra que, una vez declarado por el usuario la pérdida o robo, automáticamente su línea pasa a formar parte de esta lista, al igual que el móvil si está anclado.

12.3 Revista IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008

Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN (2008)

Según Juan Antonio Guerrero, Antonio Barba Martí El incremento en la demanda de servicios de comunicaciones inalámbricos avanzados ha hecho que los recursos que actualmente proporcionan los sistemas celulares. Móviles avanzados sean insuficientes. La integración de las redes celulares de tercera generación (3G) y las redes de área local inalámbrica (WLAN) es una solución prometedora hacia la migración de las redes de comunicaciones móviles de cuarta generación. Esta integración intenta explotar las bondades de cada una de las tecnologías y utilizarlas de forma complementaria. Sin embargo, la integración transparente de diferentes tipos de tecnologías genera un conjunto de nuevos retos relacionados a su operación y gestión, tales como gestión del acceso, autenticación, autorización, tarificación, movilidad y asignación de recursos, entre otros. Los modelos de gestión de red tradicionales están principalmente enfocados en el monitoreo y no en el control, y por lo tanto no se pueden cubrir las necesidades de este nuevo entorno de red heterogéneo. La gestión de red basada en políticas se presenta como una solución viable a estos nuevos retos. Esta tecnología de gestión está enfocado en la generación de un entorno de gestión de red autónomo que permita la operación de los recursos de red mediante la definición de una serie de reglas que dinámicamente configuradas puedan alcanzar ciertas metas y reaccionar en forma automática a los diferentes entornos de operación.

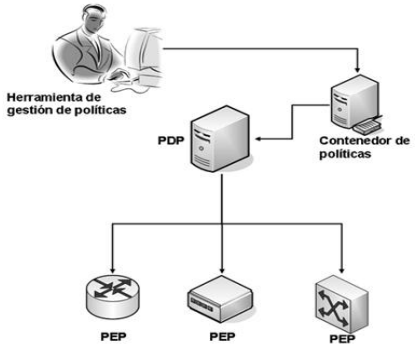
En este artículo se propone un sistema de gestión de red basado en políticas para un ambiente integrado 3G-WLAN y centrado en la gestión de acceso y recursos, control de admisión y tarificación de servicios basados en las preferencias del usuario.

La integración de las redes celulares con las redes Wi-Fi ha sido un punto de investigación en los últimos años. Algunos esfuerzos han sido dirigidos a solucionar el problema de la interconexión de las dos arquitecturas, para lo cual han propuesto modelos de interconexión dependiendo de los diferentes dominios de gestión disponibles. Con respecto al uso de la gestión basada en políticas dentro del entorno integrado 3G-WLAN se han hecho esfuerzos por resolver problemas específicos como son: control de la movilidad y traspasos, los cuales basan sus decisiones en políticas que evalúan las preferencias del usuario y condiciones de la red. Sin embargo, desde el punto de vista del entorno, los requerimientos de servicio deben ser evaluados para un mejor control de selección de traspaso. Con respecto al control de acceso, la gestión basada en políticas ha sido implementada para una gestión de control de acceso más flexible. Uno de los problemas de la gestión de entornos integrados en los que se ha propuesto con mayor auge el uso de la gestión basada en políticas es el control de la calidad de servicio (QoS) extremo a extremo. La referencia [10] muestra una arquitectura de

gestión basada en políticas para proveer un control QoS consistente sobre un sistema integrado UMTS-WLAN, pero solamente se enfoca a la ubicación adecuada de las entidades de gestión basada en políticas y los flujos de comunicación de las entidades y no en la definición de las clases de políticas a ser implementadas. Existen ejemplos de soluciones basadas en políticas para redes inalámbricas, pero el enfoque que le dan es el control desde el lado del operador de la red, sin tomar en cuenta las preferencias del usuario. Nuestra propuesta es la generación de una arquitectura de gestión de red enfocada a la gestión de acceso, recursos, movilidad y tarificación para un ambiente integrado 3G-WLAN que permita seleccionar la celda adecuada, asignar recursos para lograr un mejor equilibrio de red y tarificar el uso de los servicios usados por los clientes basados en sus requerimientos de nivel de servicio y en las condiciones de red actuales.

Elementos principales de un modelo de gestión de red basado en políticas:

Figura 5: Elementos principales de un modelo de gestión de red basado en políticas



[Fuente] IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Elementos principales de un modelo de gestión de red basado en políticas. Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN

Las políticas a ser aplicadas en cada uno de los elementos gestionados son seleccionadas por un elemento intermediario conocido como Punto de Decisión de Política (PDP – Policy Decisión Point), el cual se comunica con el PR mediante algún protocolo como LDAP[13] y es responsable de Interpretar las políticas almacenadas en el PR y proporcionar respuesta a las peticiones realizadas por el PEP.

El PDP es el elemento principal de la arquitectura definida por el IETF y se encarga de desempeñar tres tareas básicas: realizar la consulta de las políticas existentes en el contenedor, llevar a cabo la traducción de cada política al formato específico del dispositivo y distribuirlas a los PEPs de acuerdo a las peticiones

[13] Protocolo Ligero/Simplificado de Acceso a Directorios

realizadas. La comunicación entre el PDP y el PEP se lleva a cabo mediante el protocolo COPS (Common Open Policy Service).[14]

UMTS

La tecnología celular UMTS (Universal Mobile Telecommunications System) es el sistema de telecomunicaciones móviles de tercera generación (3G) que proporciona a usuarios móviles dos tipos de servicios de comunicaciones: servicios de paquetes (PS - Packet Switched) para aplicaciones de datos y servicios de conmutación de circuitos (CS - Circuit Switched) para aplicaciones de voz y telefonía.

La infraestructura de UMTS está lógicamente dividida en un núcleo de red (CN - Core Network) y una red de acceso (AN - Access Network). UMTS hace uso del General Packet Radio Service (GPRS) para ofrecer el servicio de paquete de datos. Una red UMTS en el dominio de paquetes se compone de diferentes elementos de red (Fig. 6). El Núcleo de Red es la parte por la que UMTS se conecta con otras redes de telecomunicaciones. El núcleo está formado por dos elementos claves: Serving GPRS Support Node (SGSN) y Gateway GPRS Support Node (GGSN). UMTS Terrestrial Radio Access Network (UTRAN) proporciona la conexión entre los terminales móviles y el CN[15]. Se compone de un conjunto de controladores de red conocidos como RNC (Radio Network Controller) y una serie de Nodos B o estaciones base conectados a los RNC. El terminal móvil es el equipo del usuario (UE - User Equipment)[16] que le permite acceder a los servicios de red.

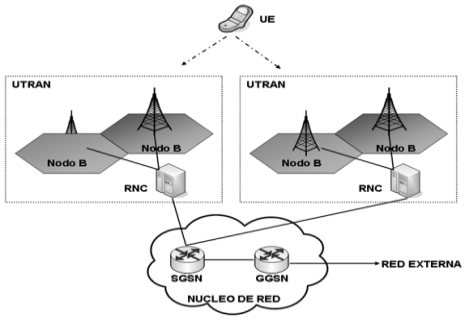
Elementos principales del dominio de paquetes de la arquitectura umts.

[14] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, "The COPS (Common Open Policy Protocol)", RFC 2748, IETF, Jan.2000.

[15] Núcleo de red.

[16] Equipo móvil del usuario

Figura 6: Elementos principales del dominio de paquetes de la arquitectura UMTS



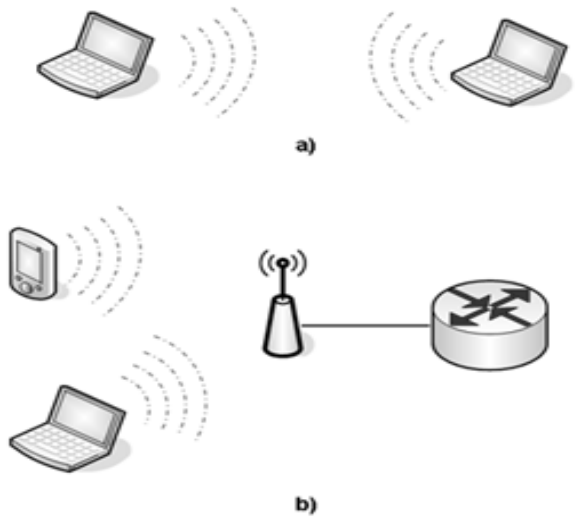
[Fuente] IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Elementos principales del dominio de paquetes de la arquitectura UMTS. Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN.

El protocolo IEEE 802.11 [26] o Wi-Fi es un estándar de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura del modelo OSI (capas física y de enlace de datos) especificando sus normas de funcionamiento en una WLAN. Esta tecnología ofrece dos formas de configuración de este entorno de comunicaciones inalámbrico. La configuración más básica es la llamada de igual a igual o ad-hoc y consiste en una red de dos terminales móviles equipados con la Correspondiente tarjeta adaptadora para comunicaciones inalámbricas. En el modo infraestructura existe un dispositivo denominado punto de acceso (AP - Access Point) que coordina la transmisión entre nodos dentro de su área de cobertura. Un nodo móvil se asocia a un solo AP.

ESCENARIOS DE INTERACCIÓN UMTS/WLAN

Desde hace pocos años se ha estado trabajando en la estandarización del entorno integrado WLAN-3G en lo que se conoce como Interworking. Este nuevo ambiente define la arquitectura y mecanismos para control de red integrado, la conectividad a nivel de red y los aspectos de autenticación, autorización y tarificación. El ETSI (European Telecommunications Standards Institute) comenzó parte del trabajo con la propuesta de integración de HIPERLAN/2 con UMTS. El estudio de integración de la tecnología WLAN al entorno de las redes móviles ha continuado en el foro de 3GPP, responsable de la especificación del sistema UMTS.

Figura 7: Configuraciones 802.11. a) Modo ad-hoc. b) Modo infraestructura



[Fuente] IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Configuraciones 802.11. a) Modo ad-hoc. b) Modo infraestructura. Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN

Como parte del trabajo, 3GPP introdujo el concepto WLAN Interworking (WLAN-I) como una nueva funcionalidad en su especificación Release 6. 3GPP realizó un estudio sobre la factibilidad de interconexión de sistemas UMTS con WLAN. La idea al interconectar estas tecnologías es ampliar los servicios de UMTS al ambiente WLAN para que sea visto como una tecnología complementaria para UMTS.

A continuación se presentan 6 posibles escenarios de interacción donde se describen entre las dos tecnologías que van desde un simple esquema de acoplamiento de facturación hasta un nivel más complejo en el cual el usuario puede moverse entre las dos redes en una forma ininterrumpida, mientras mantiene una comunicación activa.

Escenario 1: Es el esquema más simple de interconexión entre UMTS y WLAN. No requiere de una interconexión específica entre las dos tecnologías y solamente se limita aunificar los procedimientos de facturación y atención al cliente.

Escenario 2: En este escenario se especifica que los procedimientos AAA (Authentication, Authorisation and Accounting) aplicados en WLAN son los mismos que se aplican en la red 3G.

Escenario 3: El objetivo de este escenario es extender el acceso a los servicios de paquetes de la red 3G a los subscriptores en un ambiente WLAN. Sin embargo

no se especifica que se deba de garantizar la continuidad del servicio durante un proceso de transferencia de la conexión entre UMTS y WLAN.

Escenario 4: La meta de este escenario es permitir a los servicios del escenario anterior tener continuidad ante un cambio de acceso entre WLAN y 3G. El cambio es notable para el usuario, pero no requiere de restablecimiento del servicio. Puede haber un cambio en la calidad del servicio debido a las diferentes capacidades de las tecnologías.

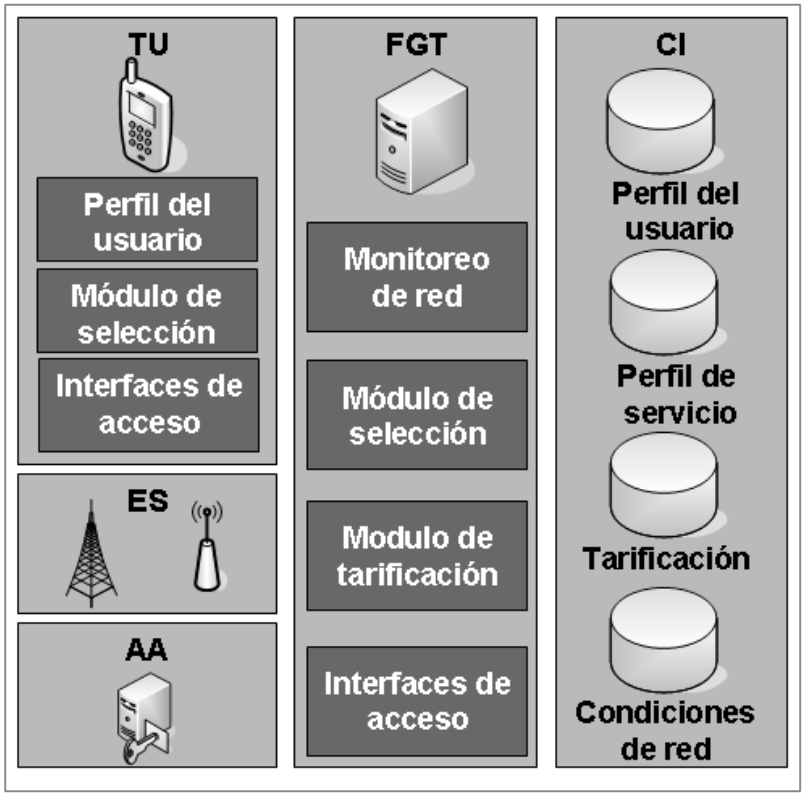
Escenario 5: Su meta es la continuidad del servicio de forma ininterrumpida entre las tecnologías de acceso 3G y WLAN. La continuidad del servicio se entiende como la minimización de aspectos tales como pérdida de paquetes durante el intercambio entre tecnologías de acceso.

Escenario 6: La meta de este escenario es permitir el acceso a los servicios que se ofrecen en el dominio de CS desde el ambiente WLAN.

Arquitectura de gestión propuesta

Con la creación de nuevos entornos integrados como UMTS-WLAN ha surgido la necesidad de una arquitectura para llevar a cabo la gestión adecuada de este nuevo entorno de red. El presente trabajo propone la implementación de una arquitectura de gestión basada en políticas para un ambiente integrado 3G-WLAN que tome en cuenta las preferencias de los usuarios y los operadores de red. La arquitectura de gestión basada en políticas está formada por un conjunto de entidades funcionales que desempeñan una serie de acciones específicas para el proceso de gestión del entorno 3G/WLAN como se muestra en la Fig. 8. La entidad TU (Terminal del Usuario) representa el dispositivo del usuario final. El TU está formado por un módulo de decisiones de políticas y un perfil del usuario que almacena la información relacionada a su contrato de servicio (SLA Service Level Agreement) establecido con su operador doméstico, un perfil de conexión del usuario (PCU) que almacena un registro del historial de conexión del usuario, y un conjunto de políticas de preferencias usadas para el proceso de selección de la celda de acceso.

Figura 8: Entidades funcionales de la arquitectura de gestión basada en políticas.



[Fuente] IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Entidades funcionales de la arquitectura de gestión basada en políticas. Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN

La entidad ES (Entidad de servicio) es el componente que proporciona al usuario un servicio específico. Esta entidad puede ser un servidor de acceso a la red (NAS), un servidor Proxy SIP, un servidor de aplicación, etc. La entidad AA es la responsable de llevar a cabo el proceso de autenticación y autorización de los usuarios mediante una serie de políticas de control de acceso definidas. El FGT es el componente principal de la arquitectura digestión. Esta entidad es responsable de realizar tres funciones principales para el proceso de gestión del entorno de comunicaciones: la función de monitoreo usada para colectar información relacionada a las condiciones actuales de las celdas de acceso; la función de gestión del acceso, que es la responsable de desempeñar el control del acceso de las diferentes peticiones recibidas mediante el módulo de selección; finalmente, la función de tarificación, que desempeña el proceso de medición de los recursos utilizados por el usuario para la tarificación final de los usuarios.

El control de esas funciones se realiza mediante una serie de políticas definidas. Por último, la entidad Contenedor de Información (CI) es la responsable de almacenar toda la información relacionada con los diferentes procesos de la arquitectura de gestión. El CI almacena información sobre el perfil del usuario y los perfiles de los diferentes servicios ofrecidos. Además almacena la información de los registros de tarificación y las condiciones de red recopilada por la función de monitoreo.

Por otro lado, se define un esquema de políticas para el proceso de gestión del entorno integrado. El esquema está formado por 5 niveles de políticas como se muestra en la Fig. 9.

Los niveles definidos dentro del esquema van desde el más simple, que consiste en control de tarificación, hasta el más complejo donde se aplican políticas para el proceso de control de movilidad del usuario entre las dos tecnologías y la negociación de nivel de servicio, con lo cual se intentan cubrir los primeros cinco escenarios definidos por el 3GPP.

Políticas de tarificación: Son las políticas definidas para configurar adecuadamente el proceso de tarificación. Las políticas se aplican mediante un servidor de políticas localizado en el dominio de gestión. Estas políticas son aplicadas durante el proceso de tarificación, en el cual cada uno de los dominios realiza el control y reporta un resultado.

Políticas de monitoreo: Las políticas de este nivel se definen para configurar adecuadamente los procesos de control de recursos utilizados por el usuario. Estas políticas se aplican cuando el usuario se autentica y recibe la autorización del servicio y son implementadas por cada uno de los dominios de acuerdo al tipo de servicio.

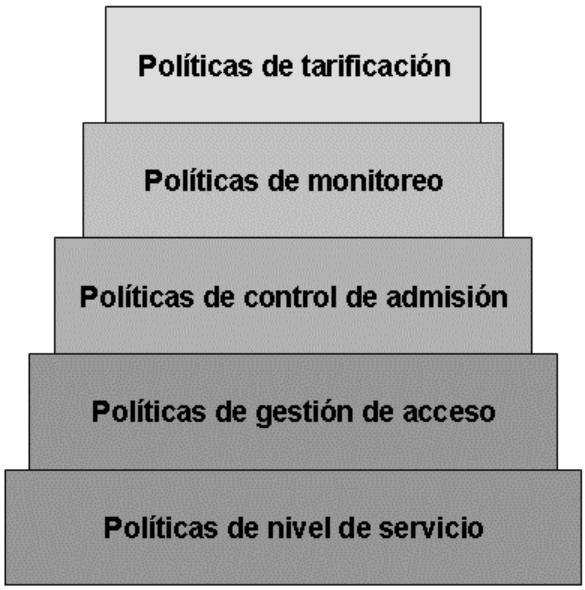
Políticas de control de admisión: Son las políticas que definen las características que tendrá la conexión del usuario basado en su perfil. Entre ellas están las de limitación del ámbito de acceso (derechos para acceder a los diferentes dominios), control de recursos y prioridades del usuario.

Estas políticas se aplican cuando el usuario se autentica y recibe la autorización del servicio.

Esquema de políticas propuesto para el ambiente integrado umts-wlan

Podemos ver en los siguientes esquemas de los elementos de la red la diferencia existente entre la gestión de la red basado en políticas vs dominio de paquetes de la arquitectura UMTS:

Figura 9: Esquema de políticas propuesto para el ambiente integrado UMTS-WLAN. Arquitectura de referencia de gestión de red basada en políticas para un entorno Integrado 3G-WLAN

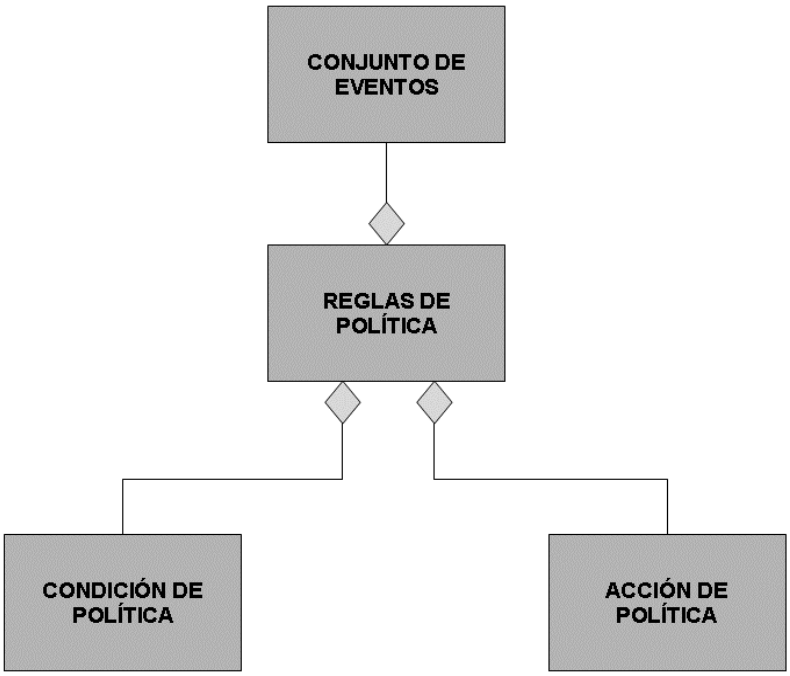


IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Esquema de políticas propuesto para el ambiente integrado UMTS-WLAN [Fuente] Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN.

Según la IEEE latín américa transactions, vol. 6, no. 2, june 2008 es una gestión basada en políticas, una política es un conjunto de directivas o reglas especificadas por el administrador para gestionar ciertos aspectos de los resultados deseados de las interacciones entre usuarios, entre aplicaciones, y entre usuarios y aplicaciones. Las políticas proporcionan las guías para especificar cómo los diferentes elementos de red, por ejemplo enrutadores, conmutadores, Servidores, cortafuegos, deberían manejar el tráfico generado por los diferentes usuarios y aplicaciones. Cada política está formada, como mínimo, por una cláusula de condición y una cláusula de acción. Si la cláusula de condición es verdadera entonces las acciones definidas en la cláusula acción son ejecutadas.

Representación de los bloques para un modelo de políticas simple

Figura 10: Representación de los bloques para un modelo de políticas simple. Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN



IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008 Esquema de políticas propuesto para el ambiente integrado UMTS-WLAN [Fuente] Recuperado: Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN.

Palabras clave— 3G, traspaso, gestión, políticas, UMTS, WLAN, inalámbrico, QoS, 802.11.

12.3.1 Performance Analysis of UMTS Handover with the Help of WLAN

Proceedings of the 2nd Int'l Conf. on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine'05) 0-7695-2423-0/05 $20.00 © 2005 IEEE (2005)

Los autores de este articulo Danyan Chen, Xiaofeng Wang, and A. K. Elhakeem afirman que Las redes móviles 3G permiten la transmisión tanto de datos como de voz y los abonados a la telefonía celular dependen de la cobertura de red de cada operador al cual están suscritos y de los costos de comunicación establecidos por cada proveedor de servicios y verificados por la Comisión de Regulación de Telecomunicaciones (CRC).

Gracias a la conectividad de voz sobre IP nace una alternativa en la realización de llamadas de voz, aprovechando las características de redes como lo son 3G y WiFi, brindando la posibilidad de establecer conexiones de voz no solo por medio de redes de telefonía, sino también a través de redes de datos, incluyendo las redes celulares.

Las redes 3G permiten la movilidad de los usuarios por la conmutación entre celdas, siendo dependientes del radio de cobertura de cada una de las bases de transmisión (BTS1), con la ventaja que la distancia entre una y otra base permite mantener la conexión mientras el usuario está en movimiento. Las redes WiFi por su parte tienen un alcance limitado al radio de cobertura de la red inalámbrica propagada por dispositivos tales como Routers y Access Points, pero a diferencia de las redes 3G y las tarifas por consumo ofrecidas por los proveedores, las redes WiFi en la mayoría de los casos brindan conectividad y transferencia de datos ilimitada con costos de tarificación fijos.

Ahora bien, conociendo ambas redes de comunicaciones podemos obtener conexión de voz tanto por las redes celulares 3G como por las redes WiFi haciendo uso de servicios VoIP. Gracias a esto es posible conmutar una llamada previamente establecida por una u otra red sin perder la conectividad de la misma, pero este servicio no está disponible para los usuarios a través de los operadores celulares en Colombia, desaprovechando la capacidad de la interoperabilidad entre redes.

El Protocolo de Inicio de Sesiones (SIP, por sus siglas en inglés) nace como un protocolo de comunicaciones IP, encargado del control y señalización de mensajes a través de la red, desarrollado por la IETF2 y definido en el RFC 3261 como el estándar para la iniciación, modificación y terminación de sesiones interactivas de usuario donde intervienen elementos multimedia como video, voz, mensajería instantánea, juegos en línea y realidad virtual. SIP es un protocolo de

control (señalización) bajo el modelo Cliente – Servidor, que opera de la forma 'request – response' y basa su funcionamiento en el registro de los usuarios en el servidor, identificándose de la forma usuario@dominio. Gracias a la funcionalidad que brinda el protocolo SIP de realizar el registro de los usuarios en un servidor, se abre la posibilidad de utilizar ventajas como la modificación de las características de la comunicación mientras ésta se encuentra en progreso [3]. Esto nos permite por ejemplo, poder cambiar el identificador de los usuarios en el servidor, en este caso la dirección IP con la cual se han registrado, para de esta forma brindar la capacidad a un dispositivo de tener movilidad entre redes 3G y WiFi (Vertical Handover3).

12.3.2 Revista IEEE: Policy Routing Architecture for IP Flow Mobility in 3GPP's Evolved Packet Core (2010)

Los autores P. Loureiro, M. Liebsch, S. Schmid en su artículo comentan que Según la mayoría de las predicciones, inalámbricas de cuarta generación se componen de redes heterogéneas. Dos importantes redes constituyentes serian inalámbricas.

LAN (WLAN) y los sistemas celulares de radio móvil (por ejemplo, UMTS). WLAN está diseñado para los de rango bajo, alto / medio acceso a velocidad de datos y se puede utilizar como un complemento de sistemas móviles celulares más grandes de radio. En este trabajo,

Considerar un sistema heterogéneo en el que las WLAN son construidas en los límites de las células UMTS con puntos calientes para proporcionar ancho de banda adicional y para apoyar traspaso entre células celulares. El celular reserva de ancho de banda para el traspaso y la nueva llamada en cola se considera. Se demuestra que tal sistema integrado puede ser modelado por una discreta 3-DCadena de Markov. El uso de este modelo de análisis, la entrega y el nuevo bloqueo de llamadas, con la probabilidad significa cola de retardo se encuentran bajo diversos parámetros del sistema. Estos resultados nos permiten entonces no sólo para cuantificar la ganancia de rendimiento de integración de sistemas, sino también para optimizar los parámetros del sistema.

La 3rd Generation Partnership Project está especificando soluciones para la movilidad flujo IP, que permiten a los flujos de datos IP siendo enrutada entre un terminal móvil y la infraestructura a través de una 3GPP y sistemas de acceso no-3GPP, por ejemplo, sobre LTE y WLAN. Conectividad a través de los diferentes sistemas de acceso se proporciona basa en el concepto de una única conexión de red de datos de paquetes compartida.

Con el fin de permitir la movilidad flujo IP, el terminal móvil debe ser capaz de identificar los flujos de datos individuales y tomar enrutamiento decisiones en el enlace ascendente. El anclaje de movilidad terminal móvil, el PDN Gateway, en el Evolved Packet Core requiere la funcionalidad equivalente para el enlace descendente. Sincronización y cambios dinámicos en estas políticas de enrutamiento de flujo, iniciaron ya sea por el terminal móvil o el operador móvil, implicaría técnico desafíos, en particular para la gestión de la movilidad basada en la red según el protocolo Proxy Mobile IPv6, lo cual NO considerar la señalización relacionada con la movilidad entre un terminal móvil y la infraestructura de red. En este trabajo se propone una solución para la movilidad flujo IP, que reutiliza la Política y de carga Sistema de control de la 3ª Generación Asociación Proyecto de núcleo de paquetes. La flexibilidad y la eficiencia del enrutamiento propuesto.

Aplicación de configuración de Política de funciones, lo que representa un parte integral de la política y la carga del sistema de control, que analizaron y discutieron sobre la base de casos de uso existentes y nuevos.

La tercera Generación del Proyecto Socio Generación (3GPP) comenzó para estudiar y normalizar soporte para multi Paquete de Acceso. Los datos de conectividad de red y Movilidad flujo IP (MAPIM) permitiendo un terminal móvil para distribuir una solo Paquetes de Datos Red (PDN) la conexión a través de un sistema de acceso de 3GPP, tales como LTE, y unos sistemas de acceso no 3GPP, como WLAN. Esta funcionalidad permite a los terminales móviles, que puede conectar a la infraestructura de red de forma simultánea a través de múltiples tecnologías de radio, para enviar y recibir datos a través de los flujos ya sea la tecnología y, por tanto, seleccione el que el acceso a utilizar para flujos individuales. la movilidad flujo IP requiere un cambio dinámico en el encaminamiento de política en el anclaje de movilidad (es decir PDN Gateway) a la entrega de un flujo de un acceso a otro sin acceso a romper la sesión de datos. Para la movilidad flujo IP, el móvil terminal debe mantener una regla de política de enrutamiento para el tráfico de enlace ascendente, mientras que la pasarela PDN debe mantener una regla de política de encaminamiento para tráfico de enlace descendente hacia el terminal móvil. De acuerdo a requisitos 3GPP, el control sobre las reglas de política de encaminamiento de flujo debe estar habilitado para ambos, el terminal móvil y el móvil operador; Sin embargo, los casos de uso definidos en la actualidad se centran principalmente en el control de terminal móvil para la movilidad flujo IP.

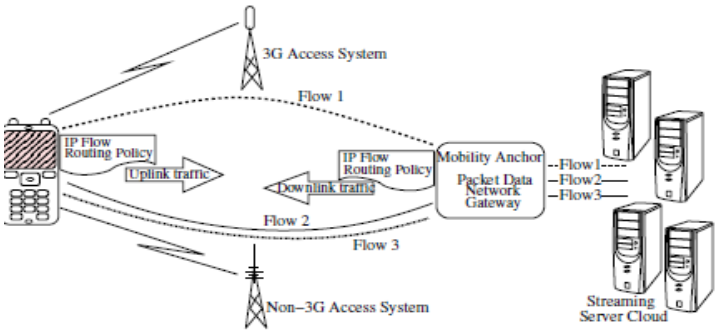
1) Representa la movilidad y el enrutamiento de los flujos a través de un acceso diferente

2) Los sistemas basados en reglas y políticas de enrutamiento.

Mientras que una solución para la movilidad flujo IP basado en el cliente, basada en Dual Stack Mobile IPv6 (DSMIPv6), está siendo actualmente estandarizada, alternativas de solución basada en la red para IP movilidad de flujo, sobre la base de Proxy Mobile IPv6 (PMIPv6) o el Protocolo de encapsulamiento de GPRS (GTP), se siguen discutido. Las soluciones basadas en cliente para la movilidad flujo IP hace uso del canal de señalización de extremo a extremo entre el terminal móvil y la puerta de enlace PDN (PDN GW) para la señalización de las reglas de política de encaminamiento de flujo. La falta de móviles participación terminal en la gestión de movilidad basada en la red y la interfaz de señalización que falta entre el terminal móvil y la infraestructura de red para llevar a cabo la señalización durante los eventos de movilidad implica desafíos técnicos adicionales para la movilidad flujo IP, como las reglas de política de encaminamiento de flujo debe estar sincronizada en el terminal móvil y en el PDN Gateway.

Este documento propone una solución flexible fuera de banda para establecer y fluya actualización de enrutamiento IP reglas de política en un móvil terminal y su pasarela PDN mientras que re-utilizando los recursos existentes arquitectura y protocolo de componentes Evolved del 3GPP la red central de paquetes. La solución hace uso de la Política y Carga de Control (PCC), la arquitectura y su concepto genérico de una función de aplicación (AF), que interconecta con una terminal móvil, así como con la Política y reglas de cobro Function (PCRF) de la red central. Las soluciones definen una función de aplicación de configuración de directivas de enrutamiento (RPCAF), lo que representa una puerta de enlace de señalización entre la política terminal móvil y el sistema de PCC. El concepto propuesto permite la señalización bidireccional de las reglas de política de enrutamiento entre terminales móviles y la red del operador móvil y puede ser utilizado para la movilidad de acogida, así como para la movilidad basada en la red sin la necesidad de depender de la tecnología de acceso linklayer específica protocolos para señalar las reglas de política de encaminamiento de flujo.

Figura 11: Movilidad flujo IP a través de 3G y sistema de acceso no 3G de acuerdo con las políticas de enrutamiento flujo IP.



IEEE Globecom Workshop on Advances in Communications and Networks 2010 Movilidad flujo IP a través de 3G y sistema de acceso no es 3G e acuerdo con las políticas de enrutamiento flujo IP. [Fuente] Recuperado: Policy Routing Architecture for IP Flow Mobility in 3GPP's Evolved Packet Core.

TRABAJOS RELACIONADOS:

El grupo 3GPP SA2 comenzó un elemento de estudio para investigar diferentes posibilidades de movilidad flujo IP. Algunos de estos Las soluciones se describen en el informe técnico.

El trabajo sobre solución de movilidad flujo IP para DSMIPv6 volvió mientras tanto en un elemento de trabajo para la normalización.

Es intrínsecamente diferente a cualquiera de las soluciones discutidas para PMIPv6, como la solución basada en el cliente se basa en los móviles terminales para proporcionar la política de enrutamiento flujo como parte de la señalización de la movilidad (Binding Update) a la PDN Gateway. En caso de que el operador quiere iniciar un cambio en la ruta de flujo políticas, la solución se basa en el descubrimiento de acceso a redes y la función de selección (ANDSF).

Por esto, los terminales móviles se registran en un servidor de ANDSF recibir información de la red de acceso y las preferencias del operador con respecto a la selección de una red de acceso. Dos cuestiones existir con el uso de ANDSF para notificar móvil individual terminales sobre las políticas de enrutamiento flujo actualizados: El ANDSF servicio no tiene interfaz para el control de Estrategia y Cargo sistema (PCC), y por lo tanto necesita otros medios para informarse sobre la política de enrutamiento actualizada flujo para un terminal en particular.

La interfaz falta hace que la adopción de cambios dinámicos en las políticas de enrutamiento IP flujo difícil. Además, la solución es muy móvil centrada en el terminal, como el operador tiene que primero realizar las políticas de enrutamiento para el terminal móvil, y luego se basa en el terminal móvil para proporcionar estas políticas a la PDN Gateway para la ejecución en el enlace descendente.

Para PMIPv6, describe hasta ahora dos propuestas de solución. Propuesta uno asume la UE para proporcionar el encaminamiento de flujo IP políticas a la PDN Gateway, y por lo tanto es muy similar a la solución para DSMIPv6. Sin embargo, ya que en la PMIPv6 móvil terminal tiene ninguna interfaz de protocolo con el PDN Gateway, se supone que las políticas de enrutamiento pueden ser transportados a la Sirviendo de puerta de enlace por medio de los mecanismos de la capa de enlace, que a continuación, se transportan a la PDN de puerta de enlace como parte de la PMIPv6 ubicación de actualización de señalización. Igual que para DSMIPv6, es ANDSF asumido para transmitir actualizaciones en las políticas de enrutamiento flujo de la red a los terminales móviles individuales en caso de operatividad y movilidad de flujo.

Esta propuesta no implica el sistema de PCC en la puesta en marcha de las políticas, antes de la señalización las políticas para el terminal móvil y luego a la PDN Puerta.

Como consecuencia de ello, la puerta de enlace PDN sólo puede autorizar a las políticas después de que hayan sido aprovisionados a través de la terminal móvil. Por lo tanto, esta propuesta trata el manejo de fluya directivas de enrutamiento diferente a otros tipos de políticas (por ejemplo, normas de calidad de servicio) proporcionados por el sistema PCC.

El protocolo PMIPv6 se basa en el PCC del 3GPP Sistema y se basa en la señalización desde el terminal móvil a la PCRF a través de la Entidad de Gestión de Movilidad (MME).

En caso de que el terminal móvil desea proporcionar una actualización del flujo IP directivas de enrutamiento, envía una portadora de radio específica comando modificación a la MME, que lleva a cuestas la fluya la información de encaminamiento de política. El MME reenvía las políticas a la pasarela de servicio con la modificación de portador señalización. La pasarela de servicio reenvía las políticas a la PCRF, que autoriza a las políticas de enrutamiento de flujo y, a su vez las hace cumplir en la PDN Gateway. En caso de operar cambios a las políticas de enrutamiento de flujo, la propuesta de dos que diferencia entre 3GPP y no 3GPP accesos.

Por el aprovisionamiento de las políticas de enrutamiento de flujo a los servicios móviles del terminal, propuesta también asume la ANDSF proporciona la políticas antes de la autorización por parte del PCC en el terminal móvil, antes de esto les señales a través de los procedimientos de 3GPP-específicas a la red. Como consecuencia de ello, se aplican las mismas deficiencias.

En cuanto a la solución a saber, falta de apoyo para la altamente dinámica actualización de la política y los caminos de señalización para el enlace ascendente y desequilibrado enlace descendente de señalización de las políticas. Una desventaja clave de la propuesta del protocolo PMIPv6.

El Grupo de Trabajo de Ingeniería de Internet (IETF) Actualmente también investiga extensiones al protocolo IP para apoyar PMIPv6 fluya la movilidad y la señal políticas de enrutamiento entre el acceso pasarela (Serving Gateway) y el anclaje de movilidad (PDN Puerta). Su actividad en este contexto no se fija en el cómo si no en las políticas de encaminamiento de flujo se señalizan entre un terminal móvil y la infraestructura de red.

Estado del arte se dirige a un conjunto limitado de casos de uso y considera que el terminal móvil juega un papel central en la política de ejecución, sin mayor intervención de la política de la EPC (arquitectura de control), el sistema de PCC. Soluciones para PMIPv6 depender de la existencia de la funcionalidad de la capa de enlace para transmitir el flujo de políticas de encaminamiento entre terminales móviles y la red con su infraestructura. Además, basándose en la arquitectura actual ANDSF para transmitir las políticas de enrutamiento de flujo limita la dinámica de IP y flujo de movilidad debido a la falta de interfaz con el sistema PCC

Este artículo propone una arquitectura para el enrutamiento de flujo IP configuración de la política de apoyo a la movilidad flujo IP en 3GPP de Evolved Packet Core. La solución propuesta introduce una aplicación en Función de configuración de directivas de enrutamiento, que puede aplicarse con flexibilidad como Application Server o coubicarse con un servidor ANDSF. El RPC AF es un componente integral del sistema de control de Estrategia y Cargo del EPC y permite bidireccional de señalización fuera de banda de la política de enrutamiento flujo reglas entre la UE y la red utilizando una simétrica ruta de señalización para el UE y el operador provisto de enrutamiento flujo políticas. La solución propuesta no depende de Acceso tecnología y protocolo de movilidad capacidades específicas para transmitir reglas de política. El flujo directivas de enrutamiento pueden ser actualizados en cualquier tiempo sin la necesidad de enviar la señalización relacionada con la movilidad y pueden ser forzadas rápidamente con la ayuda del sistema de PCC. La solución propuesta se caracteriza en una clara separación de IP y la gestión de la movilidad con la gestión de la política de enrutamiento del flujo.

12.3.2.1 Joint Call Admission Control in Integrated Wireless LAN and 3G Cellular Networks

La cuarta generación (4G) (Liu, 2004). Se espera que el sistema pueda apoyar plenamente integración de servicios y acceso ubicuo en cualquier momento y en cualquier lugar.

En lugar de desarrollar un nuevo uniforme estándar para todos los sistemas de comunicación inalámbrica, algunos esfuerzos en investigación se enfocan en 4G

La perfecta integración de diversas redes de comunicación inalámbrica existente, tales como integrada LAN inalámbrica (WLAN) y de la tercera generación (3G) de redes celulares.

Las redes celulares 3G proporcionan cobertura y servicios de itinerancia universal de ancho, con limitada velocidad de datos de hasta 2 Mbps (Liu, 2006, 2007). Con una planificación cuidadosa y la red madura.

Los algoritmos de control de admisión, la calidad alcanzable de servicio (QoS) nivel de 3G celular redes es relativamente alta. Por otro lado, las WLAN ofrecen bajo costo, alta velocidad de datos

Acceso inalámbrico en un punto de acceso de área limitada. Desde WLAN está diseñado originalmente para bestEffort servicios de datos con acceso basado en contención, es difícil de lograr estricta QoS el aprovisionamiento de servicios en tiempo real, tales como el servicio de voz (Song et al., 2006).

Debido a las diferentes capacidades de las redes, los patrones de móviles de usuario, transferencias verticales, y los niveles de calidad de servicio, la redes celulares 3G WLAN integrado y requieren un nuevo esquema de control de admisión de llamadas

Para proporcionar QoS aprovisionamiento y la utilización eficiente de los recursos. En la actualidad existen tres principales arquitecturas de interconexión entre las redes celulares 3G y WLAN celulares (Ahmavaara et al., 2003). Pero todos ellos son la falta de gestión conjunta de recursos y admisión esquemas de control de entorno integrado. El trabajo de investigación anterior sobre el control de admisión de redes celulares homogéneas y heterogéneas redes integradas se investigan con descripciones técnicas sobre sus ventajas y desventajas. Se muestra que más esfuerzos son necesarios en control conjunto de la congestión, equilibrio de carga, y el alto nivel de calidad de servicio de aprovisionamiento en el manejo integral redes.

En este capítulo, un esquema novedoso de control de admisión de llamadas conjunta (CAC) se propone el apoyo tanto los servicios de datos con QoS aprovisionamiento de voz y.

Debido a los diferentes servicios de red características, red celular 3G está definido para ser una red de voz prioridad donde la voz los servicios tienen mayor prioridad para la asignación de recursos de los servicios de datos, mientras que WLAN está definida como la red de datos con prioridad a los servicios de datos, donde tienen mayor prioridad que los servicios de voz.

Una política de admisión de llamadas en conjunto proviene fomentar una arquitectura de red heterogénea, tipos de servicios, los niveles de calidad de servicio, y las características de movilidad de usuario. Además, para aliviar el tráfico la congestión en las redes celulares, una búsqueda de canales óptima y algoritmo de sustitución y técnicas de traspaso pasiva relacionados se desarrollan más para equilibrar el tráfico total del sistema entre WLAN y la red celular 3G, así como para reducir el coste medio QoS sistema, tales como probabilidad de bloqueo del sistema.

Un modelo de Markov unidimensional para el servicio de voz es también desarrollado para analizar interfuncionamiento métricas de rendimiento del sistema.

Tanto el análisis teórico y resultados de la simulación muestran que los costos promedio de calidad de servicio del sistema, tales como el bloqueo total y dejando caer las probabilidades, se reduce, y nuestro esquema supera tanto disjuntos tradicional esquema de CAC estática y sin optimización conjunta.

Arquitectura de WLAN integrado y las redes celulares 3G

Impulsado por el lugar y en concepto de servicio móvil en cualquier momento, se espera que la conexión inalámbrica 4G y redes serán heterogéneos, la integración de las diferentes redes para proveer Internet sin fisuras acceso para los usuarios móviles.

La WLAN integrada y la red celular 3G se aprovecha de la amplia cobertura y apoyo casi universal de itinerancia redes celulares 3G y las altas velocidades de datos de las redes WLAN.

Actualmente, hay tres arquitecturas principales para interconexión entre 3G universal

Sistema de Telecomunicaciones Móviles (UMTS) de redes celulares y WLAN IEEE 802.11.

Estos son acoplamiento abierto, estrecho acoplamiento, y el acoplamiento flojo (Liu, 2006). El Open arquitectura de acoplamiento especifica un estándar abierto y se utiliza para el acceso y la itinerancia entre las redes 802.11 WLAN y UMTS. En este enfoque, las dos redes son consideradas como dos sistemas independientes que pueden compartir un esquema de facturación único entre ellos. Una WLAN 802.11 se conecta a Internet a través de una puerta de enlace, y UMTS red, está conectado a Internet a través de un nodo de soporte GPRS de puerta de enlace (GGSN).

Esquema de acoplamiento abierto es la falta de apoyos para la movilidad, gestión de recursos, calidad de servicio aprovisionamiento y la seguridad en el entorno integrado.

Como un esquema de integración directa, estrecho acoplamiento conecta la red WLAN al resto de la red de núcleo de la misma manera como otras tecnologías de acceso de radio celular (Liu y Zhou, 2005a, 2005b; Liu, 2006). Como se muestra

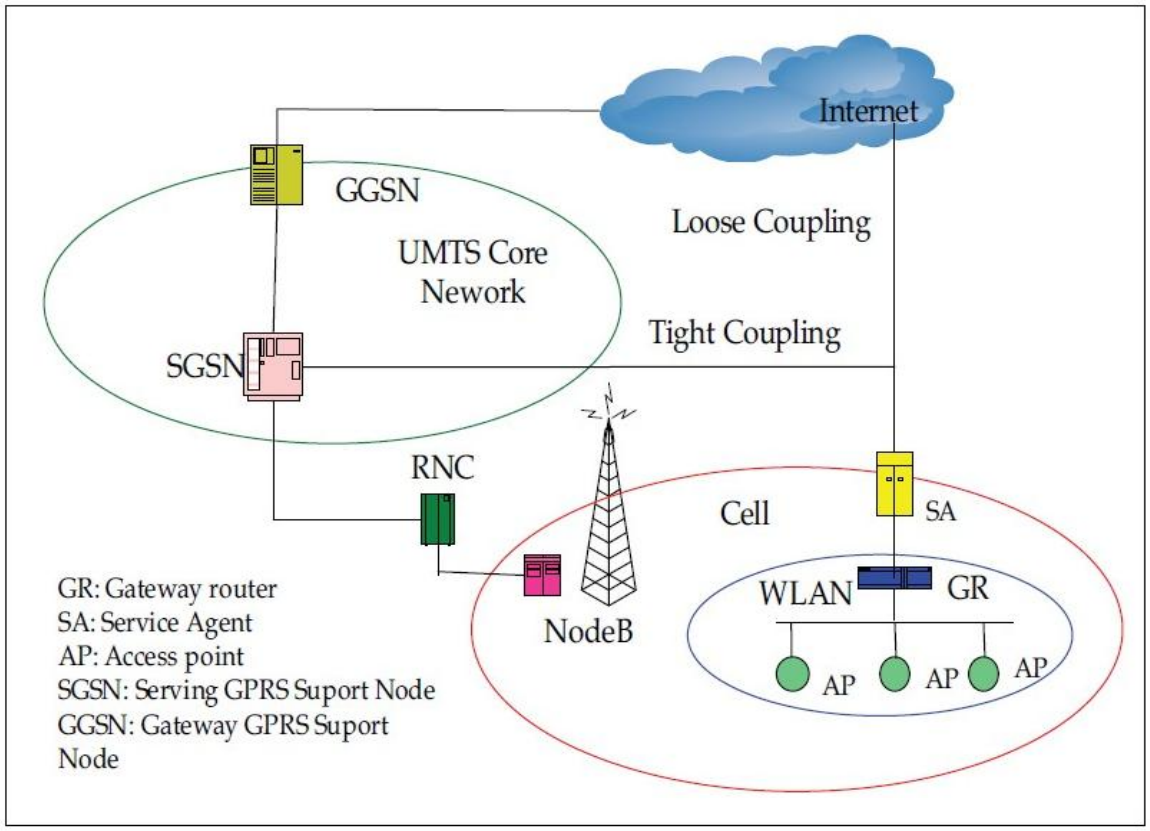
en la Fig. 1, la puerta de enlace WLAN oculta la detalles de la WLAN de la red central 3G UMTS mediante la adición de un nuevo componente, SGSN emulador, en WLAN. El emulador SGSN conecta la puerta de enlace en la red WLAN a la red central IP. Se interconecta la red central UMTS en la interfaz Gn (Liu, 2006), e implementa todos los protocolos de UMTS requeridos en una red de acceso radio 3G. En términos de UMTS protocolos, el área de servicio inalámbrico funciona como otra área de cobertura SGSN al núcleo UMTS red. Como resultado, todos los tráficos, incluyendo datos de señalización y UMTS, generado en el WLAN se inyectan directamente en la red de UMTS de núcleo a través del emulador SGSN.

Esta aumenta la carga de tráfico de la red central UMTS. Si los operadores de la WLAN son diferentes de los de la red UMTS, la nueva interfaz entre el UMTS y la WLAN puede causar fallos de seguridad. Además, las tarjetas WLAN en los dispositivos cliente deben incorporar la pila de protocolos UMTS, y Universal Subscriber Identity Module (SIM)

Mecanismo de autenticación debe ser utilizado para la autenticación en la red WLAN (Liu y Zhou, 2005a).

En contraste con alto costo de estrecho acoplamiento, el acoplamiento flojo es un mecanismo basado en el IP, y el enfoque separa las rutas de datos en la WLAN 802.11 y redes celulares 3G (Liu, 2006). Los routers de puerta de enlace 802.11 WLAN se conectan a la Internet, y todo el tráfico de datos es enrutado a Internet núcleo, en lugar de a la red de núcleo celular. Para la red central del UMTS, por ejemplo, la WLAN 802.11 aparece como una red de visitante. La puerta de enlace de la WLAN 802.11 se puede conectar a un Agente de Servicio (SA), un SGSN combinado / GGSN emulador, que proporciona el protocolo de conexión en red no sólo para la señalización entre la 802.11 WLAN y la red central UMTS 3G, pero también una interfaz para los tráficos de datos entre las redes WLAN e IP. Si la WLAN 802.11 se despliega por el mismo operador UMTS, el SA puede conectarse directamente a la red central UMTS para la señalización. De lo contrario, el SA es la interfaz con la red IP para la señalización y tráfico de datos. En comparación con abrir o apretado arquitecturas de acoplamiento, acoplamiento débil implementa el despliegue independiente y el tráfico configuración tanto de la WLAN 802.11 y redes UMTS. Además, la articulación flexible arquitectura permite a un operador móvil para proporcionar sus propios "puntos calientes" privados 802.11 WLAN e interoperar con 802.11 WLAN públicas y los operadores de UMTS a través de la interconexión acuerdos. Así que en términos generales, la articulación flexible es más preferible para integrada WLAN / red celular, debido a la simplicidad y menos trabajo de reconfiguración.

Figura 12: Estrecho acoplamiento y acoplamiento débil



[Fuente] T-Mobile, Illinois Institute of Technology, Florida International University,
Lamar University U.S.A. 2011
Recuperado: Joint, Call Admission Control in Integrated Wireless LAN and 3G Cellular Networks.

A pesar de acoplamiento prometedor, suelta tiene varios problemas técnicos que tenga que abordar antes integración con éxito, tales como la gestión integrada de ubicación, traspaso sin fisuras verticales, común de provisión de QoS y unificada de autenticación, autorización y contabilidad (AAA), convocatoria conjunta de control de admisión y así sucesivamente. Como parte de la gestión recursos, admisión de llamadas conjunta el control interactúa fuertemente con esquemas de provisiones de traspaso y de calidad de servicio integrada en verticales redes celulares de WLAN y 3G.

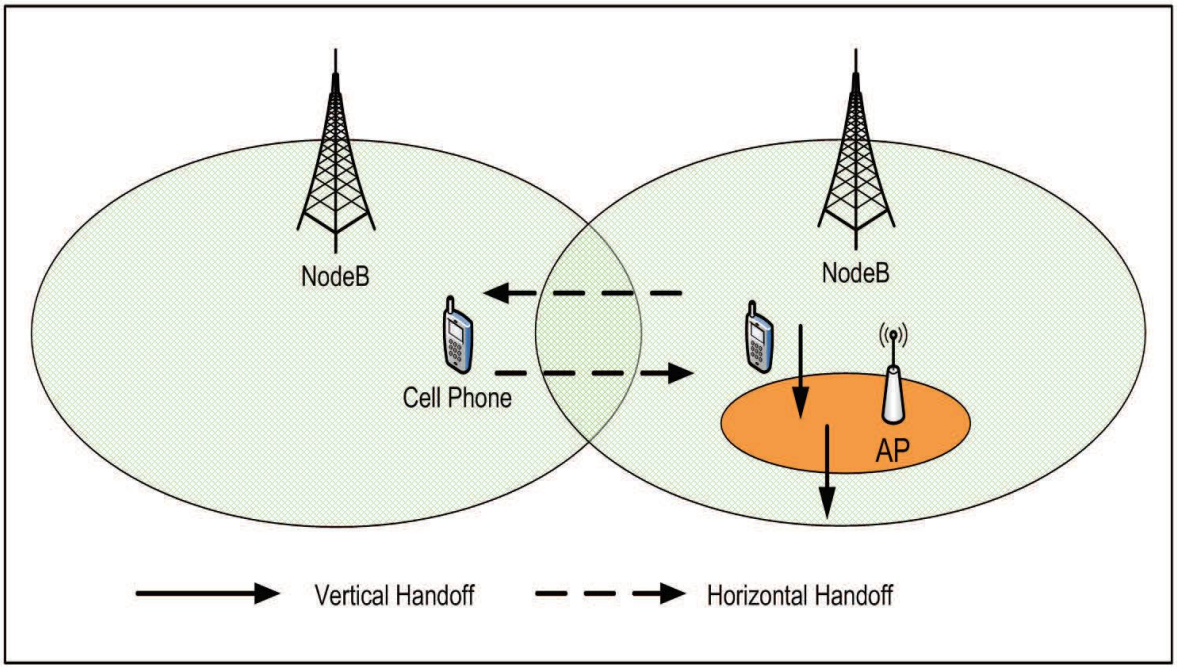
Traspaso vertical

En redes integradas, hay dos tipos de traspaso: traspaso intra-tecnología y Intertechnology traspaso (Lampropoulos et al, 2005; Shafiee et al., 2011). La intra-tecnología.

Es tradicional traspaso Horizontal (HHO) en la que los terminales móviles de traspaso entre dos estaciones bases adyacentes o puntos de acceso que utilicen misma tecnología de acceso.

El traspaso contraste, entre la tecnología se denomina traspaso vertical (VHO), y sucede cuando terminales móviles vagan entre dos redes con diferentes tecnologías de acceso, por ejemplo, entre WLAN y la red 3G UMTS.

Figura 13: Transferencias de WLAN integrado y UMTS las redes celulares



[Fuente] T-Mobile, Illinois Institute of Technology, Florida International University,
Lamar University U.S.A. 2011
Recuperado: Joint, Call Admission Control in Integrated Wireless LAN and 3G Cellular Networks.

Los traspasos verticales en WLAN integrado / UMTS tienen dos escenarios: un móvil terminal se mueve fuera de una WLAN a una red celular UMTS, y se mueve de UMTS red de celulares en una WLAN.

Teniendo en cuenta diferentes área de cobertura del servicio, la transferencia vertical de WLAN para la red celular normalmente se desencadena por desvanecimiento de la señal cuando un usuario se mueve fuera del área de servicio de la WLAN. Sin embargo, el traspaso vertical desde la red celular a la WLAN se considera como un proceso de selección de red, ya que los terminales móviles se encuentran en una el área de cobertura inalámbrica en la que tanto el acceso celular y conexión inalámbrica a Internet están disponibles para móviles terminales al mismo tiempo.

Traspasos sin fisuras verticales se enfrentan a desafíos causados por la brecha entre los diferentes niveles de calidad de servicio en red celular y WLAN (Liu, 2006; Shafiee et al., 2011): las redes celulares UMTS deben dar una amplia cobertura con alta calidad de servicio de aprovisionamiento para servicios de voz, pero con los datos de tasa limitada de Servicio. Sin embargo, las redes WLAN con compatibles con el servicio de datos de alta velocidad, pero con falta de itinerancia bajo nivel de calidad de servicio para el servicio de voz, debido a su original, en tiempo real.

Restricciones además, el control de admisión de llamadas se ha implementado en la red celular para asegurar una baja probabilidad de caída de llamadas en el sistema mediante la asignación de transferencias horizontales de voz con una mayor prioridad a los recursos que las nuevas solicitudes de llamada de voz y datos, mientras que las WLAN sólo admiten el acceso a nivel de paquetes gruesos sin tener en cuenta las prioridades de los traspasos.

Así que en WLAN integrada y redes celulares 3G, realiza transferencias sin fisuras verticales y de admisión de llamadas de control debe ser considerada como mecanismos dependientes y conjuntos para asegurar tanto de alto nivel la calidad del servicio de la llamada y la utilización eficiente de los recursos en el interfuncionamiento medio ambiente.

El Control De Admisión De Llamadas y El Trabajo Previo

En el sistema de comunicación, el esquema de control de admisión de llamadas es una estrategia de aprovisionamiento de aprovisionamiento de QoS y la reducción de la congestión de red (Ahmed, 2005). Son las llamadas que llegan concedido o denegado sobre la base de criterios predefinidos del sistema. Debido

a los recursos limitados del espectro y la creciente popularidad del uso de las redes celulares inalámbricas, el CAC ha estado recibiendo mucha de las atenciones para el aprovisionamiento de QoS, y sus principales características son extendidos para cubrir la señal la calidad, la probabilidad de bloqueo de nueva llamada, transferencia de probabilidad de caída, velocidad de datos, etc.

La próxima generación de WLAN integrado y las redes celulares 3G plantean un gran desafío a la diseño CAC debido a las características de red heterogéneos, tales como las técnicas de acceso variados, prioridades de asignación de recursos, calidad de servicio de aprovisionamiento, los niveles de transferencias verticales, etc.

Control de admisión de llamadas en WLAN integrada y redes celulares 3G

Se han realizado algunos trabajos sobre el control de admisión de llamadas en WLAN integrado y celular en redes 3G. La mayoría de los significativos son WLAN primeros enfoques, basado en algoritmos de movilidad y CAC esquemas basados en políticas.

Enfoques WLAN en primer lugar: Si los terminales móviles se localizan en un área de servicio WLAN, tanto nueva voz y llamadas de datos por primera solicitud de admisión a la WLAN.

Si es rechazada, las llamadas desbordan a 3G red celular. Si los terminales móviles con llamadas en curso de voz y datos se mueven en el WLAN, las llamadas siempre trata de traspaso a WLAN (Song et al, 2006; Song et al., 2007a).

Esta preferencia incondicional a WLAN tiene como objetivo aprovechar el ancho de banda más barato y más alto en WLAN, en comparación con la red celular 3G. Sin embargo, estos enfoques pueden causar una situación de hacinamiento del tráfico en WLAN, sin equilibrio de carga en ambas redes.

Desde el usuario la movilidad no se cubre en estos enfoques, las peticiones de transferencia frecuentes sucederán en torno el límite de WLAN, lo que puede causar efectos "ping-pong" por varios traspasos verticales con grandes tráficos s adicionales generados en las redes.

Los algoritmos basados en la movilidad: Algunos trabajos de investigación consideran usuarios con diferente movilidad y velocidades se aplican diferentes algoritmos de CAC y de traspaso vertical para ellos. Algunos autores probabilísticamente rechazar las peticiones de transferencia verticales para WLAN para usuarios de celulares de gran movilidad

(Lampropoulos et al, 2005; Klein y Han, 2004), para reducir los traspasos innecesarios. En esto esquema, la carga de procesamiento y el nuevo bloqueo de llamadas de probabilidad se pueden reducir los manteniendo el rendimiento razonable en la WLAN. Una llamada predictivo basado en la movilidad técnica de control de admisión se ha propuesto para las redes heterogéneas inalámbricas 4G

(Rashad, 2006). En este esquema, los perfiles de movilidad local y global para los terminales móviles son generados y utilizados para la toma de admisión de llamadas. Sin embargo, ya que la aleatoriedad de usuario movilidad, puede ser difícil para este tipo de algoritmos para obtener estimación de la velocidad oportuna y concisa. Además de la gestión de traspaso en base a información de movilidad, más obras son necesarias para examinar diferenciaciones de servicio, costo, calidad de servicio y las preferencias del usuario, para proporcionar optimización global para la utilización de recursos en redes integradas.

Esquemas de políticas basadas CAC: Algunas soluciones siguen el marco de actuación definido por el IETF, y combinar el control de admisión de llamadas y gestión de transferencia verticales juntos. Utilizan un esquema móvil asistido, en el que la funcionalidad del sistema se controla mediante una directiva de red y un motor de la política móvil (Zhuang et al., 2003). Como se muestra en la Fig. 14, una pareja formada por un punto de decisión de políticas (PDP) y el punto de aplicación de políticas (PEP) existen en ambos motores, junto con los repositorios de política.

PEP es responsable de la ejecución de una política que se decidió por PDP, y los repositorios de políticas definen las políticas que se deben seguir para una correcta decisión de transferencia[17]

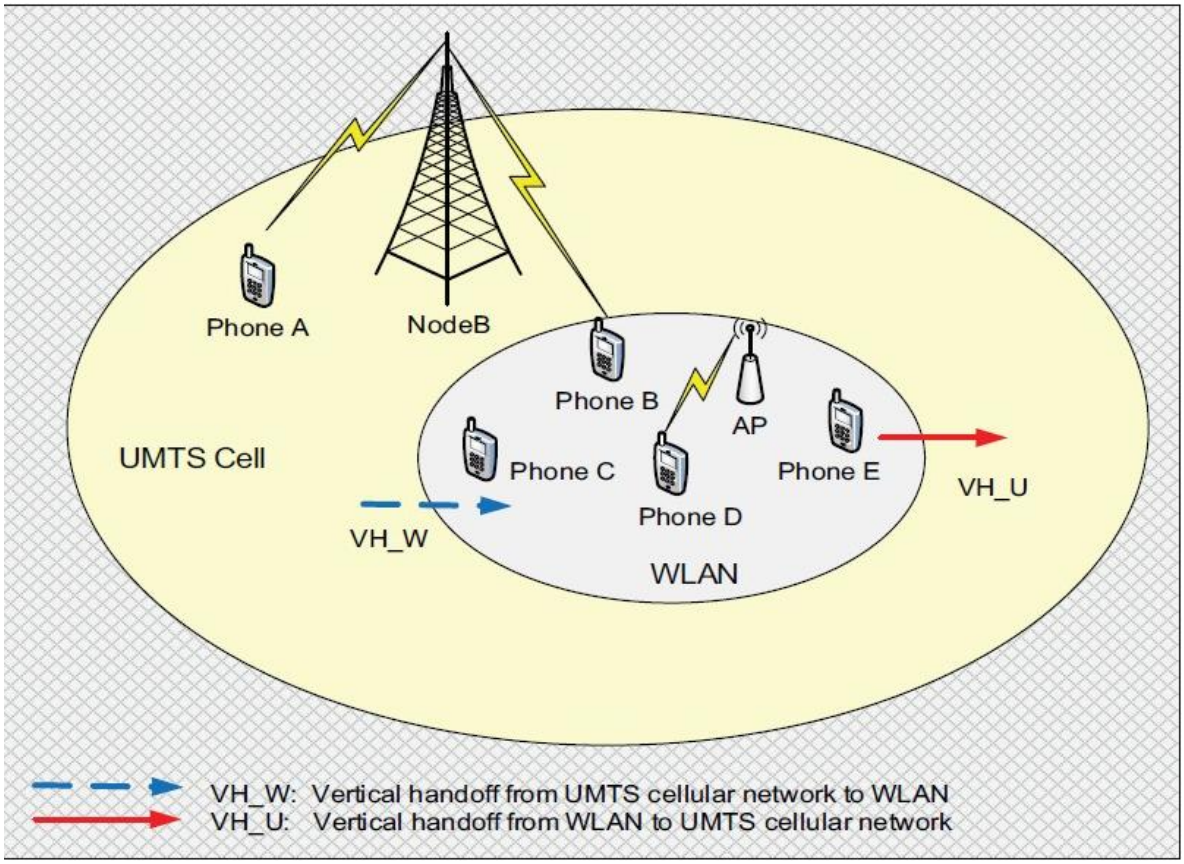
En la admisión de llamadas procedimiento de control, las PEP en los terminales móviles consulte a un PDP con domicilio en la red de recursos disponibles. El PDP tomará una decisión sobre la admisión de llamadas, basado en la red capacidades, el nivel de calidad de servicio, tipos de llamada, preferencias del usuario, así como estimaciones sobre la red actual carga y actuaciones. Este enfoque proporciona flexibilidad a la terminal y la red para tomar la mejor decisión posible traspaso, e implementa el equilibrio de carga.

[17] http://bibliotecavirtual.unad.edu.co/ - (Zhuang et al., 2003; Guerrero y Barba 2008).

Modelo de sistema

Nuestro modelo de sistema se basa en la arquitectura de articulación flexible en la que está conectado WLAN a las redes celulares a través de Internet. Todos los tráficos en WLAN se enrutan a través de Internet las puertas de enlace. Puesto que el área de cobertura de una célula UMTS es normalmente mucho más grande que área WLAN, la célula celular se denomina "célula macro", mientras que la región WLAN se considera un "micro-celular" dentro de (Liu et al., 2007). El área de servicio superpuesto entre el "macro-celular" y el "micro-celular" ofrece terminales móviles con oportunidades para conectar a cualquiera UMTS de la red o la WLAN, como se muestra en la fig. 14.

Figura 14: Modelo del sistema de célula de UMTS y WLAN integrada



[Fuente] :T-Mobile, Illinois Institute of Technology, Florida International University, Lamar University U.S.A. 2011
Recuperado: Joint, Call Admission Control in Integrated Wireless LAN and 3G Cellular Networks.

12.3.2.2 New Privacy Issues in Mobile Telephony: Fix and Verification

Aunque la mayoría de los usuarios de teléfonos móviles aceptan que la red del operador puede realizar un seguimiento de sus movimientos geográficos, pocos se sentirían felices si un tercero arbitraria lo hiciera. Tal posibilidad permitiría a todo tipo de comportamiento no deseado, que van desde el acoso criminal y el acoso a más mundanas vigilancias de los movimientos cónyuge o de los empleados, así como perfiles con fines comerciales y de publicidad.

Por esta razón, 3G (Tercera Generación) protocolos de telefonía móvil han sido diseñados para impedir que terceros, las escuchas en el enlace de radio, desde la identificación de los mensajes inalámbricos como procedente de un teléfono móvil en particular.

Por lo tanto, Los teléfonos móviles se identifican, siempre que sea posible, por medio de identificadores temporales (TMSIs) en lugar de utilizar sus largas identidades únicas plazo (IMSI). Identidades temporales son actualizadas periódicamente por la red. Para evitar linkability[18], la asignación de una nueva identidad temporal se cifra usando una clave de sesión establecida a través de la autenticación 3G y la concordancia de claves (AKA) de protocolo

Nuestras contribuciones.

Linkability de las transacciones ha sido identificados y con frecuencia lo informado por los medios de comunicación como un importante amenaza para la privacidad del usuario a pesar de que ha sido pasado por alto hasta ahora por la mayoría de los estudios existentes sobre protocolos de comunicación móviles que en su lugar se centran en la confidencialidad y los requisitos de autenticación.

En este trabajo, presentamos el primer análisis formal de los protocolos 3G w.r.t. privacidad de los usuarios de teléfonos móviles de los atacantes de terceros y, en particular w.r.t. imposibilidad de vinculación y el anonimato de abonados a la 3G. Para nuestro análisis formal de métodos de uso automatizado.

El uso de métodos formales nos permite: (i) precisamente y definir inequívocamente las propiedades deseadas de privacidad en términos de

[18] Protocolo de seguridad

anonimato fuerte de terceros y fuerte imposibilidad de vinculación; (Ii) identificar nuevas vulnerabilidades con respecto al suscriptor de privacidad gracias a una especificación rigurosa de los protocolos y de las propiedades analizadas.

Sin embargo, las herramientas automatizadas disponibles en la actualidad siguen siendo bastante limitado y no puede ser utilizado sin rodeos para verificar imposibilidad de vinculación y anonimato propiedades. Aquí desarrollamos maneras de modelar los protocolos y las propiedades deseadas como biprocesses el fin de utilizar la herramienta ProVerif en nuestro 3G caso de estudio.

La verificación automática con el ProVerif herramienta nos permite: (i) verificar la imposibilidad de vinculación fuerte y fuerte anonimato. A lo mejor de nuestro conocimiento, es el primer tiempo de estas definiciones de las propiedades de privacidad han sido exitosamente utilizado para la verificación utilizando una herramienta automatizada; (Ii) verificar que las correcciones que proponemos hacer preservar la privacidad de los usuarios de teléfonos móviles por parte de terceros en términos de imposibilidad de vinculación y el anonimato; (Iii) verificar automáticamente la privacidad características expresadas como relaciones de equivalencia entre los sistemas que consiste en un número ilimitado de agentes de ejecución un número ilimitado de sesiones; (iv) obtener una mayor nivel de confianza en las pruebas resultantes distintas de los indicados por más técnicas manuales propensos a errores.

Con nuestro ProVerif método detecta con éxito las vulnerabilidades de privacidady también demuestra con éxito que los protocolos fijos (presentados en la Sección satisfacen tanto imposibilidad de vinculación y el anonimato.

Por otra parte, nos demuestran cómo estas vulnerabilidades pueden conducir a ataques prácticos, mediante la implementación de 3G en reales redes en Alemania (Vodafone, O2, T-Mobile) y en Francia.

Requisitos de Seguridad 3G

3G tiene como objetivo proporcionar autentificación, confidencialidad de los datos y la comunicación de voz, así como la privacidad del usuario. En particular, objetivos de privacidad 3G incluyen los siguientes:

La confidencialidad de identidad de usuario: la propiedad de que la permanente la identidad del usuario (IMSI) de un usuario al que un servicio es entregado no puede ser espiado en el enlace de acceso de radio; untraceability usuario: la propiedad de que un intruso no pueda deducir si los diferentes servicios

se prestan a la misma de usuario por escuchas ilegales en el enlace de acceso de radio.

Para lograr estas dos propiedades relacionadas con la privacidad, 3G (y GSM) se basa en el uso de las identidades temporales TMSIs (Temporary Mobile Subscriber identidades) para identificar y la paginación de los teléfonos móviles (estaciones móviles con mayor precisión, EM) en lugar de utilizar sus identidades a largo plazo IMSI (International Identidades de Abonado Móvil). De hecho, las escuchas telefónicas de la IMSI en comunicaciones de texto claro haría permitir la identificación de los usuarios de telefonía móvil de tercera fiestas.

Por otra parte, el estándar 3G requiere actualizaciones periódicas de la identidad temporal, para evitar la trazabilidad de una estación móvil por parte de terceros. Las nuevas identidades temporales son asignadas periódicamente por la red a través del procedimiento de reasignación de TMSI. La TMSI recién asignado es encriptado usando una clave de sesión que se establece mediante la ejecución la autenticación de 3G y el protocolo de acuerdo de clave (AKA).

También conocido como el protocolo 3G permite MS y la red para lograr la autenticación mutua y establecer un par de compartido claves de sesión, es decir, una clave de cifrado y una clave de integridad.

Estas teclas se utilizan para asegurar el secreto y la integridad de las comunicaciones posteriores.

Ataque de paginación imsi:

El procedimiento de paginación se utiliza para localizar una estación móvil en el fin de ofrecer un servicio a la misma, por ejemplo, una llamada entrante. Mensajes de solicitud de paginación se envían por la red en todo las áreas de ubicación más recientemente visitados por la estación móvil con el fin de localizar y entregar un servicio a la misma.

La paginación mensaje de solicitud se envía en un canal de control común (CCCH) y contiene la identidad de una o más estaciones móviles.

El procedimiento de paginación se ejecuta típicamente utilizando la TMSI para identificar un MS. Sin embargo, la IMSI se puede utilizar cuando la TMSI no es conocida por la red. Una estación móvil que recibe una solicitud de búsqueda establece un canal dedicado a permitir la entrega del servicio y envía una respuesta de búsqueda que contiene la TMSI asignado más recientemente.

La posibilidad de desencadenar una solicitud de paginación para una específica IMSI permite a un atacante para verificar un área específica para la presencia de estaciones móviles, de los cuales se conoce la identidad, y correlacionar su IMSI y TMSI. A medida que detallaremos en un entorno real, el vínculo entre el paginado

IMSI y la TMSI relacionada tendrían que ser confirmadas por repitiendo el ataque varias veces.

También conocido como Protocolo de Ataque linkability

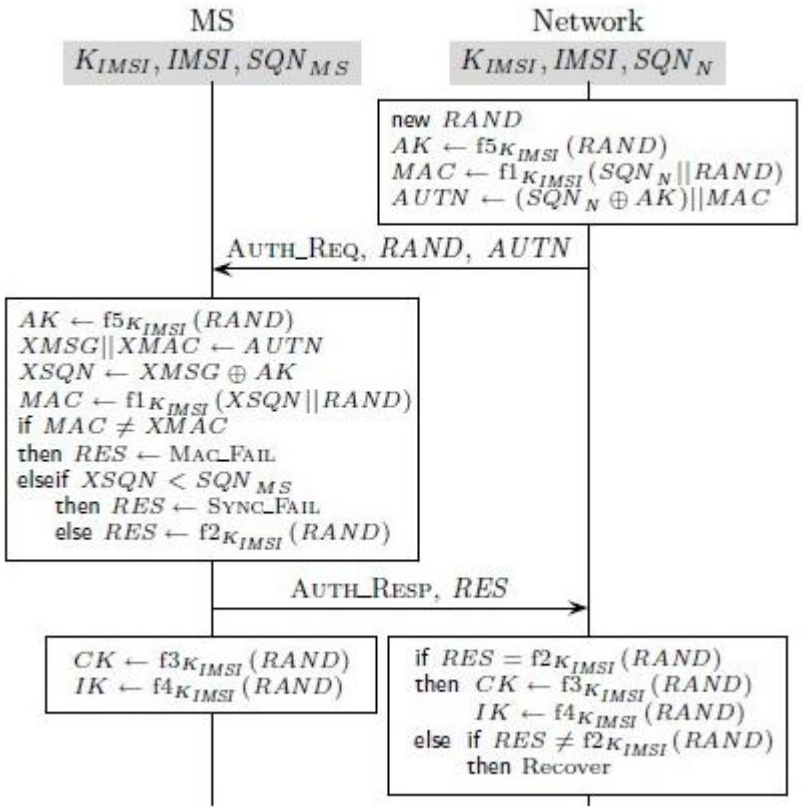
La autenticación y protocolo de acuerdo de clave (AKA) consigue la autenticación mutua entre una MS y la red, y establece claves de sesión compartidas para ser usado para asegurar las comunicaciones posteriores.

La MS con identidad IMSI y la red comparten una clave secreta a largo plazo, Kimsi, asignado al abonado por el operador de telefonía móvil y se almacena en el USIM.

La clave secreta permite que la MS y la red para calcular claves de cifrado de sesión y la integridad para ser compartidos se utiliza para el cifrado y comprobación de integridad de las comunicaciones.

El protocolo 3G También conocido como KIMSI, que se muestra en la figura 15, consiste en el intercambio de dos mensajes: la solicitud de autenticación y la respuesta de autenticación. Antes de enviar una autenticación a la estación móvil, la red calcula los datos de autenticación: un desafío aleatorio RAND fresca, el testigo de autenticación AUTN, la autenticación esperado respuesta f2k (RAND), la clave de integridad IK y el cifrado CK clave (véase la Figura 2). Las funciones F1, F2, F3, F4 y f5, utilizados para calcular los parámetros de autenticación, se funciones criptográficas con clave compartida calcula utilizando la Kimsi tecla [8]. La función f1 de autenticación se utiliza para calcular el código de autenticación de mensaje MAC; f2 se utiliza para producir los parámetros RES respuesta de autenticación; la clave de funciones de generación, f3, f4 y f5 se utilizan para generar la clave de cifrado CK, la clave de integridad IK y el anonimato clave AK, respectivamente.

Figura 15: Autenticación y acuerdo de clave



[Fuente] IEEE Recuperado: New Privacy Issues in Mobile Telephony: Fix and Verification

Arquitectura femtocell:

A femtocell es un dispositivo que actúa como una pequeña estación base para mejorar la cobertura 3G y conectividad, especialmente en el interior edificios con mala cobertura de otro modo. Su radio de cobertura varía de 10 a 50 metros. Se conecta a los teléfonos móviles la red de la correspondiente MNO (Red Móvil Operador) mediante una conexión por cable a Internet existente proporcionado por el usuario femtocell, no el operador. Femtoceldas 3G, también llamado Home Nodo B (HNB) soporta la mayor parte del funcionalidades proporcionadas por una estación base típica 3G (nodo B), por ejemplo, capa física (señalización de radio) funciones. En adición, HNB establece un túnel seguro autenticado a través de Internet con la red del operador. Utilizando esta conexión cifrada, los delanteros de femtoceldas toda la radio la señalización y el tráfico generado por los usuarios al

GANC (GAN Controller), que está conectado a la red central de la para más detalles de la arquitectura de femtoceldas).

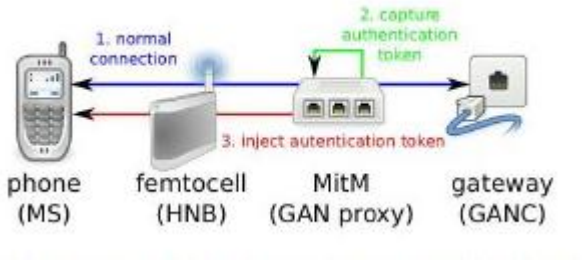
La comunicación entre el femtocell y el GANC se basa en el protocolo de red de acceso genérica (GAN).

El protocolo de GAN, fue diseñado originalmente para permitir móvil comunicación a través de puntos de acceso Wi-Fi. El protocolo era estandarizados byMNOs en 2004 [25], lo cual a la especificación GAN en 2005.

Esta especificación ha sido adoptada y ampliada para ser utilizado en entornos de femtoceldas.

El femtocell utiliza este protocolo para remitir la comunicación desde una estación móvil a través de la GANC a la red o vice versa. La MS no necesita ningún soporte especial GAN, simplemente se conecta a la femtocell de la misma manera ya que se conecta a una estación base estándar. El femtocell todos los mapas de capa 3señalización de mensajes y pases GAN basada en TCP / IP de radio ellos al GANC. Por lo tanto, de forma transparente encapsula todo tráfico generado por el teléfono y la red.

Figura 16: Configuración experimental Ataque



[Fuente] IEEE Recuperado: New Privacy Issues in Mobile Telephony: Fix and Verification

12.4 Libros

12.4.1 Las Telecomunicaciones y la Movilidad en la Sociedad de la Información:

SITUACIÓN ACTUAL DE LAS REDES MÓVILES

La situación actual de las redes móviles se caracteriza por la utilización de dos criterios de clasificación: el tipo de generación al que pertenecen (analógica, digital y multimedia), y el tipo de tecnologías y estándares que se emplean en los diferentes países. Dependiendo del país, es posible que coexistan sistemas pertenecientes a dos o tres generaciones distintas todavía en servicio.

La primera generación de las redes móviles corresponde a las comunicaciones basadas en tecnología analógica, centrad en el soporte a los servicios de voz y a los servicios de datos de muy baja tasa binaria (por ejemplo, la mensajería).

Desde el punto de vista tecnológico, esta generación se caracteriza por estar basado en soluciones propietarias desarrolladas por suministradores como Ericsson, NTT, Motorola o AT&T. Este tipo de redes llegó a contar con 20 millones de usuarios a principios de la década de los noventa.

La inexistencia de un estándar fue una de las razones que impulsaron el desarrollo de los sistemas de 2ª generación, especialmente en Europa, caracterizados por la utilización de tecnología de transmisión digital y por el soporte a los servicios de datos con velocidades binarias relativamente bajas (desde 9,6 kbit/s a 14,4 kbit/s). Su estudio y definición se inició a principios de los años 80, y las primeras redes comerciales aparecieron a principios de los 90. En esta fase se propusieron diferentes estándares para distintos tipos de aplicaciones. De este modo, sólo en

Europa, se desarrollaron los siguientes estándares:

Las Telecomunicaciones y la Movilidad en la Sociedad de la Información

- El estándar GSM para telefonía celular.
- El estándar DECT para telefonía inalámbrica.
- El estándar CT2 para telefonía inalámbrica.
- El estándar TETRA para telefonía móvil de uso privado o trunking.
- El estándar ERMES para mensajería.

■ El estándar MOBITEX para servicios de datos.

En Estados Unidos surgieron otros estándares de segunda generación, como TDMA y cdmaOne, en los que era un requisito básico la posible coexistencia con la tecnología analógica. Sin embargo, su expansión ha sido mecho menor durante la década de los noventa, debido probablemente al esquema de tarificación utilizado, en el que pagaba el usuario móvil que recibía la llamada, y al hecho de que no había un operador que proporcionara cobertura en todo el país.

Otro hecho que diferencia la situación de Estados Unidos, y los países que siguen su reglamentación, con la de Europa, fue la decisión de la FCC de subastar en el año 1994 los 140 MHz de espectro comprendidos entre 1.850 y 1.990 MHz para soportar los denominados servicios de comunicaciones personales o PCS (esta subasta, y su éxito en términos económicos, sentaron un precedente que tuvo pésimas consecuencias al ser imitado posteriormente en los procesos de asignación de espectro para los sistemas de tercera generación en muchos países europeos). Estos servicios no estaban ligados a la selección de una tecnología concreta. Al subastarse por áreas geográficas, dividiendo la superficie del país en 51 *Major Trading Areas* (MTAs) y 493 *Basic Trading Areas* (BTAs), no se crearon Operadores que proporcionaran cobertura nacional. Eso sí, el gobierno americano Consiguió recaudar 10.000 millones de dólares en el proceso (aunque la quiebra de una de las empresas que obtuvo más espectro, NextWave, daría lugar a una segunda subasta y a un embrollo jurídico que se ha resuelto recientemente).

La necesidad de unificar los distintos sistemas móviles descritos anteriormente (la mensajería, la telefonía inalámbrica, la telefonía celular y la telefonía móvil vía satélite), para resolver los problemas de compatibilidad entre los estándares de las distintas regiones geográficas y para definir unos sistemas con una eficiencia espectral más alta (ante la que se preveía escasez de espectro a corto plazo), impulsaron la investigación y el desarrollo de los sistemas de tercera generación.

En un principio, el enfoque que se promovió desde instituciones como la UIT o la Comisión Europea era que los nuevos sistemas 3G constituyeran el acceso inalámbrico a las redes de servicios integrados de banda ancha y que el soporte de la movilidad se basara en la utilización de las capacidades de la red inteligente. Es decir, se tendía hacia una convergencia entre las comunicaciones fijas y móviles. Para aumentar la eficiencia espectral se optó por considerar diversas variantes de CDMA y TDMA. Sin embargo, los temores del principal operador japonés, NTT DoCoMo, de que a medio plazo no dispondría de espectro suficiente

en su red 2G PDC para atender la creciente demanda, aceleraron el desarrollo de WCDMA. Por otro lado, la explosión de Internet hizo que en la evolución de la red troncal se contemplara como objetivo último el disponer de una red “todo IP”.

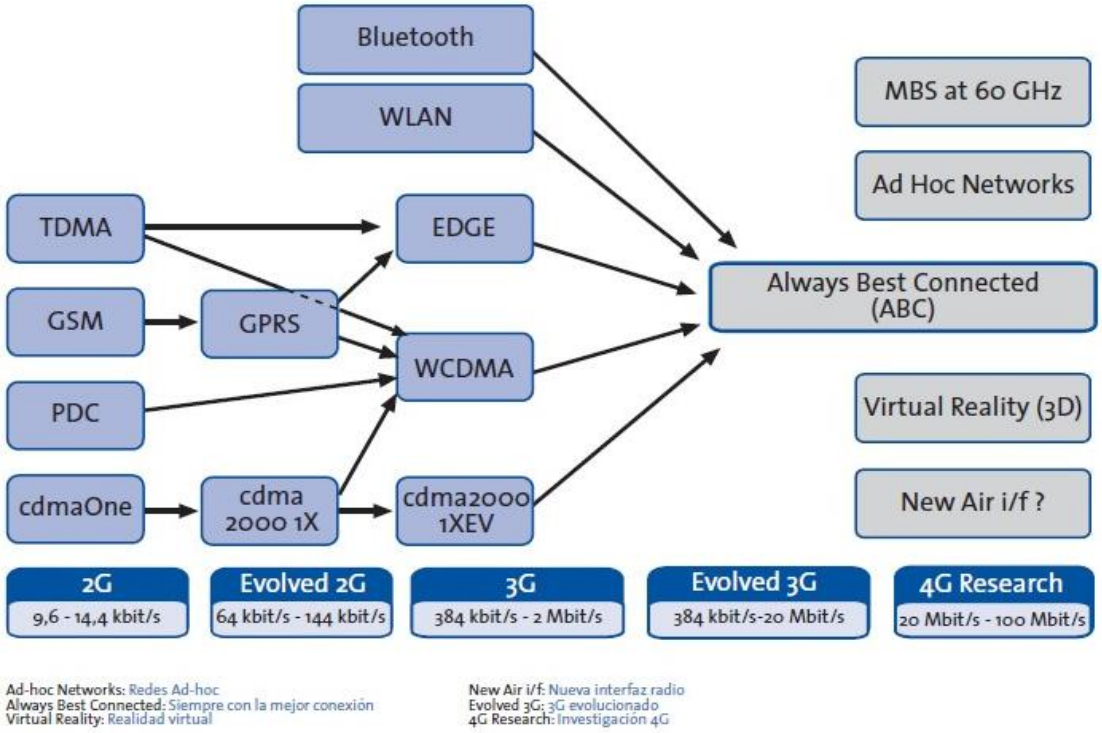
Figura 17: Tecnologías que utilizan los sistemas móviles de las distintas generaciones

	1G	2G	2,5G	3G
Europa	NMT, TACS	GSM900 & 1800, DECT	GPRS	UMTS (WCDMA), EDGE
Estados Unidos y Latinoamérica	AMPS	TDMA, cdmaOne, GSM850 & 1900	CDMA2000 1xRTT, GPRS	EDGE, CDMA2000 1xEV-DO
Japón	IMTS	PHS, cdmaOne, PDC	CDMA2000 1xRTT	FOMA, WCDMA, CDMA2000 1xEV-DO
China		GSM, cdmaOne	CDMA2000 1xRTT	TD-SCDMA

[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 34 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

La evolución técnica de los sistemas móviles se dirige a conseguir que soporten simultáneamente mayores tasas binarias y mayor movilidad. Para ello, el enfoque técnico se orienta, más que hacia el desarrollo de nuevas interfaces radio, hacia la convergencia entre los distintos tipos de redes radio que atienden a los servicios y requisitos existentes actualmente. En la Figura 2-6 se representa la visión de Ericsson respecto de esta posible evolución.

Figura 18: Evolución de las tecnologías hacia 4G



[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 35 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

LAS REDES 3G

La Unión Internacional de Telecomunicaciones (International Telecommunication Unit, ITU), en cooperación con otros organismos de la industria de telecomunicaciones de todo el mundo, es quien define y aprueba los requisitos técnicos y los estándares, así como la utilización del espectro radioeléctrico, de los sistemas 3G bajo el programa IMT-2000 (International Mobile Telecommunications-2000). El propósito final es facilitar la introducción de nuevas funcionalidades y proporcionar una evolución continua desde los sistemas de telecomunicaciones de segunda generación (2G) hacia la 3G.

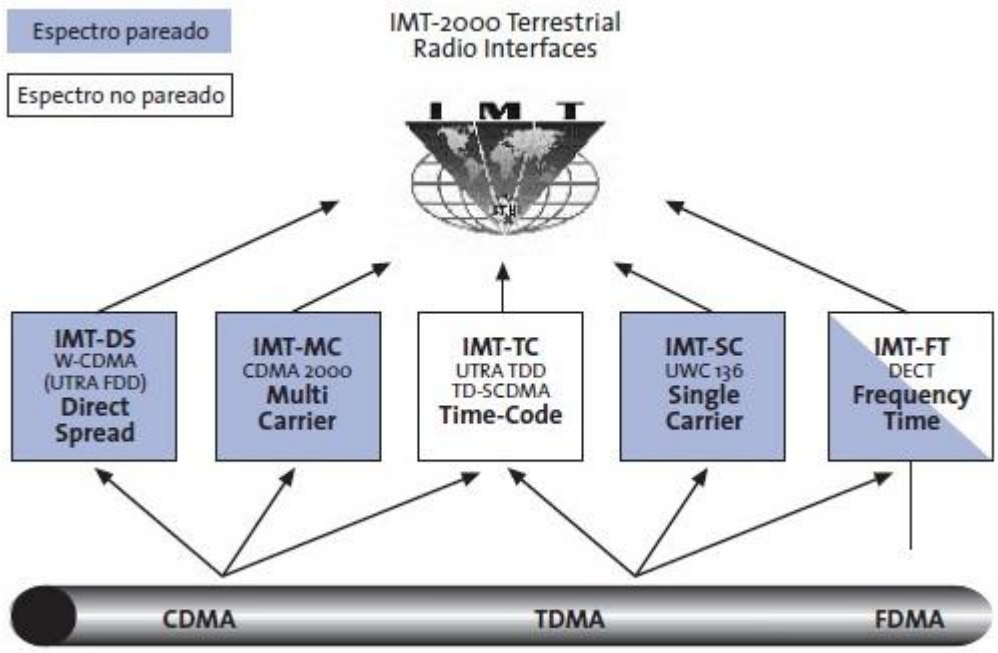
La ITU exige a las redes IMT-2000 (3G), entre otros requisitos, que proporcionen una mayor capacidad de sistema y una mayor eficiencia espectral con respecto a los sistemas 2G, que soporten servicios de transmisión de datos con una velocidad mínima de transmisión de 144 kbit/s en entornos móviles (de exterior) y de 2 Mbit/s en entornos fijos (en interiores). Basándose en estos requisitos, la ITU aprobó en el año 1999 cinco interfaces radio para la familia de estándares de IMT-2000, como parte de la recomendación ITU-R M.1457 [3.11], según se puede ver en la Figura 14. Las cinco tecnologías que componen la familia IMT-2000 son:

1. El sistema IMT-DS (Direct Sequence). Es ampliamente conocido como

UTRA FDD (UMTS Terrestrial *Radio Access FDD)*, y más comúnmente como WCDMA.

2. El sistema IMT-MC (Multicarrier*)*. Este sistema es la versión 3G del sistema IS-95 (también conocido como cdmaOne), y se suele denominar cdma2000.

Figura 19: Familia IMT-2000



[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 35 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

El sistema IMT-TC *(Time Code)*. Este sistema es el UTRA TDD. Se trata del modo UTRA que utiliza multiplexación por división en el tiempo.

4. El sistema IMT-SC *(Single Carrier)*. Esencialmente se trata de una manifestación particularizada de GSM Fase 2+, conocido como EDGE *(Enhanced Data Rates for GSM Evolution)*.

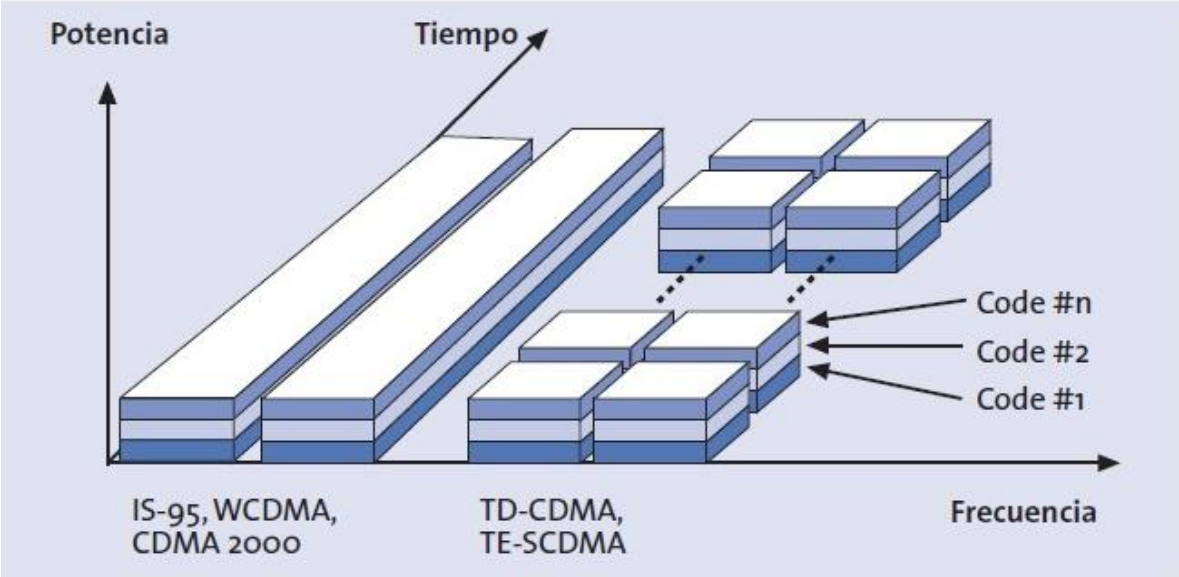
5. El sistema IMT FT *(Frequency Time)*. Este sistema se conoce como DECT *(Digital Enhanced Cordless Telecommunications)*.

En la Figura 20 se muestran los distintos sistemas de acceso múltiple, por división en el tiempo y/o en códigos.

En el punto siguiente se describe el sistema UMTS con cierto nivel de detalle.

Posteriormente se describe también el sistema cdma2000 y se analizan las principales diferencias entre ambos.

Figura 20: Acceso múltiple por división en el tiempo y/o códigos



[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 47 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

EL SISTEMA UMTS

Este apartado se centra en la descripción del sistema UMTS de forma general, con la intención de ofrecer una visión de conjunto. Para profundizar en alguno de los aspectos que aquí se mencionan, las redes UMTS se componen en realidad de dos grandes subredes:

- La red de telecomunicaciones
- La red de gestión.

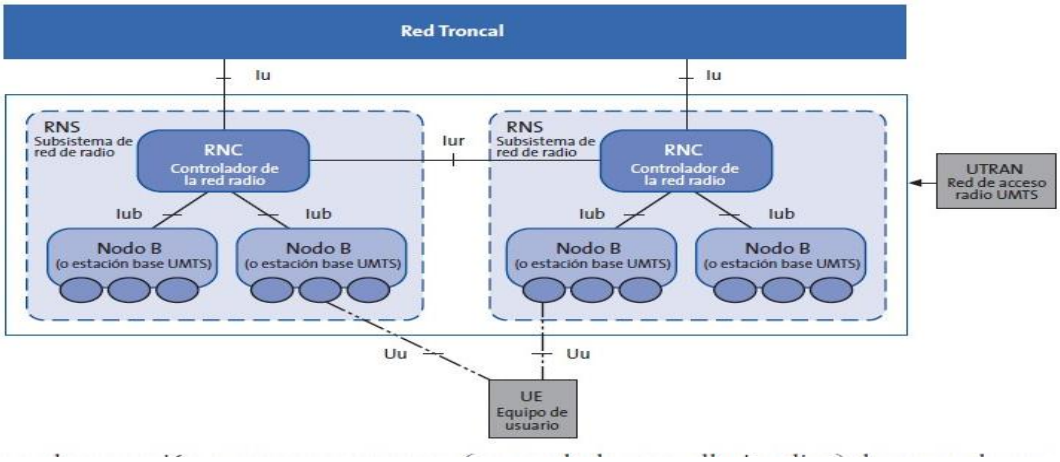
La primera se encarga de proporcionar la conexión extremo a extremo (con todo lo que ello implica); la segunda realiza la provisión de medios para la facturación y tarificación de los abonados, así como el registro y la definición de los perfiles de servicio, la seguridad y la operación de los elementos de red. Por sencillez, en

adelante se hablará de "red UMTS" para designar la red de telecomunicaciones del sistema.
Una red UMTS se compone de los siguientes elementos (ver la Figura 21):

■ El núcleo de red (core network).
■ La red de acceso radio (UTRAN).
■ Los terminales móviles.

Otra clasificación del sistema UMTS puede realizarse en relación a que se encuentre ligado o no al acceso. El sistema ligado al acceso incluye todos los protocolos que requieren de la intervención de la red de acceso radio. Por su parte el sistema no ligado al acceso abarca aquellos protocolos que conciernen al núcleo de red y al terminal móvil, sin que intervenga la red de acceso.

Figura 21: Arquitectura general de UMTS



[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 47 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

Núcleo de red

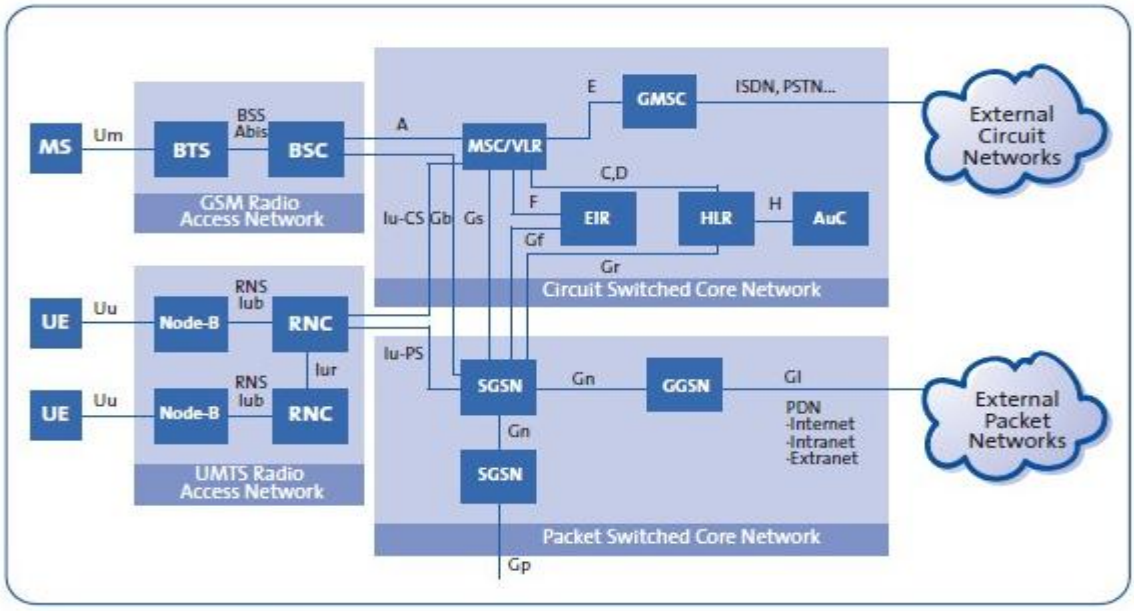
El núcleo de red incorpora funciones de transporte (de la información de tráfico y señalización, incluida la conmutación) y de inteligencia (aquí se incluye el encaminamiento, además de la lógica y el control de ciertos servicios, y la gestión de la movilidad).

En UMTS se ha buscado definir un núcleo de red universal, que pueda gestionar distintos tipos de red de acceso radio y conectarse a distintos tipos de redes fijas. En una primera fase se parte de la red troncal GSM, con lo que se busca minimizar costes y facilitar la evolución.

Como ocurría en GSM/GPRS, en la primera fase de UMTS el núcleo de red se ha dividido en dos dominios: el de conmutación de circuitos (Circuit Switch,CS) y el

de conmutación de paquetes (Packet Switch, PS). A través del modo CS se encaminarían los tráficos de voz y datos en modo circuito, y el modo PS haría lo propio con el tráfico de datos en modo paquete.

Figura 22: Elementos funcionales



GSM Radio Access Network: Red de acceso radio GSM
UMTS Radio Access Network: Red de acceso radio UMTS
Circuit Switched Core Network: Red troncal (conmutación de circuitos)
Packet Switched Core Network: Red troncal (conmutación de paquetes)
External Circuit Networks: Redes externas (por conmutación de circuitos)
External Packet Networks: Redes externas (por conmutación de paquetes)

[Fuente] Las Telecomunicaciones y la Movilidad en la Sociedad de la Información [2010] pág.: 48 Recuperado: División de Relaciones Corporativas y Comunicación de Telefónica I+D.

12.5 Tesis:

12.5.1 Trabajo de grado proyecto de aplicación práctica Conmutación de llamadas de voz ip entre redes 3G y wifi a través de un servidor sip (2013)

Los autores de este proyecto aplicado Alberto Patiño Hernández - Juan Pablo Robles Alarcón confirman que Según el boletín trimestral de las TIC en Colombia, correspondiente al cuarto trimestre del año 2012, el número de suscriptores a internet de banda ancha supera los seis millones de abonados, de los cuales se estima que el 36.9% de los accesos se realiza a través de redes móviles de tercera generación (3G), mientras que el 62.5% representa conexiones de banda ancha fijas.

Servidor SIP

El servidor SIP permite la creación y modificación de los usuarios y de sus características. En éste se asigna el número de extensión que utilizará cada usuario y su contraseña.

El SIP Register se encarga de la autorización y el registro de los clientes y el SIP Proxy realiza el enrutamiento de todos los mensajes hacia su destino, controlando la señalización durante el establecimiento de la llamada. El servidor solo genera mensajes de respuesta a las peticiones que realizan los agentes cliente (ej. 200 OK, 100 Trying).

Debido al esquema de red diseñado, mostrado más adelante en la sección 3.3, se implementa en el servidor SIP el RTP Proxy, el cual realiza el enrutamiento de todos los paquetes multimedia (voz) una vez se establece la conexión de una llamada. El RTP Proxy conoce la dirección de contacto de los usuarios mediante la información contenida en los mensajes INVITE y 200 OK que envía la aplicación durante el establecimiento de la comunicación.

ELASTIX®

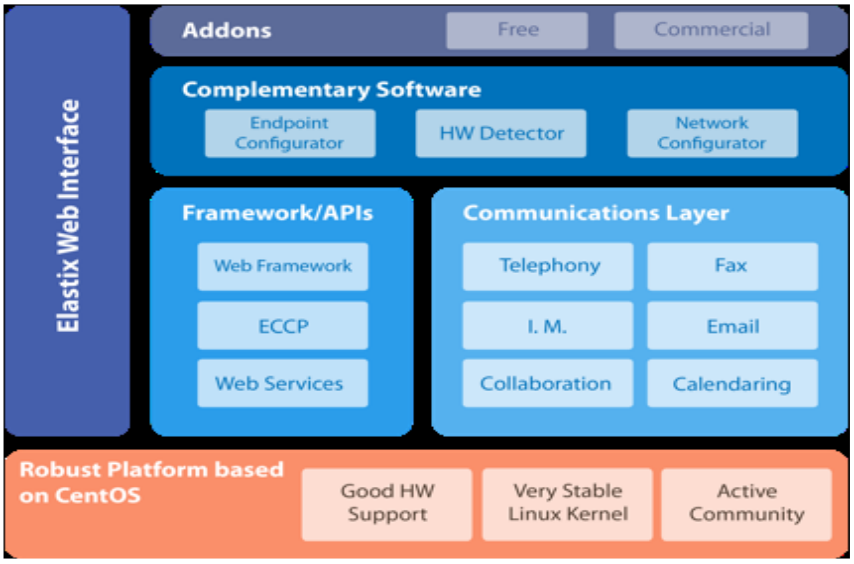
Elastix es una distribución de software libre de un servidor de comunicaciones unificadas, el cual integra en un solo paquete:

- VoIP PBX
- Fax
- Mensajería Instantánea
- Email

Elastix implementa gran parte de su funcionalidad sobre cuatro programas de software muy importantes como son Asterisk, Hylafax, Postfix y Openfire. Estos programas brindan las funciones de PBX, Fax, Email y Mensajería Instantánea, respectivamente. El sistema operativo se basa en la popular distribución de Linux orientada a servidores llamada CentOS [19]

Asterisk es uno de los componentes más importantes de Elastix y quien provee la mayoría de las características telefónicas de la distribución. Dada la importancia de Asterisk para el sistema y específicamente para la solución del presente trabajo de grado, se destacan en la siguiente sección sus características más relevantes.

Figura 23: Esquema general de los componentes de Elastix.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 Esquema de Red [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

En la Figura 23 se muestra la estructura de Elastix, sus componentes y su relación entre sí. Como se puede apreciar, la interface Web de Elastix, recoge todas las funcionalidades que éste provee y brinda un entorno común para la administración de los servicios y la integración de los mismos.

Los principales programas que conforman el núcleo de Elastix en su versión 2.4.0 y que brindan sus principales funcionalidades son:

[19] Una distribución Linux (coloquialmente llamada distro) es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios

- Asterisk (V. 1.8.20)
- vTigerCRM® and SugarCRM® – Sistemas de CRM.
- A2Billing® – Plataforma de tarjetas de llamadas y facturación para Asterisk.
- Flash Operator Panel – Consola de Operadora vía Web.
- Hylafax® – Sistemas de faxes.
- Openfire® – Servidor de mensajería instantánea.
- FreePBX® (V. 2.8.1-16) – Interface de administración Web de Asterisk y componente esencial en Elastix.
- Sistemas de Reportes – Información detallada de las operaciones de la PBX.
- OSLEC – Cancelador de Eco basado en Software.
- Postfix® – Servidor de correos.
- CentOS (V. 5.9) – Sistema Operativo.

ASTERISK®

Asterisk es un programa de software libre bajo licencia GPL que proporciona funcionalidades de central telefónica PBX, capaz de convertir un computador ordinario en un servidor de comunicaciones.

Asterisk es un programa rico en características y funcionalidades, como se detalla en su página web, dentro de las cuales podemos destacar:

- Autenticación
- Registro de llamadas detallado
- Desvío de llamadas
- Monitoreo de llamadas
- Enrutamiento de llamadas (DID y ANI)
- Transferencia de llamadas
- Identificador de llamadas
- Integración de base de datos
- Marcado por nombre
- Canalización
- VoIP Gateways
- Correo de Voz

Aplicación Móvil

La aplicación móvil actúa como cliente para el servidor; ésta permite la creación de cuentas de usuario donde es posible configurar los datos de conexión al servidor y la información de autorización (usuario y contraseña).

La aplicación móvil es la encargada de realizar todo el proceso de registro del usuario en el servidor y es quien genera todos los mensajes de petición (ej. REGISTER, INVITE, etc.).

Para efectos de la conmutación de la llamada, es la aplicación quien se encarga de comunicar al servidor la modificación de los parámetros de la sesión, es decir, es la aplicación quien informa al servidor el cambio de red enviando su nueva dirección IP de contacto.

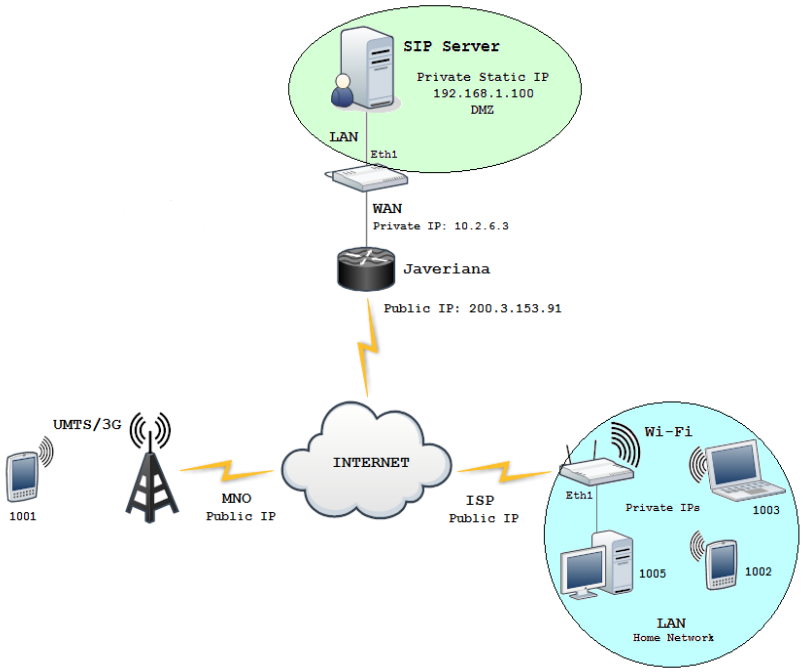
SIPDROID

SIPDroid es un cliente VoIP disponible para dispositivos Android que utiliza el protocolo SIP. Es un software de código abierto, bajo licencia GPL desarrollado completamente en Java (Android) y que brinda múltiples posibilidades para la comunicación, entre ellas:

- Formato de cambio de número
- Soporte de varios modos de tonos DTMF7
- Soporte para NAT (traducción de direcciones de red)
- Llamadas salientes simultáneas
- Enmascaramiento para llamadas anónimas
- Enrutamiento para llamadas entrantes basado en tiempo
- Transferencia de llamadas asistido
- Conferencias
- Recepción de vídeo

12.6 ESQUEMA DE RED

Figura 24: Diagrama de red.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 Esquema de Red [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

La Figura 24, muestra el esquema de red que se implementa para el desarrollo del proyecto. El servidor SIP se encuentra ubicado dentro de una red local con dirección IP estática privada y es exhibido a la red externa en una zona desmilitarizada (DMZ).

Por medio de la interfaz WAN del enrutador, se conecta el servidor con la red interna de la Pontificia Universidad Javeriana, para después salir a internet por medio de una dirección IP pública estática, asignada para este desarrollo.

Los dispositivos en cualquier red externa acceden al servidor y establecen una conexión a través de internet, bien sea por medio de la red 3G de un MNO[20] o de una red doméstica provista por un ISP[21].

Es preciso notar que la comunicación entre el servidor SIP y cualquier dispositivo cliente utilizado para realizar la conexión, está bajo el efecto de múltiples traducciones de direcciones de red por medio de NAT[22]

[20] Mobile Network Operator
[21] Internet Service Provider
[22] Network Address Translation

13 Análisis y conclusiones del estado del arte de las tecnologías disponibles para realizar control sobre el abonado mediante DDos, así como la legislación actual en telecomunicaciones y uso de terminales móviles en Colombia.

En los trabajos que se han analizado podemos encontrar que existen diferentes formas para poder tener un control mayor sobre los abonados de un red móvil, pero desafortunadamente en nuestro país esto aún no es posible por las tecnologías que se están usando en la actualidad como lo son las redes 3G o por que las compañías de celulares en nuestro país no ven esta opción como un buen negocio en cuanto a las políticas tarifarias, en países como España que ya se habla de la nueva generación de las telecomunicaciones y la llegada de las redes 4G o cuarta generación, que no es otra cosa que la interconexión entre la red 3G (UMTS) y la WLAN usando el protocolo de comunicación QoS, 802.11, para así poder determinar políticas en gestión de la red usando la red de datos como el canal preferido de comunicación de voz y dejándole a esta la movilidad al usuario de telefonía la libertad de desplazarse a cualquier lugar del mundo donde exista la red de redes internet sin necesidad de entrar costos adicionales como el roamming internacional, además de poder controlar el acceso a la red al abonado desde un servidor dedicado para ello como un SIP o mediante el protocolo de comunicación Proxy Mobile IPv6, esto gracias a una denegación de servicios producida por el servidor esta entidad puede ser un servidor de acceso a la red (NAS),el cual permite o no estar en la red al usuario por medio de la asignación de una dirección IP o negación de esta.

Teniendo un esquema de políticas propuesto para un ambiente de redes integrado UMTS – WLAN tendríamos lo siguiente:

14 COMUNICACIÓN ENTRE REDES 3G

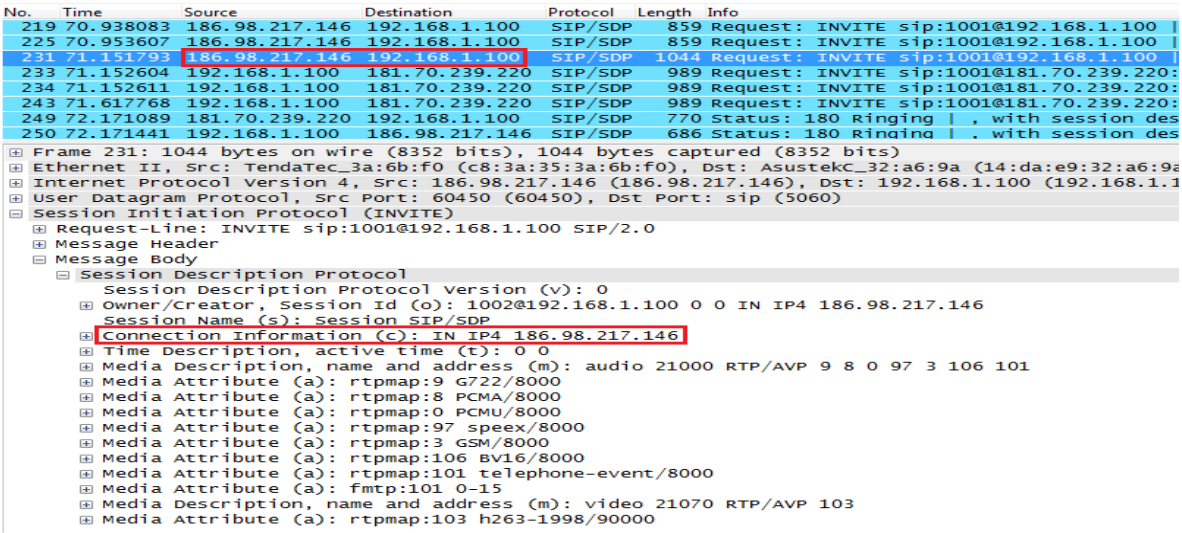
Kamailio permitió establecer una comunicación estable y de buena calidad cuando ambos dispositivos se encontraban conectados a redes 3G, como se muestra a continuación.

El servidor recibe el mensaje INVITE originado por el usuario 1002 y lo redirige al usuario 1001. Dado que este mensaje es de tipo SIP/SDP, en él se envía la información de conexión del cliente, indicando la dirección IP por medio de la cual recibirá los paquetes multimedia (voz). El servidor reenvía el mensaje INVITE, así quien recibe la solicitud de llamada obtiene la dirección IP de contacto de quien origina la comunicación.

La Figura 6 muestra el envío del mensaje INVITE al servidor por parte del usuario 1002, siendo este el que origina la llamada y la Figura 7 la redirección del mensaje al usuario 1001, quien recibe la solicitud para el establecimiento de la comunicación. En ambas figuras se destaca la información de contacto contenida en el SDP del mensaje enviado por 1002 y recibido por 1001.

El resultado de la llamada entre dos clientes conectados a redes 3G se aprecia en el flujo de mensajes que atraviesan el servidor durante todo el proceso de establecimiento, comunicación y finalización de la conexión, mediante el uso de Wireshark.[23]

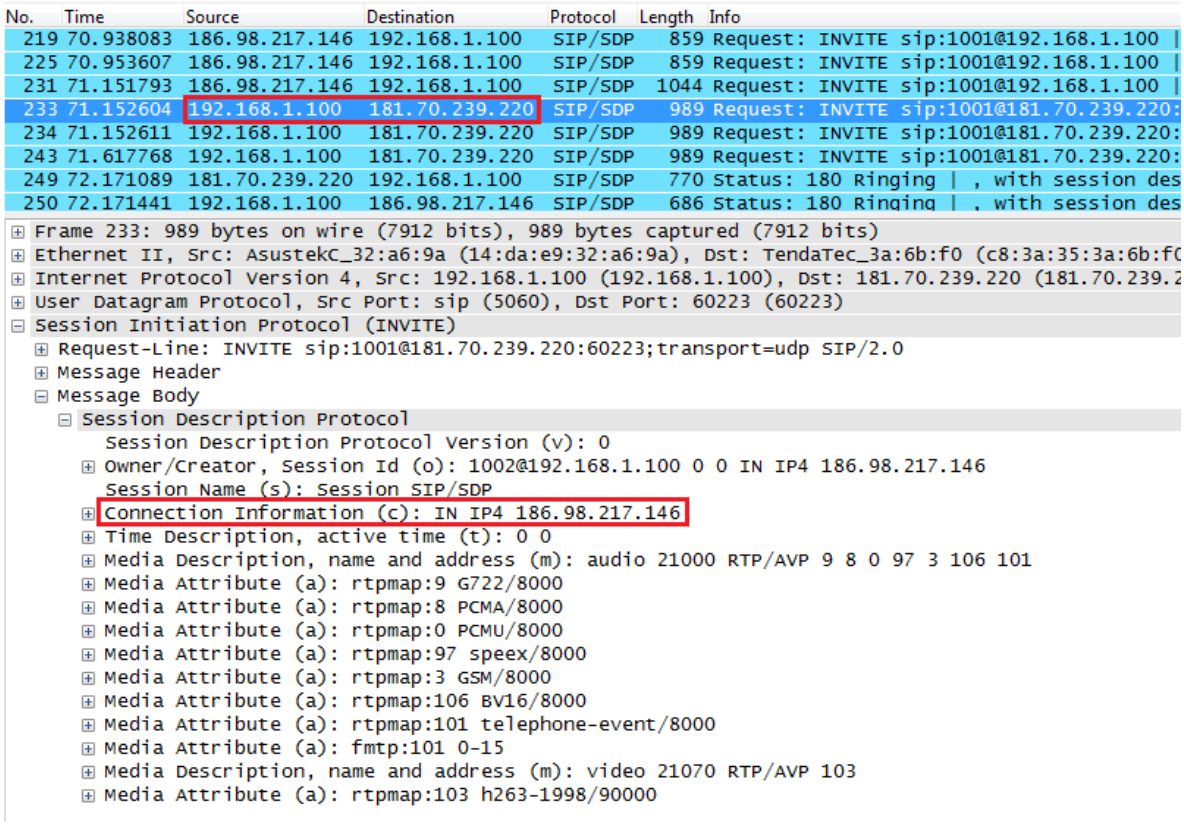
Figura 25: INVITE 3G de 1002 al servidor Kamailio.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN INVITE 3G de 1002 al Servidor Kamailio [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

[23] Programa de captura de las tramas de una red. Analizador de paquetes y protocolos

Figura 26: INVITE 3G del servidor Kamailio a 1001.

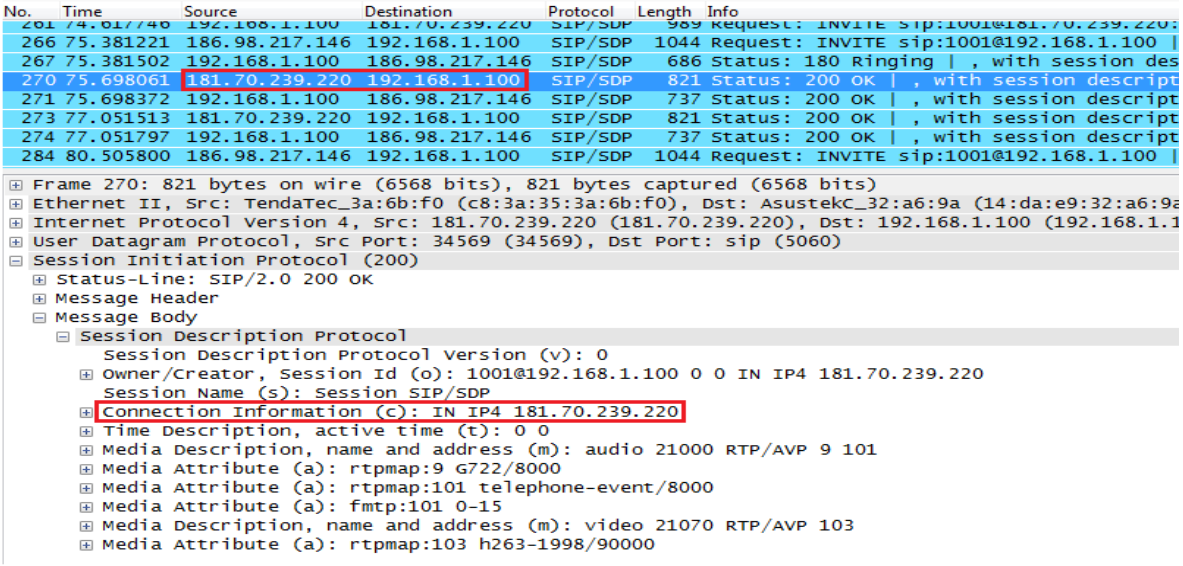


[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES. INVITE 3G del Servidor Kamailio a 1001 [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

Cuando el usuario 1001 recibe la solicitud y contesta la llamada, envía un mensaje 200 OK de tipo SIP/SDP de la misma forma como el usuario 1002 envió el mensaje INVITE. En el momento en el cual el usuario 1002 recibe el mensaje 200 OK por parte del servidor, extrae la información de contacto del usuario 1001 contenida en el SDP, permitiéndole iniciar la transmisión de paquetes de voz. El proceso es el mismo al explicado anteriormente y el flujo de mensajes se muestra en las Figuras 8 y 9.

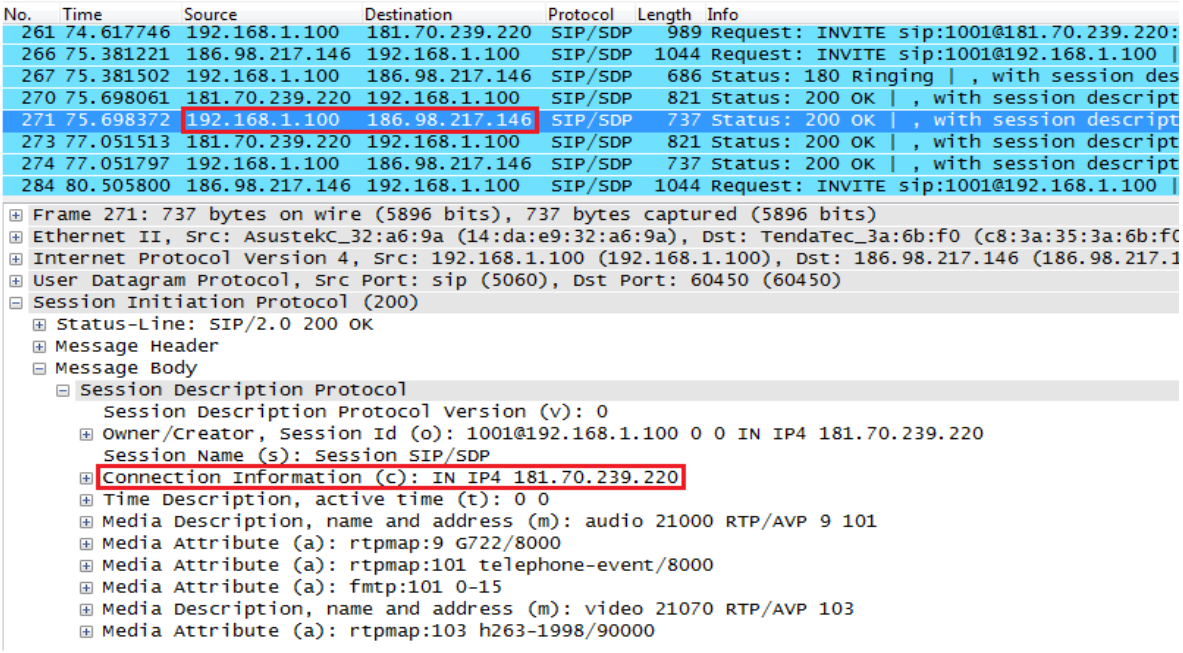
De esta forma se logró realizar una llamada exitosa, a través del servidor Kamailio, transmitiendo los paquetes de voz directamente de un cliente a otro. Como ambos usuarios obtienen la dirección pública de su contraparte y ésta es un identificador único para un dispositivo en una red 3G, el servidor RTP nunca entra en funcionamiento, haciendo que los clientes envíen directamente el contenido multimedia de un extremo de la comunicación al otro.

Figura 27:200 OK 3G de 1001 al servidor Kamailio.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES. . 200 OK 3G de 1001 al Servidor Kamailio [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

Figura 28:200 OK 3G de 1001 al servidor Kamailio.



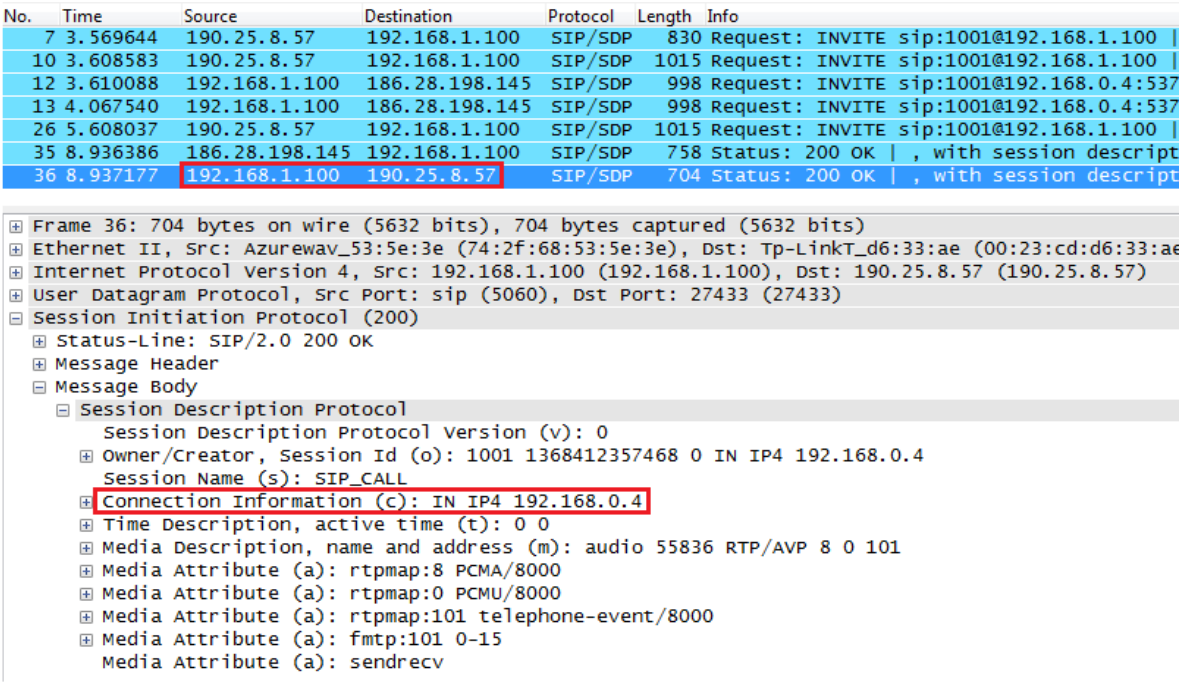
[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES. . 200 OK 3G de 1001 al Servidor Kamailio [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

15 CONMUTACIÓN DE LLAMADA – 3G A WIFI

En esta prueba, el usuario 1001 y el usuario 1002 se encuentran conectados a través de la red de datos 3G de dos operadores móviles. El usuario 1002 inicia la llamada por medio del envío al servidor de un mensaje INVITE que contiene en el SDP su dirección IP pública de contacto (Figura 29). El servidor modifica la información suministrada por el cliente 1002 y establece la dirección de contacto como su propia IP pública (Figura 30). Cuando el usuario 1001 recibe la solicitud de llamada, toma la IP pública del servidor como la dirección a la cual debe enviar los paquetes de voz durante la comunicación. El mensaje 200 OK que se envía al contestar la llamada (Figura 31) es igualmente modificado por el servidor, estableciendo la dirección de contacto del usuario 1001 como su propia IP pública (Figura 32).

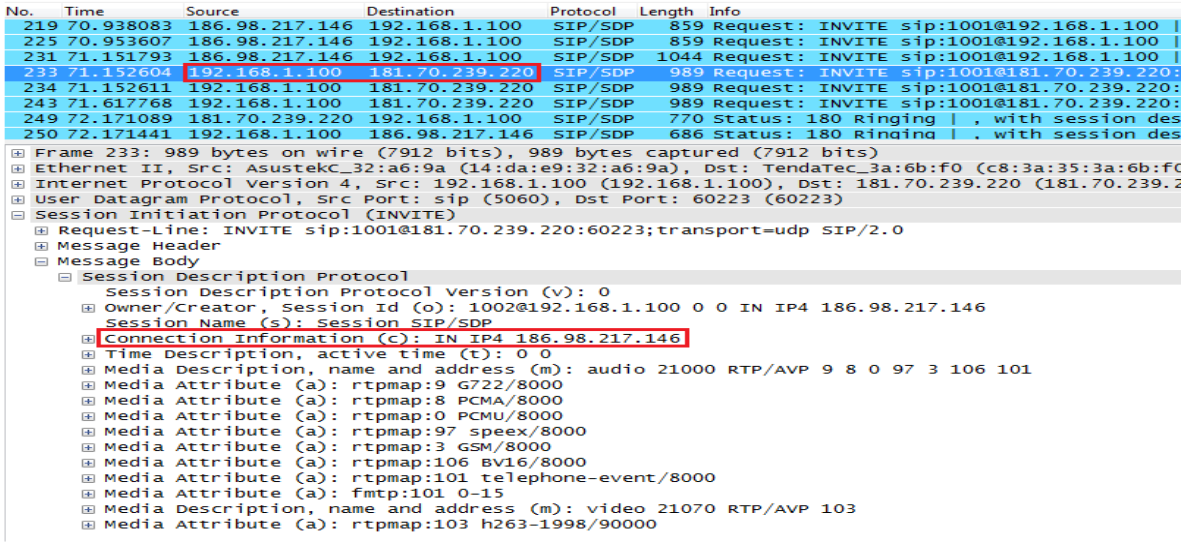
En este caso, el dispositivo que se encuentra dentro de la LAN de una red WiFi con una dirección IP privada, conmuta a una red 3G la cual le asigna una IP pública que identifica exclusivamente a esa terminal en internet.

Figura 29:200 OK WiFi del servidor Kamailio a 1002



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 200 OK WiFi del Servidor Kamailio a 1002 [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

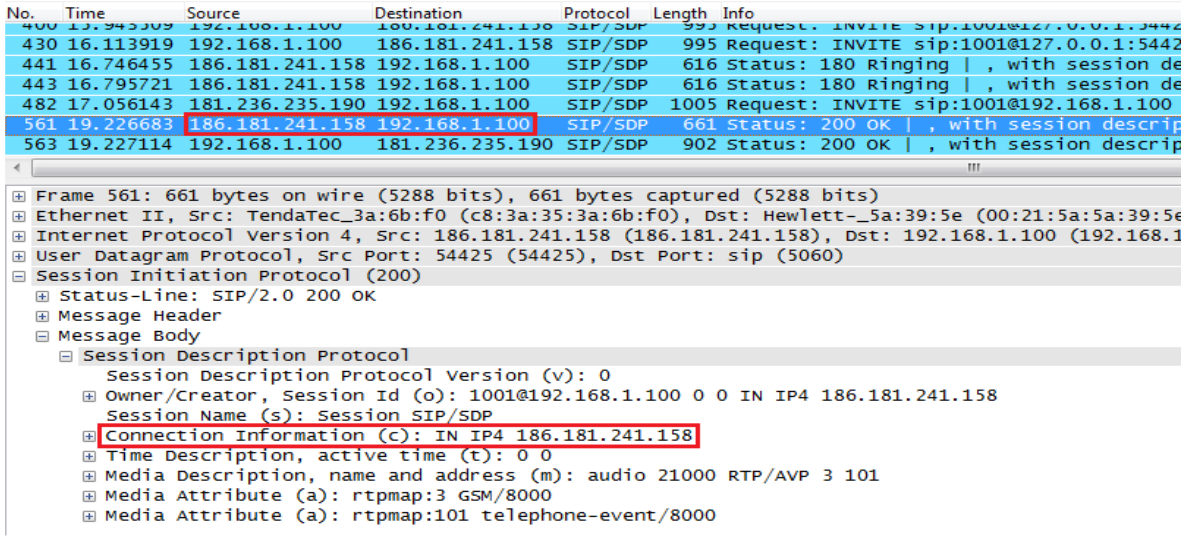
Figura 30: INVITE 3G del servidor Elastix a 1001



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 INVITE 3G del Servidor Elastix a 1001. [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

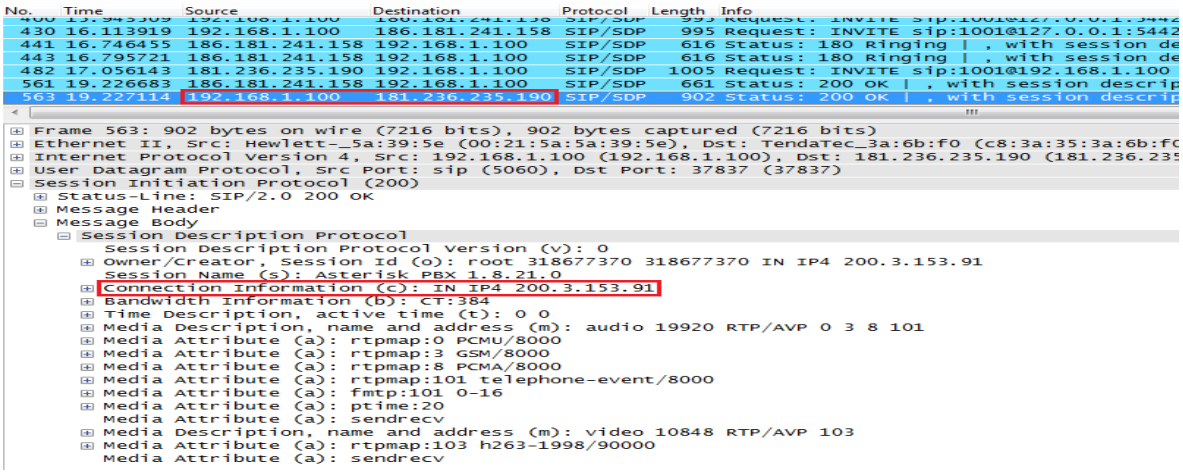
Cuando la conexión se ha establecido y los paquetes de voz se están enviando correctamente desde un extremo de la comunicación al otro, el usuario 1001 conmuta y se conecta a una red WiFi.

Figura 31:200 OK 3G de 1001 al servidor Elastix.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 200 OK 3G de 1001 al Servidor Elastix. [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

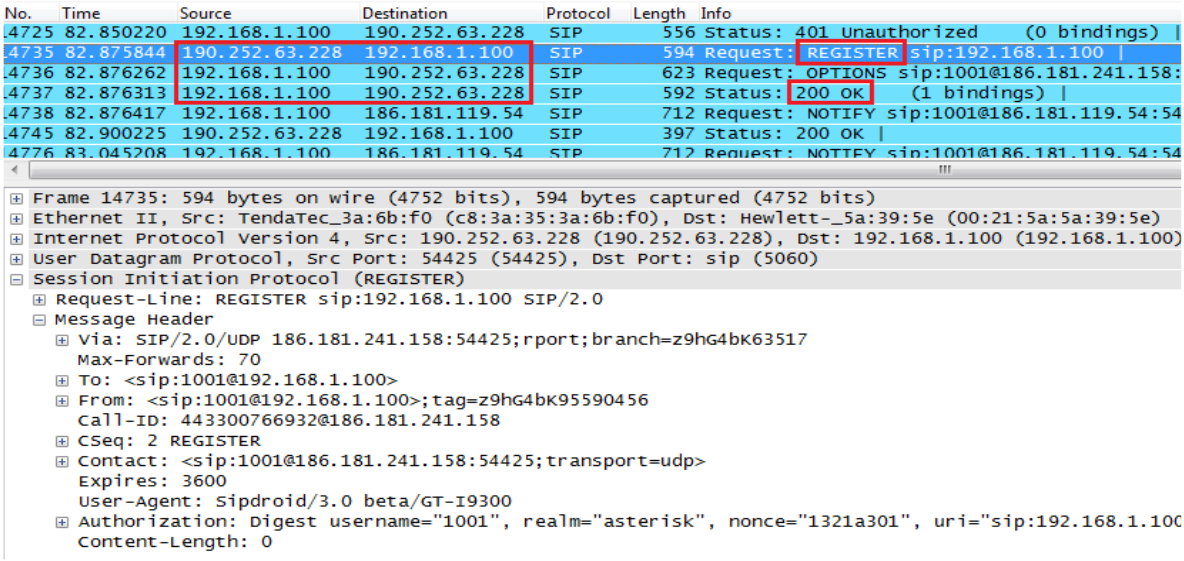
Figura 32: 200 OK 3G del servidor Elastix a 1002.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 200 OK 3G del Servidor Elastix a 1002. [Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

La Figura 33 muestra el envío del mensaje REGISTER por parte del usuario 1001 al servidor, actualizando la dirección IP de contacto con la que había establecido la conexión a través de la red 3G. Al conectarse a una red WiFi, el usuario adquiere una dirección IP privada, pero dado que el otro usuario está enviando los paquetes de voz al servidor, este nunca se entera de la conmutación de red que efectúa el cliente 1001 y por lo tanto la llamada se mantiene activa.

Figura 33: Mensaje REGISTER WiFi al conmutar de red.

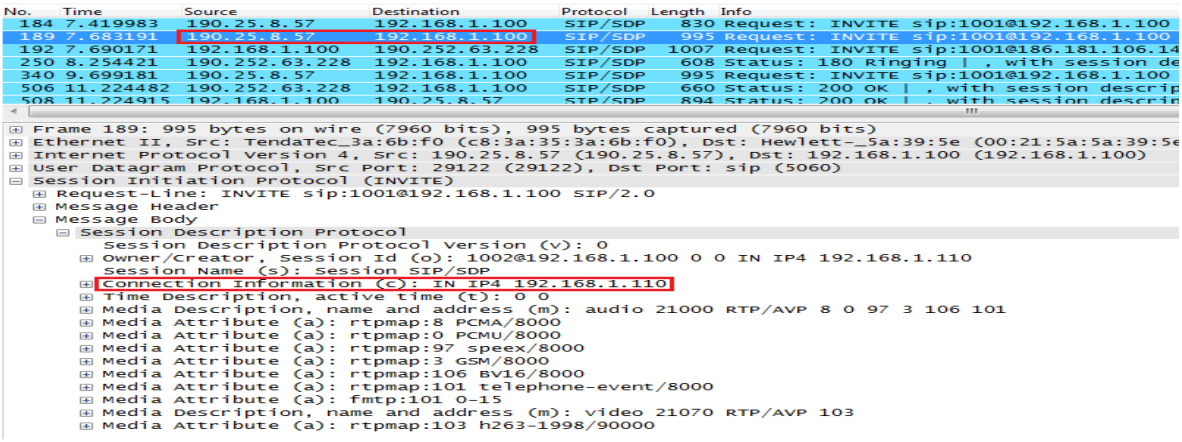


[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 REGISTER WIifi al conmutar de red.[Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

16 CONMUTACIÓN DE LLAMADA – WIFI A 3G

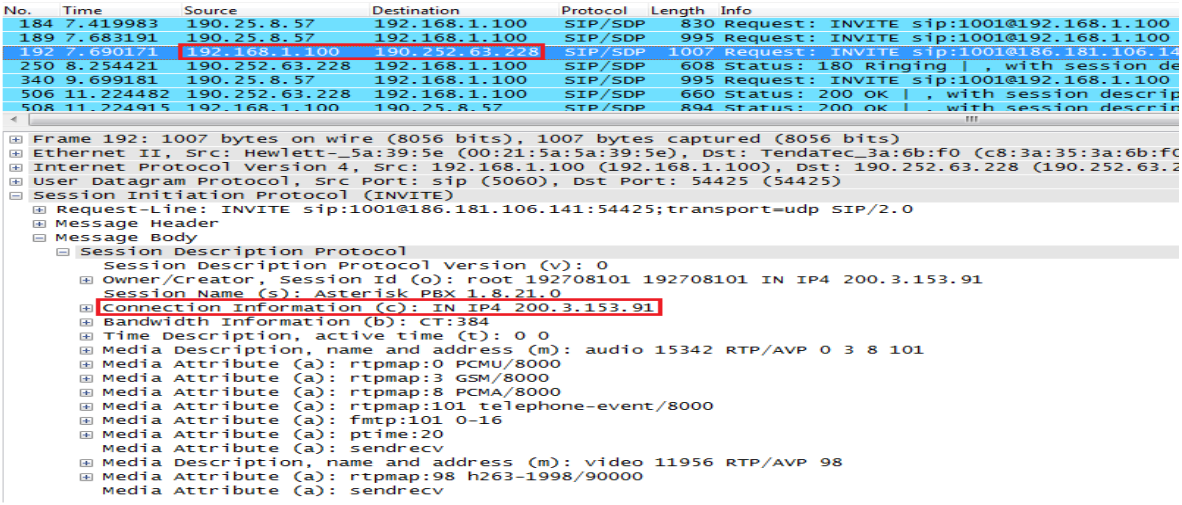
El proceso de conmutación de una llamada desde la red WiFi a una red 3G es igual al explicado anteriormente en la sección 5.2.1, donde se detalla el proceso de conmutación de la llamada desde una red 3G a una red WiFi. En este caso, el dispositivo que se encuentra dentro de la LAN de una red WiFi con una dirección IP privada, conmuta a una red 3G la cual le asigna una IP pública que identifica exclusivamente a esa terminal en internet.

Figura 34: INVITE WiFi de 1002 al servidor Elastix.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 INVITE WiFi de 1002 al Servidor Elastix.[Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

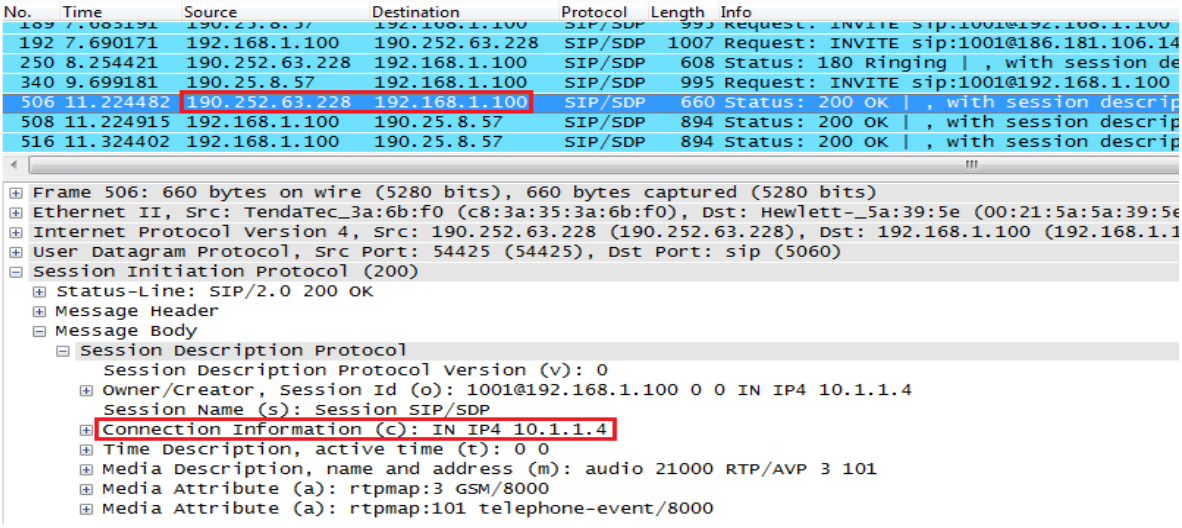
Figura 35: INVITE WiFi del servidor Elastix a 1001.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 INVITE WiFi del Servidor Elastix a 1001.[Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

En este punto de la conexión el usuario 1001 hace conexión exitosa (OK) con el servidor Elastix en la red wifi

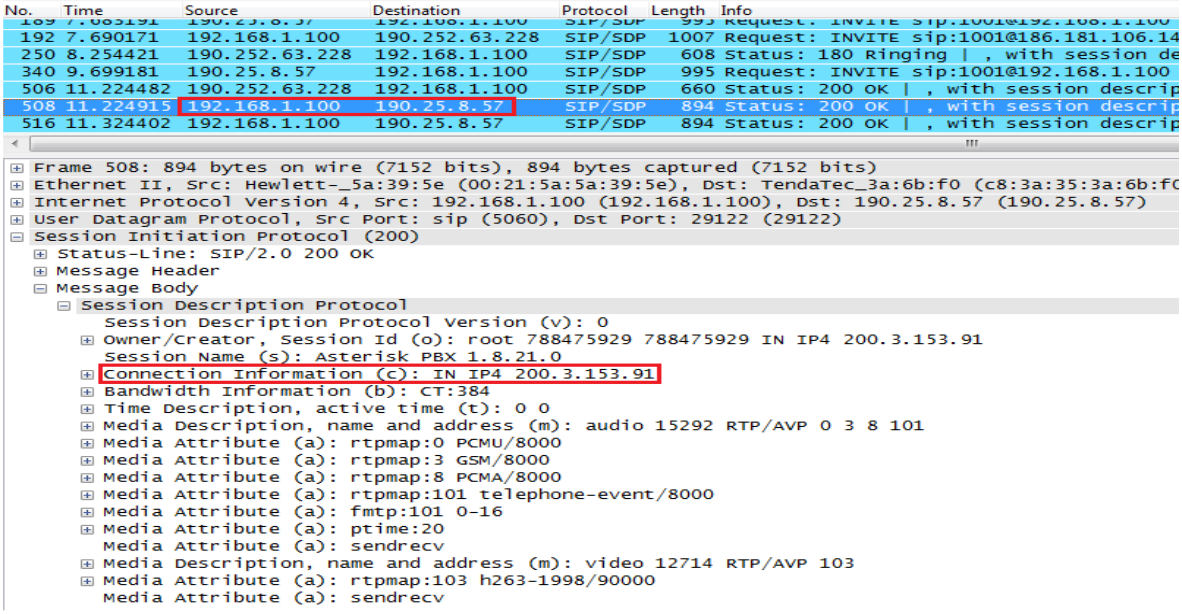
Figura 36: 200 OK WiFi de 1001 al servidor Elastix.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 200 OK WiFi de 1001 al Servidor Elastix.[Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

En este punto de la conexión el servidor Elastix conexión exitosa (OK) con el usuario 1001 en la red wifi

Figura 37:200 OK WiFi del servidor Elastix a 1001.



[Fuente] NICOLÁS ALBERTO PATIÑO HERNÁNDEZ -JUAN PABLO ROBLES ALARCÓN 2013 200 OK WiFi del Servidor Elastix a 1001.[Fuente] Recuperado: CONMUTACIÓN DE LLAMADAS DE VOZ IP ENTRE REDES 3G Y WIFI A TRAVÉS DE UN SERVIDOR SIP TRABAJO DE GRADO PROYECTO DE APLICACIÓN PRÁCTICA PONTIFICIA UNIVERSIDAD JAVERIANA

Las Figuras 29 y 30 son equivalentes a las Figuras 25 y 26 mostradas en la comunicación entre redes 3G. Su diferencia radica en que el mensaje INVITE que envía el usuario 1002 al servidor es enviado desde una red WiFi con su IP privada, la cual es traducida, a la dirección IP pública del servidor antes que el mensaje sea redirigido al usuario 1001.

De igual forma, las Figuras 31 y 32 son equivalentes a las Figuras 27 y 28, donde se muestra el mensaje 200 OK que se envía al contestar la llamada.

17 LEGISLACIÓN ACTUAL EN NUESTRO PAÍS EN EL TEMA DE TELECOMUNICACIONES MÓVILES.

17.1 Ley 1341 del 30 de Julio de 2009

El ministerio de telecomunicaciones legislo la ley de julio 30 de 2009

"POR LA CUAL SE DEFINEN PRINCIPIOS Y CONCEPTOS SOBRE LA SOCIEDAD DE LA INFORMACIÓN Y LA ORGANIZACIÓN DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TIC-, SE CREA LA AGENCIA NACIONAL DE ESPECTRO Y SE DICTAN OTRAS DISPOSICIONES"

ARTICULO 4.- INTERVENCIÓN DEL ESTADO EN EL SECTOR DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

1. Proteger los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios.

2. Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal.

3. Promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del gobierno en línea.

4. Promover la oferta de mayores capacidades en la conexión, transporte y condiciones de seguridad del servicio al usuario final, incentivando acciones de prevención de fraudes en la red.

5. Promover y garantizar la libre y leal competencia y evitar el abuso de la posición dominante y las prácticas restrictivas de la competencia.

6. Garantizar el despliegue y el uso eficiente de la infraestructura y la igualdad de oportunidades en el acceso a los recursos escasos, se buscará la expansión, y cobertura para zonas de difícil acceso, en especial beneficiando a poblaciones vulnerables.

7. Garantizar el uso adecuado del espectro radioeléctrico, así como la reorganización del mismo, respetando el principio de protección a la inversión, asociada al uso del espectro. Los proveedores de redes y servicios de

telecomunicaciones responderán jurídica y económicamente' por los daños causados a las infraestructuras.

8. Promover la ampliación de la cobertura del servicio.

9. Garantizar la interconexión y la interoperabilidad de las redes de telecomunicaciones, así como el acceso a los elementos de las redes e instalaciones esenciales de telecomunicaciones necesarios para promover la provisión y comercialización de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones.

10. Imponer a los proveedores de redes y servicios de telecomunicaciones obligaciones de provisión de los servicios y uso de su infraestructura, por razones de defensa nacional, atención y prevención de situaciones de emergencia y seguridad pública.

11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones.

12. Incentivar y promover el desarrollo de la industria de tecnologías de la información y las comunicaciones para contribuir al crecimiento económico, la competitividad, la generación de empleo y las exportaciones.

13. Propender por la construcción, operación y mantenimiento de infraestructuras de las tecnologías de la información y las comunicaciones por la protección del medio ambiente y la salud pública

18 CONCLUSIONES

- Se Estructuro el estado del arte de las redes 3G Y 4G así como su comunicación identificando que las redes de cuarta generación proporcionan mejores condiciones de administración y gestión así como de servicios a los usuarios de la red basados en políticas específicas.

- Se Analizó las diferentes vulnerabilidades que presentan las redes 3G (UMTS) y 4G para poder aprovecharlas y combatir el crimen organizado desde las penitenciarías del país.

- Se Demostró que las redes 4G son más administrables que las 3G logrando tener un mayor control y monitoreo sobre los usuarios de los operadores celulares en nuestro país.

- Se Identificó los diferentes dispositivos y elementos necesarios para configurar una red UMTS Y 4G.

- Se Reconoció la importancia de la seguridad informática en la protección de redes de datos y voz tanto wifi como UMTS.

- Se Reconoció la normatividad legal en materia de telecomunicaciones en el país.

19 BIBLIOGRAFÍA

LIBROS

- SEPÚLVEDA L, R.: Protocolo de enlace de datos para la confidencialidad y la autenticidad de las comunicaciones. Tesis doctoral, La Habana, Cuba, 1998.
- 2. SCHNEIER, B: Applied Cryptography Second Edition: protocols, algorithms, and source code in C, 1996. http://www.Enginetools.tsx.org.
- ÁLVAREZ CALVO M, TERESA APARICIO PEÑA M, Las Telecomunicaciones y la Movilidad en la Sociedad de la Información Madrid España Edición: División de Relaciones Corporativas y Comunicación de Telefónica I+D
- 4. RAINBOW TECHNOLOGIES: Sentinel SuperPro 6.0. Developers's Guide, Junio. 2000. http://www.SafeNet-Inc.
- INSTITUTO ROSARISTA DE ACCIÓN SOCIAL –SERES–, Desarrollo del sistema penitenciario y carcelario colombiano entre 1995 y 2010, en el marco de las políticas de Estado a partir de las sentencias de la Corte Constitucional. Universidad del Rosario. – Bogotá: Editorial Universidad del Rosario, 2011. 322 p.
- 6. DMITREV, VL: "Teoría de Información Aplicada". Editorial MIR, Moscú, 1989.
- 7. LAI X, MASSEY J.: "Hash Functions Based on Block Ciphers", Advances in Cryptology - EUROCRYPT'92 Proceedings, Springer- Verlag, 1992. pp. 55-70.
- 8. PRENEEL, B.: "Análisis and Design of Cryptographic Hash Functions", PhD.Dissertation, Katholieke Universiteit Leuven, Jan 1993.
- 9. DAEMEN J, RIJMEN V: The Rijndael Block Cipher. AES Proposal. http://www.esat.kuleuven.ac.be/~rijmen/rijndael/.

ARTICULOS

- J. A. GUERRERO Y A. BARBA. Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN, JUNE 2008, pp 229-234

- ALTOLINI, D. "Preamble-based Channel Estimation in HomePlug AV Systems", En: IEEE Power Line Communications and Its Applications International Symposium, Mar 2012, pp 176-181

- ANATORY, J., "Powerline Communications. The Effects of Branches on Network Performance", En: IEEE Power Line Communications and Its Applications International Symposium, 2006, pp 70-75

- ANATORY, J.,Trends in telecommunication services provision: powerline network can provide alternative for access in developing countries, En: 7th AFRICON Conference in Africa, vol. 1, Sep 2004, pp 601-606

- BABIC M. et Al, “Theoretical postulation of PLC channel model”, En:Tech. Rep., OPERA, March 2005

- BAL, G., "Implementation of a Call System with Power Line Communication", En: Application of Information and Communication Technologies International Conference, Oct. 2009, pp 1-4

- JENSEN, B. "Benchmarking and QoS of In-House Powerline Equipment for AV Streaming Applications", En: IEEE Power Line Communications and Its Applications International Symposium, 2006, pp 160-165

- KATAR, S. "Allocation Requirements for Supporting Latency Bound Traffic in HomePlug AV Networks", En: IEEE Global Telecommunications Conference, Dec. 2006, pp 1-6

- LAMASTRA, G VIALE, L. Tecnologías innovadoras para la detección y la comparación de los ataques informáticos, Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A... 2006, Issue 1, p6-19. 14p.

- J. A. GUERRERO Y A. BARBA. Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN, IEEE LATIN AMERICA TRANSACTIONS, VOL. 6, NO. 2, JUNE 2008

- GUZMÁN QUINTERO Y, Gestión de redes y servicios NGN/4G, Revista Técnica de la Empresa de Telecomunicaciones de Cuba, S.A... 2008.

- P.JAYASHREEL, K.S.EASWARAKUMAR 2, D.RADHAKRISHNAN, N.LAKSHMANAN 4, P.DINAKARAN. A Payload driven Security model for flooding attacks in Active networks, IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

- ALTOLINI, D. "Preamble-based Channel Estimation in HomePlug AV Systems", En: IEEE Power Line Communications and Its Applications International Symposium, pp 176-181, Mar 2012

- MYRTO ARAPINIS, LORETTA MANCINI, EIKE RITTER, MARK RYAN, New Privacy Issues in Mobile Telephony: Fix and Verification. University of Birmingham School of Computer Science Birmingham, UK, Technische Universität Berlin and Deutsche Telekom Laboratories Berlin.

- IEEE Standards Association. "iEEE Standards interpretation for iEEE Std C57.12.90™-2006 IEEE Standard Test Code for Liquid-immersed Distribution, Power, and Regulating Transformers", September, 2009. http://standards.ieee.org/findstds/interps/C57.12.90-2006.html (acceso: Marzo 23, 2009).