Ingeniaritza Goi Eskola Teknikoa
Escuela Técnica Superior de Ingeniería
Bilbao

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

UNIVERSIDAD DEL PAÍS VASCO
EUSKAL HERRIKO UNIBERTSITATEA

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA
BILBAO
BILBOKO INGENIARITZA GOI ESKOLA TEKNIKOA

TRABAJO FIN DE MÁSTER

DE

DEFINICIÓN Y ANÁLISIS DE UNA SOLUCIÓN DE SEGURIDAD EN ENTORNOS D2D OPORTUNISTAS MULTIOPERADOR

Autor: *Chaves, Hernández, Maitane*
Director: *Higuero, Aperribay, Mariví*
Titulación: *Máster Universitario en Ingeniería de Telecomunicación*

Fecha *Junio, 2016*

Tabla de contenido

1. Resumen

Este estudio tiene como objetivo definir y analizar una solución de seguridad en entornos D2D oportunistas multioperador. En primer lugar, se analizan los aspectos de la topología de red a securizar y se define la solución de seguridad que se ajusta a esa topología. A continuación, se identifican los parámetros más significativos para medir el rendimiento de dicha solución y se define un plan de pruebas y un escenario tanto en entorno simulado como en entorno real. Posteriormente se realizan las medidas en ambos entornos, y por último se analizan los resultados obtenidos para determinar la eficiencia la solución de seguridad.

Ikerketa honen helburua D2D oportunista multioperadore inguruneentzako segurtasun irtenbide bat zehaztu eta aztertzea da. Hasteko, sarearen topologiaren alderdiak aztertuta, segurtasun irtenbidea zehazten da, topologia horrekin bat datorrena. Jarraian, errendimendua neurtzeko parametro adierazgarrienak identifikatzeaz gain, neurketak egiteko proba-lana eta egoera definituko dira, ingurune itxuratuetan zein errealetan. Ondoren, ingurune bietan neurketak gauzatzen dira, eta azkenik lortutako ondorioak aztertzen dira, eta azkenik lortutako ondorioak aztertzen dira, proposatutako irtenbidearen errendimendua zehazteko.

This study has its aim in defining and analyzing a security solution in D2D opportunistic environment. Firstly, the main aspects of the topology that will be secured will be analyzed and the security solution that fits that topology will be defined. After this, the most significant parameters to measure the performance of the solution will be identified and a test plan and scenario will be defined. Then measurements will be taken in both environment, and finally, the obtained results will be analyzed to determine the efficiency of the security solution.

2. Lista de tablas

3. Lista de ilustraciones

4. Lista de acrónimos

ACRÓNIMO	SIGNIFICADO
D2D	Device to Device – Dispositivo a Dispositivo
IP	Internet Protocol
MCN	Multi-Hop Cellular Netwoks
3GPP	3rd Generation Partnership Project
ProSe	Servicios de Proximidad
LTE	Long Term Evolution
MOTO	Mobile Opportunistic Traffic Offloading
QoS	Quality of Service
Oppnet	Red oportunista
MANET	Mobile ad hoc networks
AODV	Protocolo de descubrimiento de ruta bajo demanda
NS-3	Network Simulator-3
UE	Dispositivo de Usuario
eNB	eNodo B

Tabla 1: Tabla de acrónimos.

5. Introducción

Con el uso generalizado de los Smartphones el tráfico de datos móviles está creciendo exponencialmente. Este hecho plantea un reto importante en términos de capacidad para los operadores móviles [1], cuyas infraestructuras no son capaces de soportar todo el tráfico adicional generado por los usuarios de este tipo de dispositivos IP (Internet Protocol).

De esta situación surgen una serie de enfoques para dar solución a este problema de capacidad. Un enfoque posible es mediante el incremento de la granularidad de las antenas desplegadas, es decir, mediante el despliegue de un mayor número de antenas con menor cobertura, conocidas como Small Cells. Sin embargo, la necesidad de infraestructura adicional tiene costes significativos tanto en el despliegue como en las fases de planificación y gestión, requiriendo su escalado una planificación minuciosa. Por lo tanto, esta solución de forma aislada (desplegar más infraestructura) no es adecuada para satisfacer la creciente demanda de capacidad de datos a la que se enfrentan las redes actuales y por consiguiente a la que se enfrentarán las futuras en mayor medida. Otras alternativas emergentes que actualmente se consideran como parte de la evolución 5G (quinta generación) de la red incluyen la migración del tráfico de datos móviles de la infraestructura del operador a los dispositivos de los usuarios (offloading) [2], aprovechando las capacidades de conexión de los actuales Smartphones para transmitir los datos mediante comunicaciones dispositivo a dispositivo (Device-To-Device - D2D) [3], y la integración de las comunicaciones celulares, WiFi y ad-hoc o comunicaciones D2D, constituyendo las denominadas redes celulares multisalto (Multi-Hop Cellular Netwoks - MCN) [4] [5].

El organismo de estandarización 3GPP (3rd Generation Partnership Project) está trabajando paralelamente a estas aproximaciones en las comunicaciones D2D oportunistas. De hecho, el soporte de los Servicios de Proximidad (ProSe) y la estandarización D2D se ha convertido en una de las piezas claves de la versión 13 del estándar LTE (Long Term Evolution) y, por tanto, de las futuras redes celulares (es decir, 4G y 5G).

En línea con esta última aproximación, en el proyecto europeo MOTO (Mobile Opportunistic Traffic Offloading) [6] se propone una arquitectura para gestionar de manera eficiente el offloading de tráfico en entornos multioperador. MOTO explota de forma sinérgica un conjunto de esquemas de offloading, incluyendo la descarga de LTE a otras infraestructuras inalámbricas (tales como WiFi), así como el uso de comunicaciones ad-hoc multisalto entre dispositivos de usuarios. Esta arquitectura, enfocada a resolver las necesidades de los entornos D2D oportunistas donde hay muchos operadores LTE y WiFi, ofrece, además de la reducción de la carga en las infraestructuras de los operadores, la reducción de los retardos en las comunicaciones al posibilitar la transmisión de contenido entre usuarios en base a su proximidad.

Sin embargo, este tipo de esquemas de comunicaciones plantean importantes retos de seguridad, puesto que son susceptibles a numerosos ataques, que pueden poner en peligro no

sólo la seguridad de las comunicaciones, sino también la privacidad de los usuarios y la integridad de la información transmitida. Es por ello que es necesario encontrar soluciones que sean capaces de garantizar la seguridad extremo a extremo y la privacidad de los usuarios, sin que su posición o identidad sea desvelada a usuarios malintencionados.

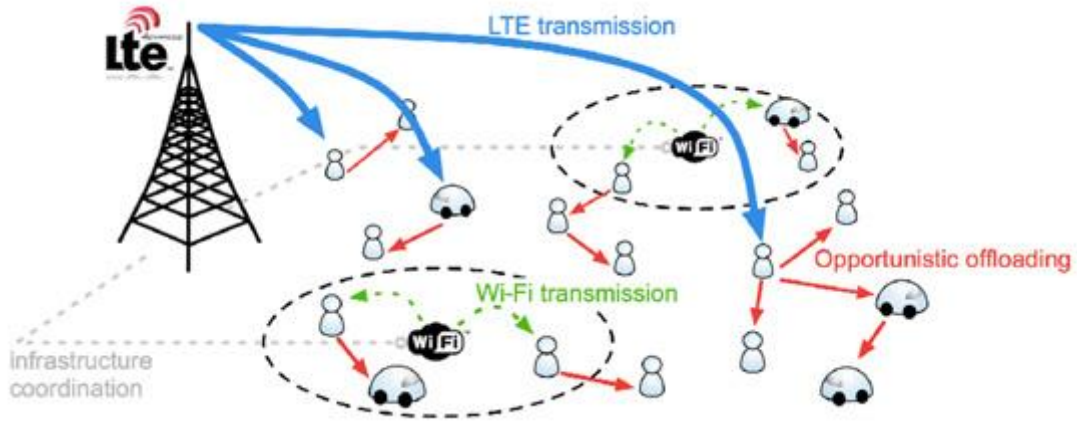


Ilustración 1: posibilidades de offloading en MOTO

Este TFM (Trabajo Fin de Máster) desarrollado en la empresa *Asociación de Empresas Tecnológicas Innovalia* perteneciente al *Grupo Innovalia* forma parte del proyecto MOTO financiado por la Comisión Europea dentro del *7th Framework Programme* (FP7) y presenta una propuesta de seguridad en redes de comunicaciones móviles oportunistas (D2D offloading) multioperador. El objetivo del proyecto MOTO es proporcionar una solución eficiente y segura con el fin de descargar la infraestructura de los operadores y hacer posibles las comunicaciones en entornos congestionados y de alta concentración de tráfico de datos.

En este contexto, este TFM propone una solución de seguridad cuyo objetivo es proteger las comunicaciones, el contenido intercambiado y la identidad de los usuarios del sistema de la solución propuesta en el proyecto MOTO. Además analiza el rendimiento de esta solución de seguridad en diferentes escenarios y con diferentes concentraciones de usuarios y tráfico.

6. Objetivos

Los principales objetivos de este proyecto son definir y analizar una solución de seguridad para realizar de manera segura y eficiente comunicaciones D2D oportunistas en entornos multioperador con altas concentraciones de tráfico de datos móviles.

Para poder completar con éxito estos objetivos es necesario definir una serie de objetivos parciales que son necesarios llevar a cabo.

En primer lugar hay que realizar un análisis de los posibles problemas de seguridad en este tipo de comunicaciones y de las diferentes tecnologías para solucionarlos.

A continuación al querer evaluar los diferentes comportamientos que puede presentar este tipo de red, es necesario definir diferentes escenarios para a través de los mismos examinar la forma en la que actúan las comunicaciones D2D. Estos escenarios a diseñar y desarrollar se refieren a todo aquello que pueda afectar al comportamiento de la red de dispositivos que se está analizando. Es decir, el número de dispositivos que se utilizan, los nodos del operador que dan cobertura, la cobertura que dan estos nodos, la cantidad de datos intercambiada, etc.

Con todos los factores se pueden establecer multitud de escenarios que ayudan a analizar el comportamiento de este tipo de comunicaciones, pero para que se pueda evaluar la red y la solución de seguridad es necesario, además, la definición de los parámetros que se van a medir.

De esta forma se permite medir si la solución de seguridad es eficiente y no sobrecarga las comunicaciones de forma excesiva.

En último lugar se lleva a cabo una serie de pruebas, con un prototipo que implemente la solución de seguridad, en una maqueta con el fin de poder evaluar la solución en un entorno real además de en un entorno simulado.

7. Beneficios

En este apartado se van a analizar los beneficios que supone realizar este TFM que busca definir y analizar el rendimiento de una solución de seguridad para un entorno de comunicaciones D2D oportunistas multioperador.

Los beneficios principales que suponen realizar este TFM son securizar la topología de red propuesta en el proyecto MOTO y conocer el comportamiento de dicha solución de seguridad con diferentes concentraciones de usuarios y tráfico. Asimismo, permite comprobar cómo se comporta la implementación de una maqueta en un entorno real.

7.1. Beneficios tecnológicos

El principal beneficio tecnológico es ofrecer una solución de seguridad eficiente para poder establecer comunicaciones D2D oportunistas en entornos congestionados de forma segura, en los cuales con las redes actuales es imposible tener conexión a Internet. Definir una solución completa para ofrecer seguridad en este tipo de conexiones (D2D oportunistas) es de vital importancia, ya que éstas presentan una serie de amenazas que ponen en riesgo la confidencialidad de los datos de usuarios.

Asimismo, con la realización de un análisis se podrá conocer si dicha solución de seguridad cumple con las expectativas iniciales que se tienen sobre ella en un entorno virtual, y además si cumple con los requerimientos de seguridad y QoS que son necesarios en este tipo de redes.

Por otro lado, una vez realizado este análisis se podrán comparar los resultados finales con los obtenidos en otros estudios sobre soluciones similares, con el fin de conocer que método para ofrecer seguridad es más adecuado para trabajar en este tipo de entornos.

Además, analizando los resultados obtenidos en las simulaciones se pueden solucionar algunas carencias de seguridad y eficiencia que se observen en las pruebas con el fin de optimizar la solución definida de cara a una posterior implementación real.

7.2. Beneficios económicos

Ofrecer una solución de seguridad para la topología de red propuesta en el proyecto MOTO supone el principal beneficio económico ya que este tipo de topologías son una solución mediante las cuales, con una pequeña inversión de dinero, las operadoras pueden descargar sus redes de acceso haciendo uso de las capacidades de conexión de los dispositivos de usuario.

Por otro lado, al analizar dicha solución mediante un entorno de simulación se puede conocer cómo se comporta con diferentes concentraciones de usuarios y de tráfico sin desplegar ninguna maqueta real, lo que conlleva una disminución de riesgo y coste. Además, al realizarse

un análisis mediante simulaciones previo, se puede conocer la viabilidad de implementar una maqueta real o bien desplegar una red de las características probadas.

Este estudio previo a la posible implementación de una solución de este tipo para subsanar los problemas de capacidad que tienen actualmente las operadoras permitiría ofrecer una alternativa segura y optimizada que garantice la conectividad en entornos congestionados debido a las altas concentraciones de tráfico de datos móviles existente. Y, por otro lado, a los usuarios de la plataforma les permitiría tener conectividad de forma segura mientras que sin este tipo de implementaciones sería imposible.

7.3.Beneficios sociales

El principal beneficio social es ofrecer una topología de red segura con la que garantizar unos niveles de seguridad adecuados para que los dispositivos de usuario puedan disponer de conectividad a Internet incluso en momentos de alta concentración de tráfico de usuario. Esto supondría un gran avance en las comunicaciones celulares con el fin de ofrecer conectividad en momentos puntuales de congestión, ya que actualmente para los usuarios de Internet es vital tener conectividad en todo momento con el fin de descargarse o compartir contenido multimedia mediante mensajería instantánea o en redes sociales.

Además, si los resultados obtenidos, una vez comparados con otros estudios de características similares, son los que mejor se adecuan a un entorno oportunista multioperador esto puede suponer que en un futuro se despliegue una red real implementando la solución de seguridad presentada en este TFM encargado de ofrecer seguridad en entornos de comunicaciones D2D oportunistas multioperador con alta densidad de tráfico de datos. Por lo tanto, el despliegue de dicha red supondría un gran nivel de seguridad y rendimiento en entornos oportunistas en los que no solo se gestionan las comunicaciones de los usuarios, sino que también se garantizarán la seguridad y la eficiencia para las aplicaciones encargadas de distribuir el contenido entre ellos.

8. Estado del arte

En este apartado se analiza el estado del arte de la seguridad en las redes oportunistas. Para ello, en primer lugar se hace una descripción de las redes oportunistas y después se analizan diferentes soluciones propuestas en este entorno para dar solución a las vulnerabilidades que se presentan en este tipo de redes.

8.1.Descripción de las redes oportunistas

En este apartado se realiza una revisión de las redes oportunistas ya que son la base de la red que se pretende securizar en este TFM. En primer lugar, se introduce esta tecnología, y a continuación se muestran las principales amenazas, ataques y vulnerabilidades de ellas. En último lugar se exponen las soluciones disponibles actualmente para solucionar estos retos de seguridad.

8.1.1. Introducción a las redes oportunistas

Las redes oportunistas u oppnets se consideran como una aproximación de las actuales tecnologías de offloading. Este concepto de offloading de datos móviles, o simplemente “data offloading”, se refiere al uso de tecnologías de red complementarias y técnicas innovadoras para redes móviles/celulares con el fin de aliviar la congestión y hacer un mejor uso de los recursos de red disponibles. El objetivo es mantener la QoS para los usuarios, mientras que se reduce el coste y el impacto de soportar servicios que consumen muchos recursos de las redes móviles. Se espera que la tecnología de data offloading se convierta en un sector clave en la industria en el futuro próximo ya que el consumo de datos en las redes móviles se incrementa a gran velocidad.

La tecnología de “traffic offloading” ha estado atrayendo la atención de las operadoras de red en los últimos años debido a los esfuerzos realizados para mejorar los beneficios y reducir los costes mediante un manejo eficiente del incremento del tráfico móvil. Esta tecnología se usa como un medio para reducir los costes de operación y mejorar las experiencias de los usuarios. Por tanto, mediante la incorporación de estas tecnologías permite a las operadoras móviles reducir el tráfico que pasa por las redes móviles a través de la tecnología de offloading y los usuarios finales pueden obtener beneficios de la reducción del RTT para lograr una mejor experiencia de usuario.

Hasta ahora las tecnologías de offloading preferidas han sido WiFi y las femtoceldas [7]. Sin embargo, las redes oportunistas (oppnets) recientemente están surgiendo como una aproximación atractiva de offloading porque hay un coste reducido o nulo asociado a él ya que se hace uso de las capacidades de conectividad de los Smartphones. En los años recientes las redes oportunistas están ganando popularidad en la industria y la investigación como una evolución natural de las redes MANET (mobile ad hoc networks). En las redes oportunistas los

nodos entran en contacto con otros de forma oportunista y se comunican inalámbricamente. El objetivo de las oppnets es aprovechar los recursos y las capacidades que tienen todos los elementos de la red (incluidos los terminales de usuario).

8.1.2. Funcionamiento de las redes oportunistas (oppnets)

En las redes oportunistas se crea un nodo denominado "seed node" que es la raíz de la red entera. Estos nodos pueden ser dispositivos Bluetooth, portátiles, teléfonos móviles o cualquier otro dispositivo.

Cuando se crea un nodo "seed", éste cuando detecta otros nodos les pide unirse a su red, es decir les solicita ser nodos colaboradores "helpers", para formar una más grande. Entonces, el nodo puede aceptar y unirse a la red o simplemente ignorarlo. Una vez los "helpers" están totalmente unidos, se pueden añadir nuevos nodos de tal forma que se consigue una red amplia y completa.

El principio de las oppnet es simple: cuanto mayor es la red, mayor es la efectividad de la misma. En las oppnet no existe una ruta completa; este tipo de redes se basan principalmente en las comunicaciones multisalto, lo que significa que los datos se propagan a través de múltiples saltos hasta llegar al destino. La propagación en las oppnet se hace a través de los nodos que colaboran en la red.

8.1.3. Principales amenazas en las redes oportunistas

Cada red oportunista desplegada comparte un conjunto de características comunes y componentes que se pueden describir como "activos". A continuación se evalúan los posibles activos de la red asociándolos con las vulnerabilidades en la Tabla 2, ataques específicos a esas vulnerabilidades y su clasificación dentro de las amenazas [8].

Activos	Vulnerabilidades
Componentes de almacenamiento: elementos que mantienen los algoritmos para la parte radio que se cargan en el arranque o bajo petición.	La información radio y los algoritmos pueden ser leídos o alterados en el almacenamiento del nodo/radio. La vulnerabilidad reside en los mecanismos de almacenamiento utilizados para los datos en el nodo radio.
Información local: información almacenada localmente en el nodo radio. Ayuda al enrutamiento y puede contener información como la ubicación del nodo, la disponibilidad de energía, la velocidad y la dirección de nodo, los perfiles de radio, perfiles de usuario, etc. Esto también incluye las tablas	La información de los protocolos de enrutamiento necesarios para los cálculos de rutado puede revelar información del usuario y la ubicación. Las tablas pueden ser maliciosamente alteradas y las alteraciones a continuación, se pueden propagar cuando se intercambia dicha información de rutado.

de encaminamiento almacenadas en un nodo.	Esta información puede ser leída o modificada.
Información sobre el aire: información OTA (Over the Air) específica transmitida: • **Mensajes de datos**: mensajes que contienen datos que necesitan ser rutados y entregados que contienen la información de rutado en la cabecera del mensaje. • **Mensaje de rutado**: descubrimiento de ruta, mensajes de actualizaciones e informes que son críticos para un mantenimiento satisfactorio de las capacidades de conectividad y rutado.	Los mensajes requieren nodos intermediarios para ayudar a propagar la información a los receptores legítimos de los mismos. Los mensajes pueden ser interceptados por nodos y reenviados, normalmente con modificaciones en la información de rutado y que son susceptibles a lectura no autorizada y modificaciones malintencionadas. Los errores debidos a fallos en el rutado pueden ser ejecutados de forma inadecuada acabando con la no entrega del mensaje. La petición de ruta puede generar una tormenta de difusión donde se requiere que los nodos receptores reenvíen los paquetes mientras se encuentra una ruta o se ejecuta un mecanismo de fin de tiempo de vida de los paquetes. El enrutamiento inadecuado puede ser destructivo.

Tabla 2: activos y vulnerabilidades en una red móvil ad hoc.

8.1.3.1. Clasificación de los ataques en redes oportunistas

Los ataques a las redes aparecen de formas muy diversas y se pueden clasificar en grupos de una forma diferente: por su tipo, por su fuente, por el mecanismo con el que atacan o por la capa a la que ocurren. A continuación se muestra los diferentes ataques clasificados en los grupos anteriormente citados:

- **Tipo de ataque**: de acuerdo al criterio de si el atacante interrumpe la operación de un protocolo de rutado o no, los ataques en las redes móviles ad hoc se pueden dividir en dos clases [9]: ataques pasivos y ataques activos.
  - En un ataque pasivo, el atacante no interrumpe la operación de un protocolo de rutado sino que intenta descubrir información valiosa escuchando (spoofing) el tráfico de rutado. Por esto, se puede violar el requerimiento de confidencialidad si un adversario es también capaz de interpretar los datos obtenidos mediante spoofing. Una forma de sobreponerse a esos problemas es usar **mecanismos de cifrado potentes** para ocultar los datos que van a ser transmitidos, de tal forma que sea imposible a los que escuchan obtener información útil de los datos obtenidos.

  - En un ataque activo, sin embargo las acciones que se llevan a cabo por adversarios incluyen la modificación y borrado de datos intercambiados para atacar los paquetes destinados a otros nodos o para analizarlos por el atacante o simplemente para desactivar la red. Los ataques pasivos se pueden clasificar en dos categorías, ataques externos o internos.
- **Fuente del ataque**: en relación a de donde viene el ataque se pueden encontrar dos tipos de ataques:
  - El primero viene de un atacante externo que no es parte de la red de forma legítima. Inyectando información errónea, replicando información antigua o distorsionando la información de rutado intercambiada un atacante puede particionar de forma satisfactoria la red o introducir una sobrecarga de tráfico causando retransmisiones y rutado ineficiente. Estos ataques se pueden prevenir usando mecanismos de seguridad estándares como técnicas de cifrado o firewalls [10].
  - El segundo y más peligroso viene de un nodo legítimo y malicioso (atacante interno), que puede usar de forma incorrecta la información de rutado de otros nodos o actuar sobre los datos para inducir a fallos del servicio.

- **Capa a la que ocurre dicho ataque** [11]:
  - Capa física: jamming, eavesdropping o intercepción de mensajes, etc.
  - Capa de enlace de datos: análisis y monitoreo de tráfico, interrupción del servicio, etc.
  - Capa de red:
    - Descubrimiento de ruta: inundación de mensajes, saturar la tabla de rutado, corromper la cache de rutado, etc.
    - Mantenimiento de ruta: enviar mensajes de control falsos.
    - Reenvío de datos: wormhole attack, blackhole attack, greyhole attack.
    - Otros ataque complejos: impedir que los nodos se queden en estado “idle” o revelación de la localización.
  - Capa de transporte: secuestro de la sesión (session hijacking). En este tipo de ataque un adversario obtiene el control de la sesión entre dos nodos. Como en la mayoría de los casos de procesos de autenticación esta solo se lleva a cabo al inicio, una vez está establecida la sesión entre los dos nodos, el nodo adversario puede hacerse pasar por uno de los dos nodos de la sesión y secuestrarla.
  - Capa de aplicación: ataque con scripts, virus, repudiación, etc.

Ataques a las redes oportunistas

En este apartado se exponen y se da una breve descripción de los principales ataques a las redes oportunistas que se tienen en cuenta para este proyecto. Como se ha explicado anteriormente en las redes oportunistas los nodos “seed” cuando se encuentran con otros nodos les solicitan unirse a la red y de esta forma se crea la topología de red. Sin embargo, los nodos no conocen la topología completa de la red y tiene que descubrir la ruta óptima a través

de la cual pueden alcanzar al destino. Debido a que escoger una ruta sin nodos malintencionados es de vital importancia en este tipo de entorno, a continuación se explican los principales ataques contra este proceso.

Por otro lado, con el fin de comprender el impacto de estos ataques, los cuales están relacionados con la seguridad del descubrimiento de ruta y son trasladable al posterior envío de la información, es esencial explicar primero como funciona el descubrimiento de ruta en una situación ideal.

AODV [12] es un protocolo de descubrimiento de ruta bajo demanda e iniciado por la fuente en una red móvil ad hoc. De acuerdo al protocolo original AODV cuando un nodo fuente necesita enviar paquetes a un nodo destino del que no tiene información de rutado disponible, este distribuye un paquete RREQ (Routing Request) a sus nodos vecinos. Los nodos vecinos activos actualizan sus tablas de rutado (RT) con una entrada para el nodo fuente y comprueban si es el nodo destino o tiene una ruta suficientemente fresca al nodo destino. Si no la tiene los nodos intermedios que reciben el paquete RREQ lo distribuyen a sus vecinos hasta conseguir una ruta con el nodo destino [9]. De esta forma, el paquete RREQ se distribuye por la red (Ilustración 2a) y cuando llega al destino o a un nodo intermedio que puede proporcionar una ruta suficientemente fresca al destino se genera desde ese nodo un paquete RREP (Route Response). El paquete RREP se propaga a través de la ruta en sentido inverso hasta llegar al nodo fuente [13] como se muestra en la Ilustración 2b. En la siguiente imagen se muestran los dos procesos explicados anteriormente. El nodo S envía inunda la red con el paquete de petición (RREQ) y cuando el nodo D recibe el paquete responde al nodo S con el paquete de respuesta (RREQ) por la ruta por la que ha recibido el paquete de petición en primer lugar.

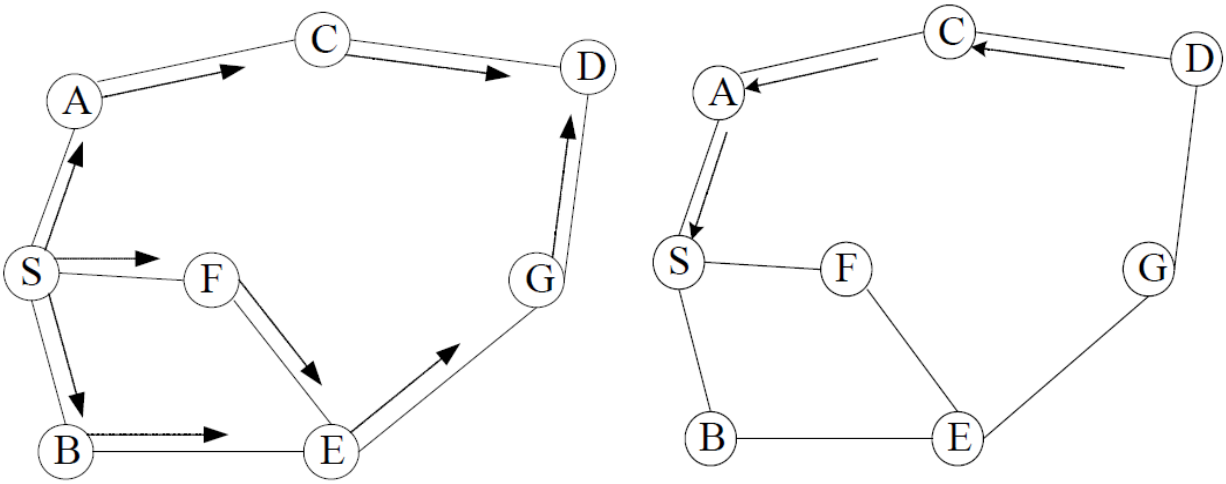


Ilustración 2: inundación de la red de RREQ (a) y propagación del mensaje RREP (b)

Ataque Black Hole

Un ataque black hole se define como una situación en la que un nodo malicioso utiliza el protocolo de rutado para difundir que él mismo es el camino más corto hasta el nodo destino. Un ejemplo de este ataque se ve en la Ilustración 3. El nodo 1 es el nodo fuente, el nodo 4 el

nodo destino y el nodo 3 es el nodo malicioso. Usando el protocolo de rutado el nodo malicioso (nodo 3) pretende tener la ruta al nodo destino (nodo 4) cuando recibe los paquetes RREQ y envía la respuesta RREP al nodo fuente (nodo 1). El destinatario real (nodo 4) también dará una respuesta. Entonces, si la respuesta desde el nodo destinatario llega a la fuente antes todo funciona bien pero se puede dar el caso en el que el nodo malicioso (nodo3) esté más cerca y por lo tanto la respuesta de éste llegará al nodo fuente antes. Es más, el nodo malicioso no tiene que consultar su RT cuando envía un mensaje falso, por lo tanto su respuesta es más probable que llegue antes al nodo fuente aunque esté más lejano.

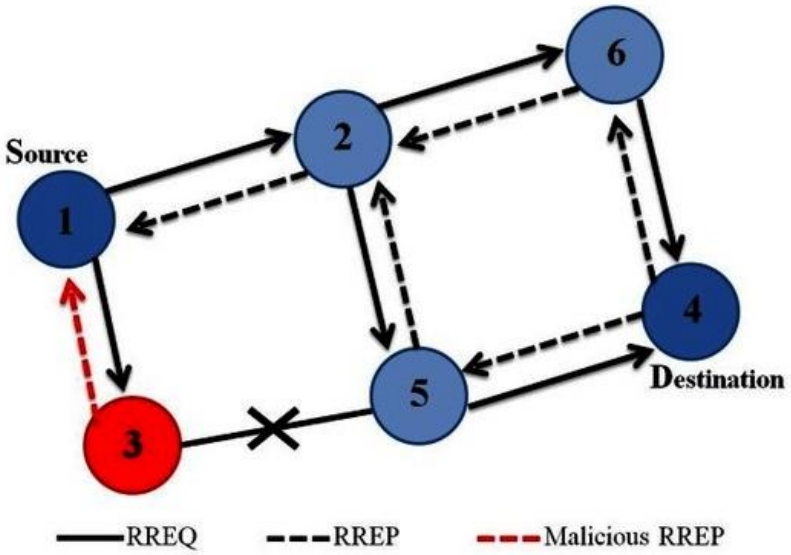


Ilustración 3: ataque black-hole en una MANET (RREQ: petición de ruta, RREP: respuesta de ruta)

Esto hace que el nodo fuente piense que el proceso de descubrimiento de ruta está completo, ignore todos los demás mensajes de respuesta y empiece a enviar paquetes de datos. En este momento se ha creado la ruta falsa.

Como resultado de la ruta falsa todos los paquetes a través del nodo 3 (el nodo malicioso) se leerán y modificarán o simplemente se descartarán. Las acciones no maliciosas como que se apague un nodo o que se salga del alcance de la red pueden comportarse como un ataque black hole.

Ataque Black Hole cooperativo

En un ataque black hole cooperativo un nodo o más de uno colaboran con otro u otros, con lo que este ataque es más difícil de identificar. No obstante cuando dos o más nodos black hole actúan de forma coordinada el primer nodo black hole (B1) y el otro nodo black hole (B2) tienen que estar conectados directamente, es decir el nodo 2 tiene que ser el siguiente salto del nodo 1 o viceversa como se muestra en la Ilustración 4.

De acuerdo a Hongmei [13], el nodo fuente S envía un “Further Request (FRq)” a B2 a través de diferentes rutas (S-3-4-B2) que no sean B1. El nodo S pregunta a B2 si tiene una ruta al nodo B1 y una ruta al nodo destino D. como B2 coopera con B1 su respuesta “Further Reply

(FRp)" será que sí a las dos cuestiones. A continuación, el nodo S comienza a enviar paquetes a través de la ruta S-B1-B2 pensando que es segura. Mientras que en realidad los paquetes están siendo tratados por B1 y la seguridad de la red está comprometida.

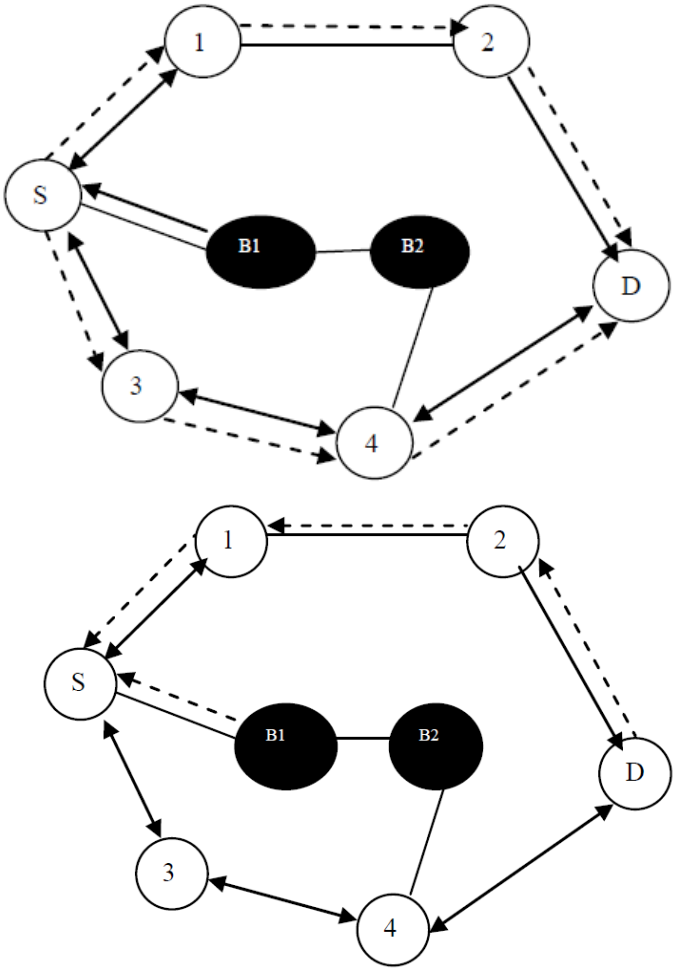


Ilustración 4: inundación de RREQ (a) y propagación de RREP (b) en un ataque black hole cooperativo

Ataque Grey Hole/Reenvío selectivo

Un atacante grey hole descarta un cierto porcentaje de todos los mensajes que debería enviar, mientras que el atacante black hole descarta todos (100%). En realidad, un ataque grey hole es una variante del ataque black hole, donde un adversario primero se comporta de forma honesta durante el procedimiento de descubrimiento de ruta, y después descarta alguno o todos los paquetes de datos que le envían para su posterior reenvío incluso cuando no hay congestión. Detectar un ataque grey hole es incluso más difícil de detectar un ataque black hole ya que los nodos pueden descartar paquetes parcialmente no solo debido a actos maliciosos sino que también debido a sobrecarga o congestión. Los nodos maliciosos más difícil de identificar son los nodos egoístas. Se conoce como un nodo egoísta a aquel que no está dispuesto a gastar su batería, ciclos de CPU o ancho de banda disponible para reenviar paquetes que no le interesen directamente, pero espera que otros reenvíen los paquetes en su favor.

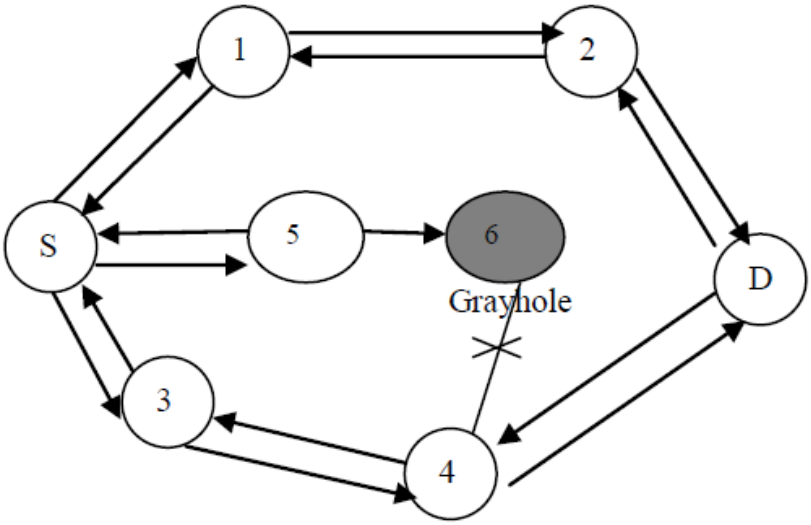


Ilustración 5: ataque grey hole en una MANET

Ataque Wormhole

En un ataque wormhole un nodo malicioso usa una ruta de fuera de la red para enviar mensajes a otro nodo malicioso en otro punto de la red.

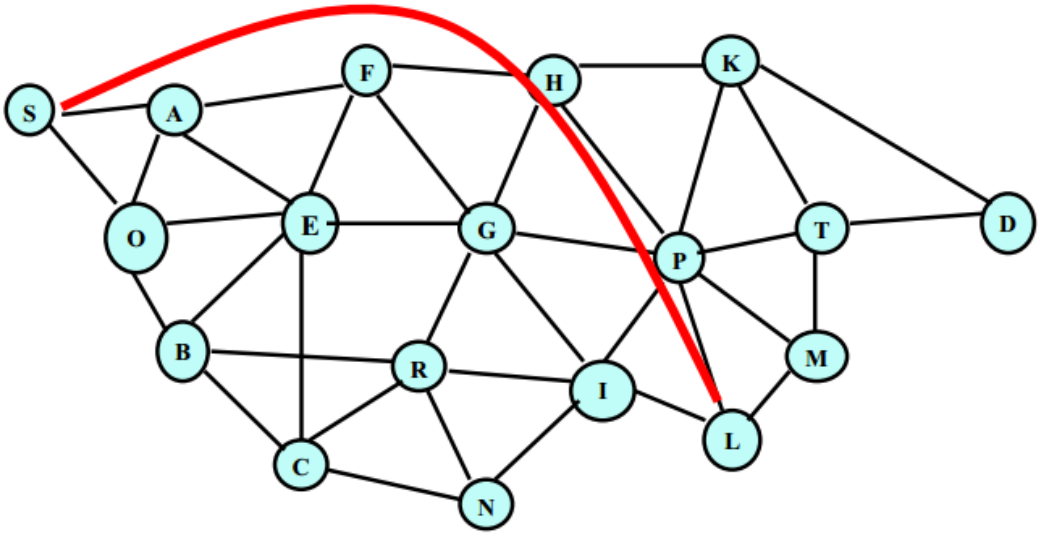


Ilustración 6: ataque Wormhole (fuente: [11])

Los ataques wormholes son difíciles de detectar porque la ruta utilizada para pasar la información no es parte de la red actual normalmente. Curiosamente, un wormhole no tiene que ser perjudicial porque normalmente toma un tiempo menor en llegar el paquete al destino. Pero este comportamiento puede dañar la operación ya que los wormholes falsean una ruta que es más corta en lugar de una incluida en la red; esto puede confundir a los mecanismos de rutado que dependen del conocimiento de la distancia entre los nodos.

Una vez se establece una ruta wormhole, el nodo adversario graba los datos que escucha de forma casual por la red wireless y los reenvía al otro nodo a través del enlace wormhole en el otro extremo de la red. Reenviando mensajes de red validos a lugares inadecuados los atacantes pueden hacer creer que son vecinos de nodos que están lejos y de esta forma forzar que todas las comunicaciones que afecten a esos nodos vayan a través de ellos.

Ataque Sinkhole

Llevando a cabo un ataque sinkhole un nodo malintencionado intenta atraer todos los datos a él mismo de los nodos vecinos. Esto le da acceso a todos los datos, por lo tanto este ataque puede ser la base para otros muchos ataques como eavesdropping o alteración de datos o modificación de información secreta. Los ataques sinkhole hacen uso de las lagunas en los algoritmos de rutado en redes ad hoc y se presentan a los nodos adyacentes como el compañero más adecuado en una ruta multisalto. De hecho, la ruta a través del nodo malicioso aparenta ser la mejor de las disponibles para que los nodos la utilicen para comunicarse.

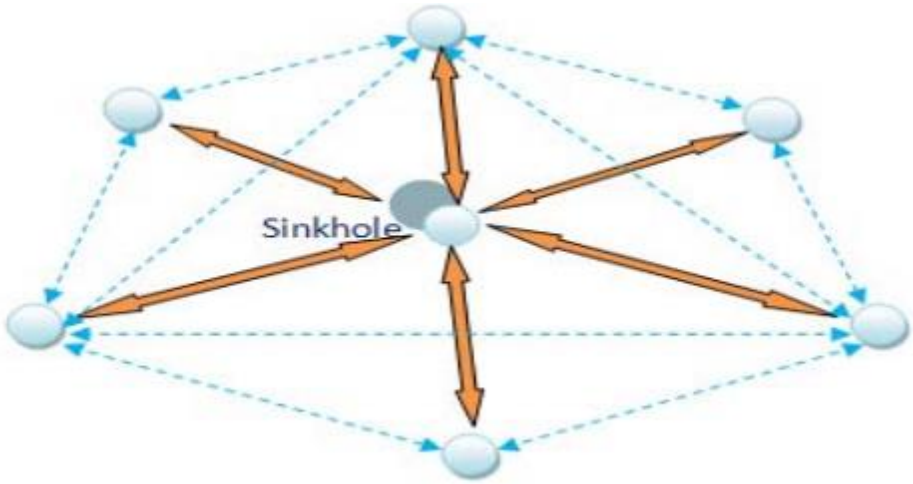


Ilustración 7: ataque sinkhole [14]

Ataques de rutado

Hay multitud de ataques sobre los protocolos de rutado que pretenden interrumpir la operación normal de la red [15]. Siguiendo con esto, a continuación se describen brevemente una serie de ataques a protocolos de rutado:

- **Saturación de la tabla de rutado**: en este tipo de ataque, un adversario intenta crear rutas a nodos no existentes para los nodos autorizados presentes en la red. El objetivo principal de un ataque como este es causar un desbordamiento de las tablas de rutado, lo que conlleva que va a impedir crear nuevas entradas correspondientes a rutas de los nodos autorizados. Los protocolos de rutado proactivo que actualizan la información de rutado periódicamente son más vulnerables a este ataque en comparación a los protocolos de rutado reactivo que crean rutas cuando lo desean los nodos fuente.

- **"Envenenamiento" de las tablas de rutado**: en este caso, los nodos malintencionados en la red mandan mensajes de actualización de ruta o modifican paquetes de modificación de ruta verdaderos enviados por otros nodos que hacen uso correcto de ellos. Este ataque puede desencadenar una situación de rutado no óptimo, congestión en partes de la red, o incluso hacer algunas partes de la red inaccesibles.
- **"Envenenamiento" de la cache de rutas**: En el caso de protocolos de rutado bajo demanda (como el protocolo AODV [12] anteriormente explicado), cada nodo mantiene una cache de rutas que mantiene la información referente a las rutas que se han convertido en conocidas para el nodo en el pasado reciente. Al igual que en el caso de las tablas de rutado un adversario puede también modificar la cache de rutas para conseguir objetivos similares.
- **Replicación de paquetes**: en este ataque, un nodo malicioso replica un paquete antiguo. Esto consume ancho de banda adicional y recursos de batería disponibles en los nodos y puede causar confusiones en los procesos de rutado.
- **Ataque tipo "rushing" (asaltar)**: los protocolos de rutado bajo demanda (o reactivos) que implementan supresión de duplicados durante el proceso de descubrimiento de ruta son vulnerables a este ataque [16]. En un protocolo bajo demanda, un nodo que necesita una ruta inunda la red con paquetes RREQ en un intento de encontrar una ruta al destino. Para limitar la sobrecarga de esta inundación, cada nodo normalmente reenvía únicamente un RREQ originado por cualquier descubrimiento de ruta. En concreto, en los protocolos de rutado bajo demanda solo reenvían el primero que llega para cada descubrimiento de ruta. En este tipo de ataque, el atacante hace uso de esta propiedad en la operación de descubrimiento de ruta.

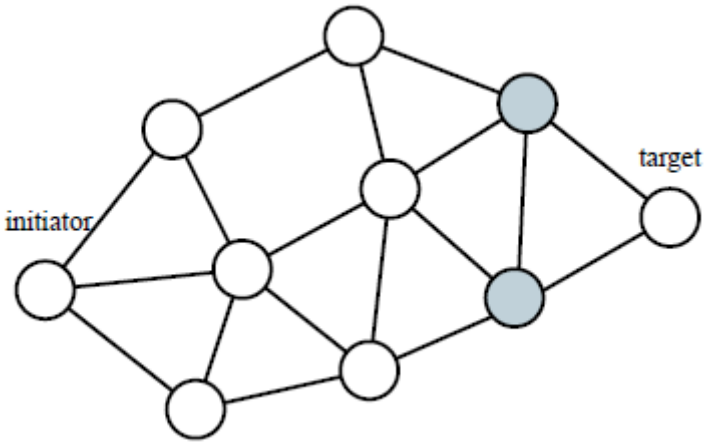


Ilustración 8: ejemplo de red mostrando el ataque tipo "rushing".

El nodo "initiator", es decir el nodo fuente, comienza el proceso de descubrimiento de ruta para el nodo "target", es decir el nodo destino. Si los paquetes RREQ del atacante para el descubrimiento de la ruta son los primeros que llegan a cada vecino del nodo destino (mostrados en gris en la Ilustración 8: ejemplo de red mostrando el ataque tipo "rushing".), cualquier ruta seleccionada por este descubrimiento de ruta incluirá un

salto a través del atacante. Esto es, cuando un vecino del nodo destino recibe la petición del atacante ("rushed request"), este reenvía dicha petición y por lo tanto no reenviará más peticiones posteriores de descubrimiento de ruta. Cuando la petición de nodos no atacantes llegan posteriormente a estos nodos, descartarán las peticiones legítimas. Como resultado, el nodo fuente no será capaz de descubrir ninguna ruta segura (es decir, rutas que no tengan como salto un atacante). Es extremadamente difícil detectar estos ataques en estas redes.

Byzantine attack

En este ataque, un nodo malicioso intermedio o un conjunto de nodos maliciosos intermedios trabajan conjuntamente y llevan a cabo ataques como creación de bucles en las rutas, rutar paquetes por caminos no óptimos y descartar paquetes de forma selectiva [17]. Estas acciones tienen como resultado una degradación o interrupción de los servicios de rutado. Los ataques de este tipo son muy difíciles de detectar ya que la red aparentemente está operando de forma correcta desde el punto de vista de los nodos.

8.1.4. Mecanismos de seguridad específicos para redes oportunistas

En un entorno sin conexión, los mecanismos para establecer asociaciones entre nodos que sean de confianza juegan un factor crítico. La colaboración de confianza entre las entidades crea oportunidades para la ejecución de tareas de computación distribuidas. Sin embargo, la creciente tendencia hacia la descentralización ha dado lugar a importantes retos debido a que las soluciones de seguridad tradicionales normalmente requieren autoridades de confianza centralizadas o repositorios de certificados, que no encajan bien con las redes oportunistas en las que tanto la conectividad como los requerimientos de centralización son muy "relajados". Los intercambios a través de redes oportunistas requieren un paradigma centralizado para establecer la confianza entre parejas para interacciones.

A continuación se muestran una serie de soluciones para los ataques "wormhole", "blackhole" y "greyhole" [18], ya que las soluciones para los ataques "blackhole" y "greyhole" son trasladables a los ataques "sinkhole" y "byzantine attacks" debido a las características similares que tienen, es decir, que en todos los casos los nodos hacen creer a los otros nodos que son la mejor ruta para llegar al destino cada uno con un objetivo diferente.

Solución al ataque wormhole

Los ataques wormhole están basados en un nodo que falsifica su localización. Por lo tanto, los protocolos de rutado que se basan en la localización tienen la capacidad de prevenir los ataques wormhole. La localización se puede hacer globalmente mediante beacons que se difunden con la localización [19].

Se propuso una solución para los ataques wormhole en la que todos los nodos se equipaban con antenas direccionales. Los nodos usan unos sectores específicos de sus antenas para comunicarse con las otras. Cada par de nodos examina la dirección de las señales recibidas por sus vecinos. Si la dirección de ambos encaja se establece la asociación entre los vecinos. Este método solo puede ser usado en redes donde se usan antenas direccionales. Otra solución disponible propone que el nodo estime la distancia a su vecino mediante la potencia de la señal recibida. El valor se envía a un controlador central que calcula la topología física basándose en un sensor individual de medición de distancia. El ataque wormhole se detecta si se produce en un terreno llano [20]. No se han tenido en cuenta los terrenos con desniveles o la movilidad [21].

Solución al ataque blackhole y greyhole

Una propuesta para detectar a los nodos blackhole y greyhole, es tener de vez en cuando chequeado al nodo fuente a través de todas las rutas disponibles para conocer si el destinatario recibe todos los paquetes intactos. Esto debe llevarse a cabo una vez algunos datos se hayan enviado. Para esquivar a un nodo blackhole que pueda interferir el tráfico, el emisor divulga un mensaje de petición de "comprobación" (Ilustración 9a) y la respuesta del destinatario seguirá el mismo camino que la petición (Ilustración 9b). Para lidiar con la posibilidad de que un nodo esté alterando la respuesta el cliente la compara con los datos que envía al destinatario. Si la respuesta difiere con lo que envía el emisor, esto indica que es un enlace inadecuado o que hay un nodo malicioso. Si difieren dos respuestas de clientes cualquiera, entonces es seguro un nodo malicioso [22].

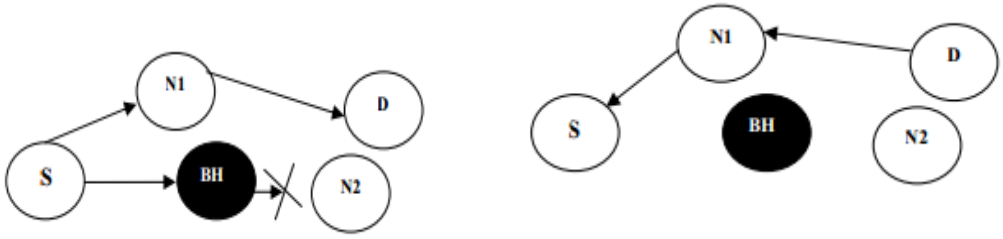


Ilustración 9: envío del mensaje de petición (a) y respuesta del destinatario (b)

8.2.Seguridad en redes oportunistas

En las redes oportunistas se han presentado a lo largo del tiempo diferentes propuestas de seguridad. En este apartado se evalúan diferentes protocolos que se usan en redes oportunistas con sus puntos fuertes y debilidades:

Protocolo	Aplicación	Puntos fuertes	Debilidades
Protocolo Shamir's three-pass [23]	Cifrado de mensajes sin intercambio de claves	Las contraseñas no se envían en claro sobre el canal de comunicaciones y que no necesita	• No tiene autenticación

		certificados o la sobrecarga de una infraestructura de clave pública.	• Vulnerable al ataque man-in-the-middle
Security-Aware Ad Hoc Routing Protocol (SAR) [24]	Redes wireless ad-hoc	SAR busca la ruta óptima con una garantía cuantificable de seguridad, pero puede que no sea la ruta más corta.	Prioriza la seguridad de una ruta sobre la efectividad o sobre el éxito de la comunicación.
Protocolo AODV [25]	Redes wireless ad-hoc	• Las rutas se establecen bajo demanda. • Los números de secuencia de destino se aplican para buscar la última ruta que se ha utilizado al destino. • El retardo de conexión es más bajo.	**Vulnerable a:** • Modificaciones de números de secuencia. • Modificación de número de saltos. • Tunelado. • Spoofing. • Errores de falsificación de rutas. • Ataques tipo rushing.
Secure efficient ad hoc distance vector (SEAD) routing protocol [26]	Redes wireless ad-hoc	• Minimiza los ataques de consumo de recursos. • Robusto contra múltiples ataques descoordinados.	No es capaz de sobreponerse a ataques donde el atacante usa el mismo número de secuencia los cuales se usan para mensajes de actualización recientes y envía una nueva actualización de ruta.
Destination-sequenced distance vector (DSDV) routing protocol [27]	Redes wireless ad-hoc	• Previene la formación de bucles.	• Consume muchos recursos de ancho de banda y batería como consecuencia de la actualización regular de las tablas de rutado. • No es apto para redes muy dinámicas (cambian muy rápidamente) porque cuando cambia la topología de la red, se necesita un nuevo número de secuencia antes de que la red vuelva a converger.
Authenticated routing for ad hoc networks routing protocol (ARAN) [28]	Redes wireless ad-hoc	Hace frente a todos los ataques identificados en la capa de red: participación no autorizada, señalización de rutas falsas, mensajes	**Vulnerable a:** • Ataque black hole. • Ataque wormhole.

		de fabricación de rutas, alteración de mensajes de rutado, securización de los caminos más cortos y ataques de reenvío.	• Ataque de denegación de servicio. • Ataques que descartan paquetes. • Ataques que modifican mensajes del protocolo.
TESLA broadcast authentication protocol [29]	Situaciones de broadcast	• Baja sobrecarga de computación en generación y verificación de información de autenticación. • Baja sobrecarga de comunicación. • Robusto a pérdida de paquetes. • Escala para un número alto de receptores.	• Buffering limitado para el emisor y receptor, por lo que hay que autenticarse para cada paquete. • El transmisor y el receptor tienen que estar sincronizado en tiempo.

Tabla 3: Análisis de las diferentes soluciones en redes oportunistas.

9. Análisis de alternativas

9.1. Confidencialidad de los datos

Para poder llevar a cabo el TFM en primer lugar hay que decidir cómo se realiza el cifrado para ofrecer confidencialidad de los datos. En este ámbito se evalúan el cifrado de enlace, el cifrado extremo a extremo y el uso de una combinación de ambos.

9.1.1. Cifrado de enlace

En este método de cifrado de capa 2 OSI cifra todo el mensaje incluidas las cabeceras de niveles superiores. Esto requiere que todos los nodos intermedio cuenten con capacidades de cifrado y de descifrado y además permite comprobar en cada nodo si ha habido errores de difusión. Este método de cifrado cuenta con las siguientes ventajas:

- El cifrado que se aplica es transparente para el usuario.
- Se necesita una clave para cada par de nodos, por lo tanto ante un problema de seguridad sólo se comprometen las claves relacionadas con sus adyacentes y no toda la red.
- Proporciona autenticación de los nodos que retransmiten el mensaje.

Y como desventajas:

- El mensaje queda expuesto en los nodos intermedios.
- El cifrado se aplica en el nodo emisor y en todos los intermedios requiriendo un mayor tiempo de procesamiento.

9.1.2. Cifrado extremo a extremo

En este esquema de cifrado de capa 7 OSI solamente se cifran los datos en el origen y viajan cifrados hasta el destino de esta forma. De esta forma no es necesario que los nodos intermedio cuenten con capacidades de cifrado y descifrado. Este método de cifrado cuenta con las siguientes ventajas:

- El mensaje solo queda expuesto en el emisor y en el receptor.
- El cifrado se aplica en el nodo emisor por lo que el tiempo de procesamiento es menor.
- Es más flexible en cuanto a que los nodos intermedios no necesitan capacidades de cifrado y descifrado.

Y como desventaja:

- No proporciona control de errores salto a salto.

9.1.3. Selección de la solución

En este apartado se han evaluado las características de los dos métodos de cifrado anteriores y la posibilidad de ofrecer seguridad haciendo uso de los dos métodos de cifrado. Se ha llegado a la conclusión que la mejor opción es ofrecer seguridad multicapa, es decir, hacer uso de cifrado extremo a extremo entre el emisor y el receptor final de los datos ya que los datos pueden ser sensible y que solo los deban conocer los extremos y sobre eso ofrecer cifrado de enlace con el fin de poder autenticar a los nodos que retransmiten el mensaje y poder controlar los errores de los datos cifrados.

9.2. Método para probar la solución de seguridad

En segundo lugar hay que decidir qué método es más adecuado para probar la solución de seguridad. En este ámbito existen tres opciones. Estas opciones son análisis mediante simulaciones, análisis mediante maqueta o análisis mediante ambas.

9.2.1. Análisis mediante simulaciones

La primera alternativa es la simulación. En este caso se utilizaría una herramienta de simulación como puede ser OMNeT++ o NS-3 para crear el escenario, modelar el tráfico en las redes de telecomunicaciones y realizar una evaluación del rendimiento. Por lo tanto esta herramienta permitiría simular la solución de seguridad propuesta. Como ventajas tiene:

- Herramientas de simulación sin coste.
- Capacidad de realizar simulaciones de larga duración (horas, días…) en un intervalo de tiempo pequeño (segundos, minutos…).
- Facilidad para establecer los parámetros a diferentes valores.
- Facilidad para obtener un conjunto de resultados en los que un parámetro se encuentra dentro de un rango de valores, realizando para ello las simulaciones de manera paralela.
- Necesidad de un único equipo real.
- Facilidad para configurar el escenario deseado.

Como desventajas tiene las que se detallan a continuación:

- No es posible tener en cuenta todas las posibles variaciones que pueden tener lugar en la realidad.
- Necesidad de desarrollar módulos adicionales para las implementaciones de las diferentes aplicaciones.
- Necesidad de un equipo con una potencia media-alta para llevar a cabo las simulaciones de manera fluida.
- A pesar de asemejarse a la realidad, no aporta una medida exacta de la realidad.

9.2.2. Análisis mediante maqueta

En este caso los resultados se obtendrían realizando las mediciones con dos equipos reales. Un terminal móvil para instalar la aplicación móvil y un servidor para instalar la plataforma MOTO. Como ventajas tiene las que se detallan a continuación:

- Gran diversidad de herramientas mediante las cuales es posible realizar las mediciones y analizar los resultados.
- Medidas de la realidad muy cercanas, aunque no exactas.

Como desventajas tiene las que se detallan a continuación:

- Necesidad de dos equipos reales.
- Necesidad de equipamiento para interconectar ambos equipos.
- Mayor coste.

9.2.3. Análisis mediante ambas

En este caso se realizaría en primer lugar pruebas mediante simulación y posteriormente pruebas mediante maqueta real. Este método ofrece las ventajas de los dos métodos anteriores y además al realizar un análisis previo mediante simulación se reduce el coste del análisis mediante maqueta. Por lo tanto, este método aportaría unas medidas muy cercanas a la realidad y con un coste más cercano al de las simulaciones.

9.2.4. Criterios de selección del método de pruebas

Para la elección del simulador de red se tendrán en cuenta los siguientes criterios:

- **Coste**: Coste necesario para llevar a cabo el proyecto.
- **Proximidad de los resultados a la realidad**: Cuánto de próximos a la realidad son los resultados obtenidos.
- **Tiempo**: Tiempo que supone realizar las mediciones.
- **Facilidad de puesta en marcha**: Facilidad de puesta en marcha del escenario.
- **Facilidad de despliegue de escenarios**: Facilidad de despliegue del escenario que implemente la solución de seguridad.

9.2.5. Selección del método de pruebas

En último lugar se pasará a seleccionar el método para realizar las pruebas entre las diferentes opciones propuestas. Estos métodos a comparar son análisis mediante simulaciones, análisis mediante maqueta y análisis mediante ambas. Se evaluarán los criterios del 1 al 5.

Criterio	Ponderación	Análisis mediante simulaciones	Análisis mediante maqueta	**Análisis mediante ambas**
Coste	35%	4	2,5	3,5
Proximidad de los resultados a la realidad	35%	2,5	3,5	4,5
Tiempo	10%	3,5	3	2,5
Facilidad de puesta en marcha	10%	2	4	3,5
Facilidad de despliegue de escenarios	10%	3,5	4	4
RESULTADO	100%	3,175	3,2	**3,8**

Tabla 4: Comparación del método de pruebas.

Los tres métodos tienen características similares, pero el parámetro que marca la diferencia es la proximidad de los resultados a la realidad. Por lo tanto, el método para realizar las pruebas es primero mediante simulaciones y después mediante maqueta real.

9.3.Simulador de red

En último lugar hay que decidir entre los diferentes simuladores de red disponibles para seleccionar el más adecuado para este trabajo.

De la herramienta de simulación de red se espera que sea una herramienta portable y flexible que nos permita simular la solución de seguridad que se propone en este TFM de la forma más fácil y económica posible. Las tres opciones que se plantean para el simulador de red son OMNeT++, Opnet y NS-3.

9.3.1. OMNeT++

OMNeT++ es un entorno de simulación de eventos discretos. Su área de aplicación principal es la simulación de redes de comunicación, pero debido a su arquitectura genérica y flexible, OMNeT++ se utiliza con éxito en otras áreas, como son la simulación de sistemas complejos, simulación de colas en redes y también en arquitecturas de hardware.

OMNeT++ proporciona una arquitectura de componentes, los cuales están programados en C++. OMNeT++ tiene un amplio soporte GUI (interfaz gráfica de usuario), y debido a su arquitectura modular, el núcleo de simulación puede ser fácilmente integrado en sus aplicaciones.

Este software está disponible tanto para Linux como para Windows.

9.3.2. NS-3

El simulador de red NS-3 es una plataforma abierta y extensible, que ha sido desarrollada para la creación de redes de investigación y educación. En resumen, ns-3 proporciona modelos de cómo trabajan las redes de paquetes de datos, y proporciona un motor de simulación.

Una de las razones de utilizar NS-3 es que está disponible para realizar estudios complejos o imposibles de realizar con los sistemas reales, para estudiar el comportamiento del sistema en un entorno altamente reproducible, y para aprender acerca de cómo funcionan las redes. El modelo disponible en ns-3 se centra en el modelado de la pila de protocolos TCP/IP, pero ns-3 no se limita solo a dichos sistemas, ya que se puede simular con él sistemas diferentes de los basados en Internet.

En este simulador existe un módulo DTN (Delay Tolerant Networks) de Aalto, base para construir una red oportunista, que está probada para la versión 3.16 de NS-3.

Como OMNeT++, este software está disponible tanto para Linux como para Windows.

9.3.3. OPNET

OPNET es un simulador de redes, que proporciona un entorno virtual que modela el comportamiento de una red completa. Este entorno de trabajo es de gran utilidad ya que permite diagnosticar problemas de una forma eficiente, validar cambios en la red antes de implementarlos y prever el comportamiento de la red ante futuros escenarios como crecimiento de tráfico, fallos de red, etc.

Al igual que los dos anteriores, este software está disponible tanto para Linux como para Windows.

9.3.4. Criterios de selección para el simulador de red

Para la elección del simulador de red se tendrán en cuenta los siguientes criterios:

- **Sencillez del lenguaje de programación**: se va a tener en cuenta si el lenguaje de programación de la herramienta es más sencillo, con el fin de minimizar la complejidad de la solución, siempre y cuando el lenguaje cubra nuestras necesidades de programación.
- **Aprovechamiento de módulos**: una de los criterios de mayor peso es que la herramienta proporcione módulos que puedan ser reutilizados para conseguir la solución.
- **Coste**: un aspecto importante es el coste que supone el uso de la herramienta. Uno de los aspectos importantes es maximizar los beneficios del proyecto y minimizar los costes, por lo tanto, es preferible una herramienta lo más económica posible.

- **Portabilidad**: un aspecto a tener en cuenta es que se puedan portar las redes para poder simular con otras plataformas.
- **Flexibilidad**: es importante que se pueda modificar los módulos ya definidos por la herramienta con el fin de adecuarlos a nuestras necesidades.
- **Sistema Operativo**: un aspecto a tener en cuenta es la compatibilidad de la herramienta con distintos sistemas operativos por si se requiere en un momento dado utilizar un sistema operativo diferente al seleccionado inicialmente.

9.3.5. Selección de la herramienta de simulación de red

En último lugar se pasará a seleccionar el simulador de red entre las diferentes herramientas propuestas. Estas herramientas a comparar son OMNET++, OPNET y NS-3. Se evaluarán los criterios del 1 al 5.

Criterio	Ponderación	OMNET++	OPNET	**NS-3**
Sencillez del lenguaje de programación	10%	4	3	4
Aprovechamiento de módulos	25%	2	3	5
Coste	20%	4	3	4
Portabilidad	20%	4	4	4
Flexibilidad	20%	4	4	4
Sistema operativo	5%	3	3	3
RESULTADO	100%	3,45	3,4	**4,2**

Tabla 5: Comparación de simuladores de red.

Los tres simuladores de red tienen características similares, pero el criterio que marca la diferencia es el aprovechamiento de módulos. Por lo tanto, el simulador de red a utilizar en este TFM será NS-3.

10. Análisis de riesgos

Los principales riesgos que supone la realización del TFM "Definición y análisis de una solución de seguridad en entornos D2D oportunistas multioperador" son los que se detallan en este apartado.

El primer riesgo, y quizás el que más impacto tendría en este TFM, es que un organismo de estandarización proponga una solución de seguridad que se tome como referencia y de esta forma los resultados de este TFM queden eclipsados por esta solución estándar. Este hecho supondría además, que la solución de seguridad aquí presentada no se tomaría como punto de partida para posibles trabajos futuros en esta misma línea de investigación. Este riesgo hay que tenerlo muy en cuenta ya que el organismo de estandarización 3GPP está trabajando en las comunicaciones de proximidad con el fin de incluirlas en próximas releases del estándar de LTE.

El segundo riesgo, también relacionado con los organismos de estandarización es que dichos organismos descarten las redes oportunistas como la evolución de las redes actuales y tomen otro camino para solucionar el problema de la congestión en las redes de datos. Este hecho supondría que la solución de seguridad no tendría utilidad para un futuro.

El tercer riesgo es que los resultados de las simulaciones no sean como se espera y de esta forma se tenga que rediseñar la solución de seguridad. Esto supondría un retraso en tiempo y por lo tanto un coste adicional para la finalización de este proyecto.

11. Descripción de la solución de seguridad

Para poder especificar la solución de seguridad, en primer lugar, es necesario conocer cómo es la arquitectura a securizar. Como se ha comentado anteriormente, el objetivo de MOTO es proporcionar una solución para descargar el tráfico de datos de las redes de operadores, en favor de las capacidades de conectividad de los dispositivos de usuario. Para ello, se considera la existencia de una plataforma en la nube responsable de coordinar la difusión de contenido (plataforma MOTO) entre los usuarios que lo han solicitado. Este esquema de funcionamiento sirve para liberar a los operadores de la difusión de contenido redundante. La plataforma MOTO puede integrarse dentro o fuera de la red del operador. Cualquier aplicación de distribución de contenidos puede usar la plataforma para difundir contenido entre los usuarios del servicio. Este contenido será enviado por MOTO a ciertos usuarios "semilla" ("seed") que, a continuación, retransmitirán este contenido a través de conexiones multisalto a otro usuarios, y estos a otros, hasta que la información llegue a los destinatarios finales (Ilustración 10).

De cara a poder proponer una solución de seguridad adecuada al contexto de difusión oportunista multioperador propuesto en MOTO, es necesario analizar las características principales de las comunicaciones de un entorno como el propuesto y que se incluyen a continuación:

1. la topología es dinámica
2. los nodos pueden desplazarse durante la distribución del contenido
3. los recursos son limitados (vida de la batería y capacidades de procesamiento)
4. los nodos pueden desconectarse en cualquier momento (perder la cobertura, desconectar las capacidades de conectividad, agotarse la batería, etc.)
5. los nodos pueden ser maliciosos o egoístas incluso una vez autenticados en la plataforma MOTO.

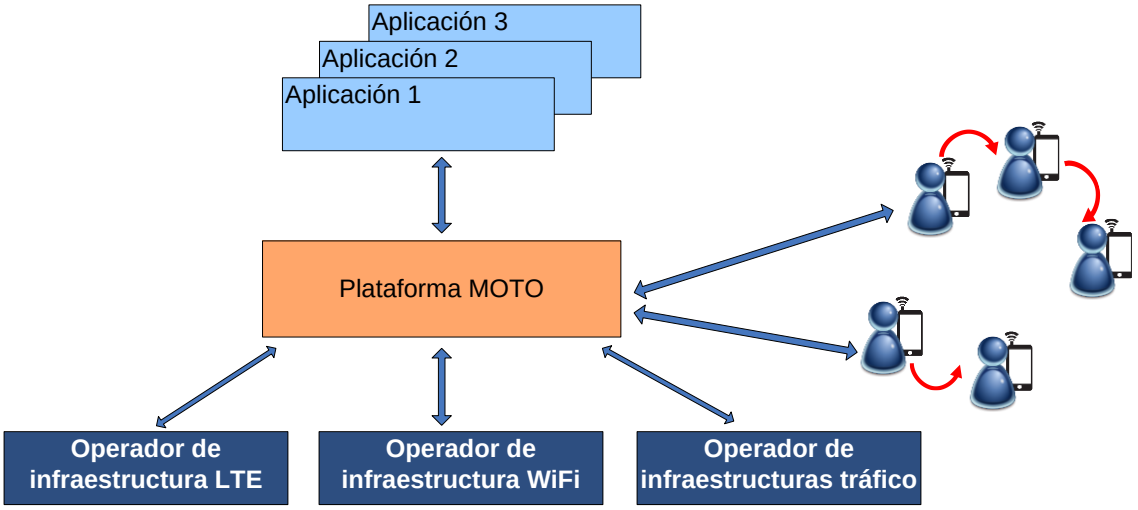


Ilustración 10: arquitectura MOTO

11.1. Retos de seguridad en MOTO

La naturaleza dinámica de las redes oportunistas plantea una serie de nuevos retos de seguridad y privacidad [30]. Por otra parte, el esquema de comunicación que se establece en las redes oportunistas, como es el caso de MOTO, conlleva la necesidad de compartir la ubicación de los usuarios para gestionar la distribución de contenidos. Esto establece un nuevo desafío para la seguridad, dado que la privacidad de la ubicación se ha convertido en una de las preocupaciones principales en las redes móviles y hace particularmente difícil alcanzar un nivel satisfactorio de privacidad respecto a la ubicación en situaciones donde los nodos confían en los Servicios Basados en la Localización (LBS) [31].

Los principales riesgos que se presentan en el entorno MOTO en relación a los usuarios, son:

1. La posibilidad de inyectar contenido erróneo, es decir, que o bien el "seed" o el nodo que lo retransmite modifique el contenido antes de entregarlo.
2. Que uno de los nodos no reenvíe el contenido y por lo tanto, los usuarios finales entren en la denominada "zona de pánico" y tengan que pedir el contenido a la plataforma MOTO de nuevo vía LTE.
3. La revelación de datos personales, es decir, que un nodo comunique a los otros nodos la identidad de un usuario de la plataforma o que un nodo intente monitorizar la actividad de otro usuario con el fin de obtener datos personales.

La solución de seguridad propuesta en este TFM debe evitar los riesgos citados anteriormente y, por tanto, cumplir una serie de requisitos como son: confidencialidad, es decir, que los datos enviados no sean leídos por terceras partes, integridad de los datos, que consiste en poder detectar si los datos han sido modificados y, finalmente, disponibilidad de recursos, es decir, garantizar que los usuarios puedan acceder cuando lo necesiten.

11.2. Solución de seguridad en MOTO

La solución de seguridad que se propone en MOTO se basa en tres mecanismos principalmente:

1. **Criptografía**: para proporcionar confidencialidad e integridad desde el origen de los mensajes.
2. **Anonimización de los usuarios mediante pseudónimos**: para evitar divulgación de identidades y localización.
3. **Gestión de la confianza y la reputación**: para identificar nodos maliciosos y egoístas.

Con los mecanismos expuestos a continuación se pretende conseguir una seguridad extremo a extremo y garantías de privacidad tanto para el contenido como para los usuarios.

11.2.1. Confidencialidad, integridad y autenticidad de los datos

En primer lugar, como ya se ha comentado anteriormente en los objetivos de seguridad, es muy importante proporcionar confidencialidad, integridad y autenticidad de los datos transmitidos. Para cumplir estas expectativas se hace uso de técnicas de criptografía que se compone de tres niveles de seguridad.

El primer nivel está orientado a asegurar que el contenido a difundir a través de MOTO sólo sea "legible" por parte de los destinatarios que solicitan la información. El proveedor de contenidos debe cifrar el contenido que envía a través de los servicios de MOTO y distribuir la clave de dicha encriptación a los receptores finales externamente de manera segura (vía LTE). De esta forma, se garantiza que sólo el destinatario final sea capaz de descifrar el contenido para poder visualizar los datos enviados.

El segundo nivel tiene por objetivo proporcionar integridad de los datos y asegurar su origen. Este nivel se genera cuando la plataforma MOTO firma el contenido cifrado, que ha recibido del proveedor de contenidos, con su clave privada. Solamente los nodos pertenecientes a MOTO que están en disposición de la clave pública de la plataforma MOTO, pueden hacerse con el contenido recibido del proveedor de contenidos. De esta forma, no será posible la modificación del contenido enviado sin que sea detectable por el destinatario de los datos.

Por último, el tercer nivel proporciona autenticación en las comunicaciones oportunistas, y garantiza que los nodos no acepten contenido de nodos no pertenecientes a los servicios MOTO. Este nivel comporta la encriptación que realiza cada nodo que retransmite el contenido (semilla o repetidor) con la clave pública de los nodos receptores (repetidor o destinatario). Con esta última capa de encriptación, se garantiza que sólo el nodo receptor sea capaz de descifrar los datos con su clave privada.

11.2.2. Anonimización mediante pseudónimos

En segundo lugar, se pretende que ningún usuario a excepción de la plataforma MOTO pueda conocer la información personal del resto de usuarios: su identidad real, su localización a lo largo del tiempo o su actividad en la red. Esto se consigue sustituyendo el uso de datos personales de usuarios por el uso de un conjunto de pseudónimos junto con claves asimétricas, que cada usuario recibe de la plataforma MOTO. Los pseudónimos proporcionados están correlacionados con un usuario concreto y con pares de claves público-privadas en cada instante, y esta correlación únicamente es conocida por el usuario concreto que tiene asignado cada conjunto de seudónimos y claves, y por la plataforma MOTO, siendo inviable obtener dicha información por parte de otro usuario. En ningún momento se difunde entre los nodos la identidad real de un usuario, y para mayor confidencialidad, se estipula un intervalo de tiempo en el que los pseudónimos y las claves público-privadas se cambian para cada usuario. En el caso de desear mayor privacidad, se plantea la asignación de un mismo pseudónimo a distintos

usuarios a lo largo del tiempo, evitando que se pueda seguir a un usuario en concreto a través del mismo.

Los nodos sólo intercambian los pseudónimos. Por lo tanto, si dos nodos quieren comunicarse y necesitan obtener la clave pública del otro, intercambian sus respectivos pseudónimos y con esos pseudónimos solicitan a la plataforma MOTO la clave pública del nodo con el que se van a comunicar. El hecho de que sea MOTO quien proporciona la clave pública garantiza que ésta se envía por una conexión segura (SSL/TLS) entre MOTO y el nodo además de que si el nodo es malicioso, es decir, su seudónimo no es válido, éste no reciba la clave pública solicitada.

De esta forma, además de garantizar el anonimato, los usuarios no tienen que enviar sus claves por la red (aun siendo públicas) sino que es MOTO quien las proporciona de forma segura.

11.2.3. Gestión de la confianza y la reputación

En último lugar, se pretende garantizar un proceso de difusión óptimo entre los nodos de la red móvil oportunista, mediante un marco que gestiona la confianza y reputación de los usuarios de los servicios MOTO. La gestión de la confianza en una red ad-hoc usualmente se basa en el intercambio entre los nodos de información acerca de la misma (feedback) y en base a la información que cada nodo recopila sobre los demás, deciden si aceptan o no una conexión con un determinado nodo.

En el esquema de comunicaciones propuesto en MOTO, esto tiene un grado añadido de dificultad, puesto que la plataforma MOTO realiza la gestión del feedback pero no toma parte en las comunicaciones entre los nodos. Por lo tanto, tras la comunicación entre dos nodos en la red oportunista, estos envían un mensaje (feedback) a MOTO, que debe actualizar el nivel de confianza del nodo emisor. Ambos nodos envían un mensaje de feedback a MOTO, el emisor con la confianza que espera recibir, y el receptor con la que otorga al emisor. Este mensaje tiene una doble función, informar a la plataforma acerca de la recepción del contenido para tomar decisiones de difusión, y, monitorizar el comportamiento que tienen los nodos por motivos de seguridad.

El feedback cumple los siguientes objetivos:

1. Demostrar que el contenido recibido es correcto, mediante el envío del resultado de aplicar una función hash al contenido recibido (calculado en base al contenido encriptado por el proveedor de contenidos, es decir, a los datos del primer nivel de criptografía).
2. Que la comunicación efectivamente tuvo lugar mediante el envío del tiempo en el que se recibió el mismo, la identificación mediante pseudónimos del otro nodo involucrado y el rol del nodo que envía el feedback: emisor o receptor.

3. La calidad de la conexión, basada en una escala definida previamente.

11.2.4. Distribución de claves

Para aplicar estos procedimientos de seguridad es necesario que los nodos obtengan las claves de una forma segura. En MOTO se plantea que el proveedor de contenidos sea el encargado de acordar la clave de sesión con el usuario final. A su vez, la plataforma MOTO es la encargada de distribuir las claves público-privadas a los nodos por el canal de control de la interfaz LTE por una comunicación segura (SSL/TLS).

11.3. Asunciones de seguridad

En este apartado se presentan una serie de asunciones que se han tenido en cuenta a la hora de definir los intercambios de seguridad:

- La conexión entre el proveedor de contenido y el nodo es segura debido a que se realiza sobre la tecnología LTE y se considera que el operador móvil se encarga de esa seguridad.
- El proveedor de contenido distribuye claves de sesión para el cifrado/descifrado del contenido a los usuarios a través de este canal seguro (el canal LTE).
- La plataforma MOTO siempre está accesible a los nodos.
- La conexión entre los nodos y la plataforma MOTO es segura debido a que se realiza sobre la tecnología LTE.
- Todos los nodos autorizados para usar la plataforma MOTO tienen la clave pública de la plataforma MOTO.
- Se asume que las capas físicas y lógicas de la infraestructura donde se despliegan los servicios MOTO son seguras mediante técnicas con un nivel de seguridad suficiente.

11.4. Intercambios previos de seguridad

En este apartado se detallan los mensajes intercambiados previamente al envío de contenido para garantizar que este sea confidencial e íntegro. Así como para que se mantenga el anonimato de todos los nodos que toman parte en la diseminación del contenido. En esta propuesta como se ha comentado anteriormente la confianza es una parte fundamental por lo tanto tras el intercambio del contenido se intercambian unos mensajes referentes a este ámbito.

Con el fin de asegurar la confidencialidad del contenido a distribuir a través de los servicios de MOTO se tienen que cumplir dos condiciones:

- El proveedor de contenido y el usuario tienen un canal seguro entre ellos para comunicarse sin ser a través de los servicios MOTO.

- Previo a la diseminación de contenido por MOTO, el usuario que solicita un contenido determinado acuerda una clave de sesión por este canal seguro con el proveedor de contenido para cifrar el contenido.

En las ilustraciones que se presenta a continuación se detallan todos los procesos necesarios para conseguir los objetivos de seguridad que se han detallado en apartados anteriores.

Ilustración 11: autenticación e identificación en MOTO

En la Ilustración 11 se representa el proceso de autenticación e identificación frente a la plataforma MOTO. Cabe comentar que para este proceso se utilizan las claves asimétricas del usuario que se quiere autenticar y de MOTO, es decir las claves de uso genérico. Para las posteriores comunicaciones se generan durante este proceso las claves de sesión que se utilizarán en los posteriores intercambios. Además de esto cabe mencionar que las comunicaciones referentes a este proceso se realizan sobre la tecnología LTE o WiFi, según tenga configurado el usuario su conexión a Internet, de forma segura.

En primer lugar el usuario comienza la comunicación con un mensaje de solicitud de conexión. A este mensaje le responde la plataforma MOTO con un mensaje en el que solicita al usuario que se autentique frente a la plataforma. A continuación y respondiendo a la solicitud de la plataforma MOTO el usuario que se quiere conectar le envía a MOTO su certificado firmado con la clave pública de la plataforma con el fin de que sólo MOTO sea capaz de descifrarlo con su clave privada. En el siguiente paso MOTO comprueba el estado del certificado, es decir que este certificado sea válido, y que el usuario tenga privilegios para hacer uso de la plataforma, en

caso de que no sea válido el certificado, es decir que no sea de un usuario legítimo, o que el usuario sea legítimo pero haya perdido el derecho a usar la plataforma por hacer uso de ella de forma incorrecta, no le permite al usuario conectarse y se acaba el proceso; y en caso de que sea correcto se generan los seudónimos de sesión y las claves asociadas a esos seudónimos y se las envía al usuario cifrado con la claves pública del usuario. El usuario contesta con un ACK cifrado con su clave privada para que se pueda comprobar que el mismo lo ha generado y no un usuario malicioso.

Una vez se han intercambiado todos los mensajes anteriormente citados el usuario está autenticado frente a la plataforma y ambos nodos (el usuario y MOTO) actualizan sus tablas de correlación de seudónimos y claves.

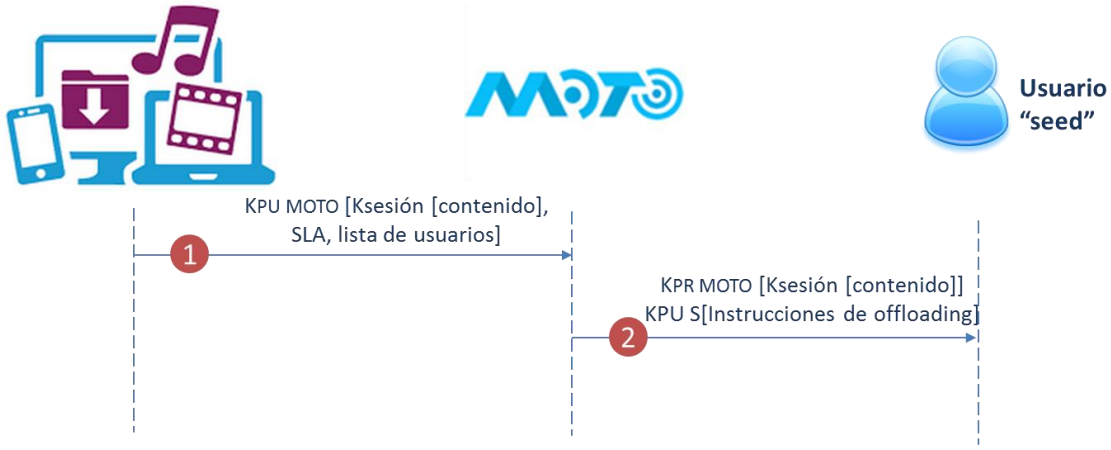


Ilustración 12: del proveedor de contenido a MOTO

En la Ilustración 12 se muestra como se envía el contenido solicitado al nodo "seed" que se encarga de distribuirlo hasta los destinatarios que lo han solicitado. Cabe mencionar que al igual que en el caso anterior las comunicaciones referentes a este proceso se realizan sobre la tecnología LTE o WiFi de forma segura. En este caso se utiliza una clave de sesión que se ha acordado entre el proveedor de contenido y el usuario final que desea recibir el contenido (proceso ajeno a la plataforma MOTO) y las claves asimétricas de MOTO y el usuario "seed".

Este proceso consta de dos pasos. En primer lugar, el proveedor de contenido tras haber recibido la petición del usuario y haber acordado con este la clave de sesión que utilizarán para la comunicación, envía a la plataforma MOTO el contenido cifrado con la clave de sesión, así como la lista de usuarios destinatarios y los SLAs acordados todo ello firmado con la clave pública de MOTO. En segundo lugar, la plataforma MOTO le envía al usuario "seed" cifrado con su clave privada el contenido firmado con la clave de sesión y además las instrucciones necesarias para llevar a cabo el offloading cifradas con la clave pública del nodo "seed".

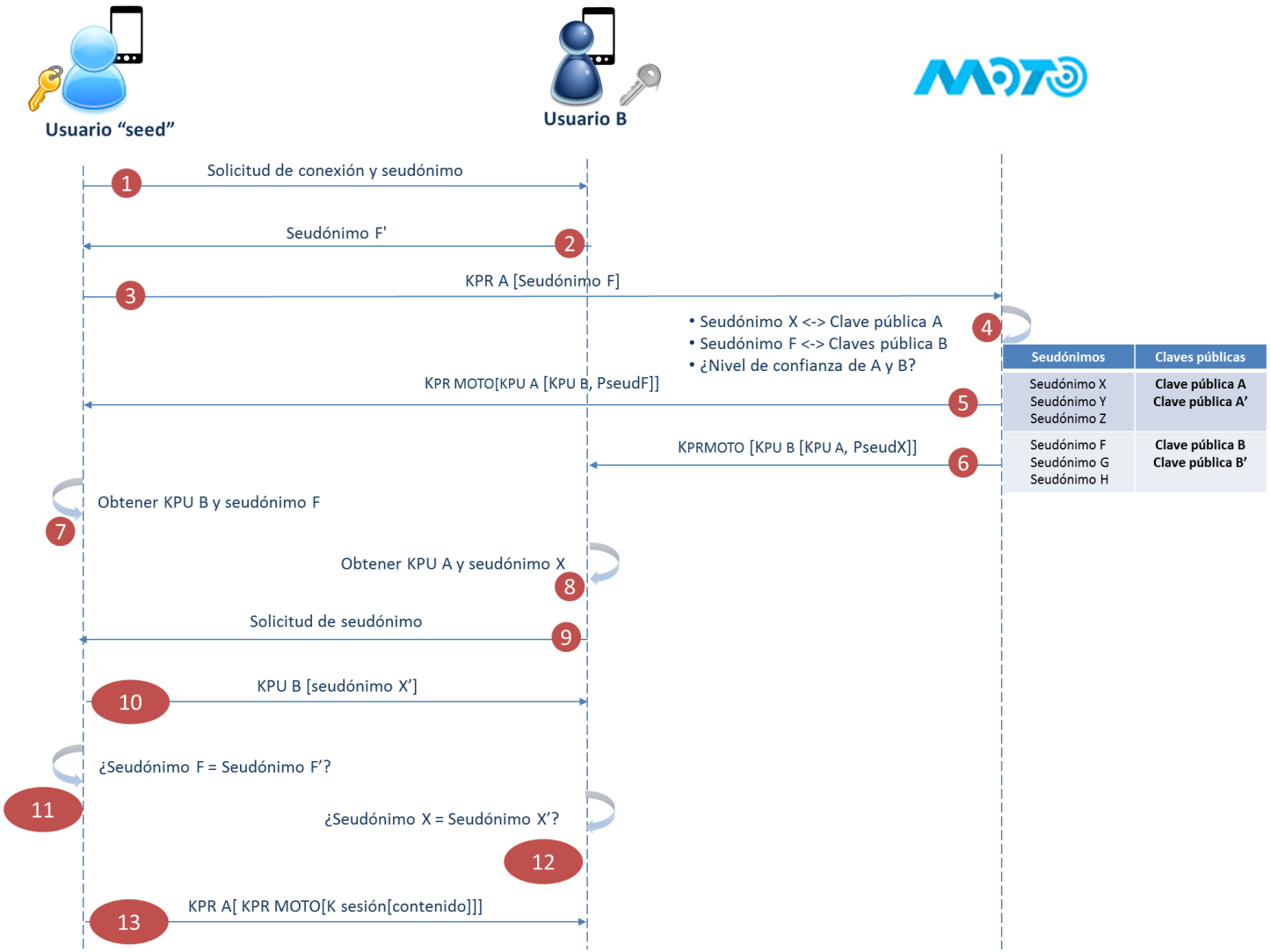


Ilustración 13: comunicación Ad-hoc

En la Ilustración 13 se muestran los mensajes previos al envío del contenido y el posterior envío del propio contenido. En esta comunicación toman parte el usuario A que es el "seed" al que MOTO le ha enviado anteriormente el contenido, el usuario B que es el usuario destinatario del contenido y la plataforma MOTO. Cabe comentar que las comunicaciones entre los nodos son a través de la plataforma de offloading y que las comunicaciones de los usuarios con la plataforma MOTO a través de WiFi o LTE. En este caso las claves utilizadas son las claves asimétricas de MOTO y las claves asimétricas y los seudónimos enviados por la plataforma MOTO a los usuarios en el proceso de autenticación.

En primer lugar, el nodo "seed" le envía al nodo destinatario del contenido una solicitud de conexión en la que le solicita el seudónimo de éste para comenzar con el proceso de autenticación entre ambos nodos. A esta solicitud el usuario B le envía su seudónimo en claro para que el nodo "seed" lo verifique ante MOTO. El nodo "seed" para proceder a la verificación le envía a MOTO el seudónimo recibido del usuario B firmado con su clave privada. Cuando MOTO recibe este mensaje del nodo "seed", comprueba (1) la correlación del seudónimo correspondiente a la clave pública de A (nodo "seed") para enviárselo a continuación al nodo B, (2) comprueba que el seudónimo recibido del usuario "seed" es válido y obtiene la clave pública asociada a ese seudónimo y (3) que el nivel de confianza de ambos nodos es válido y no han perdido el derecho a usar la plataforma. Una vez se han realizado las comprobaciones y se ha corroborado que ambos niveles de confianza están por encima del umbral que declina el derecho a uso de la plataforma MOTO genera dos mensajes que envía a ambos nodos que se componen de la clave pública y el seudónimo de su compañero firmado con la claves pública del nodo y esto a su vez firmado con la clave pública de MOTO (como se puede observar en los mensajes 5 y 6 de la Ilustración 13. A continuación ambos nodos (el nodo "seed" y el nodo B) obtienen de los mensajes recibidos de MOTO la clave pública y el seudónimo de su compañero.

Cuando el nodo B recibe la clave pública del "seed" y su seudónimo, le solicita al nodo "seed" el seudónimo para poder comprobar que no es un usuario malicioso. A esta solicitud el nodo "seed" responde con el seudónimo propio cifrado con la clave pública del nodo B.

Ambos comprueban que los seudónimos son correctos, es decir de nodos legítimos, y el nodo "seed" envía al nodo destinatario los datos que le ha enviado MOTO cifrados con su clave privada (es decir los datos que han salido del proceso en el que el proveedor de contenido ha cifrado el contenido que ha solicitado el usuario con la clave de sesión acordada entre ambos) a su vez cifrados con la clave privada del nodo "seed".

En caso de que el nodo destinatario descubriera mediante la comprobación de seudónimos que el nodo "seed" es un usuario malintencionado descartaría el paquete.

Y en caso de que sea el nodo "seed" el que descubra que el usuario B no es quien dice ser no se llegaría a enviar el último mensaje.

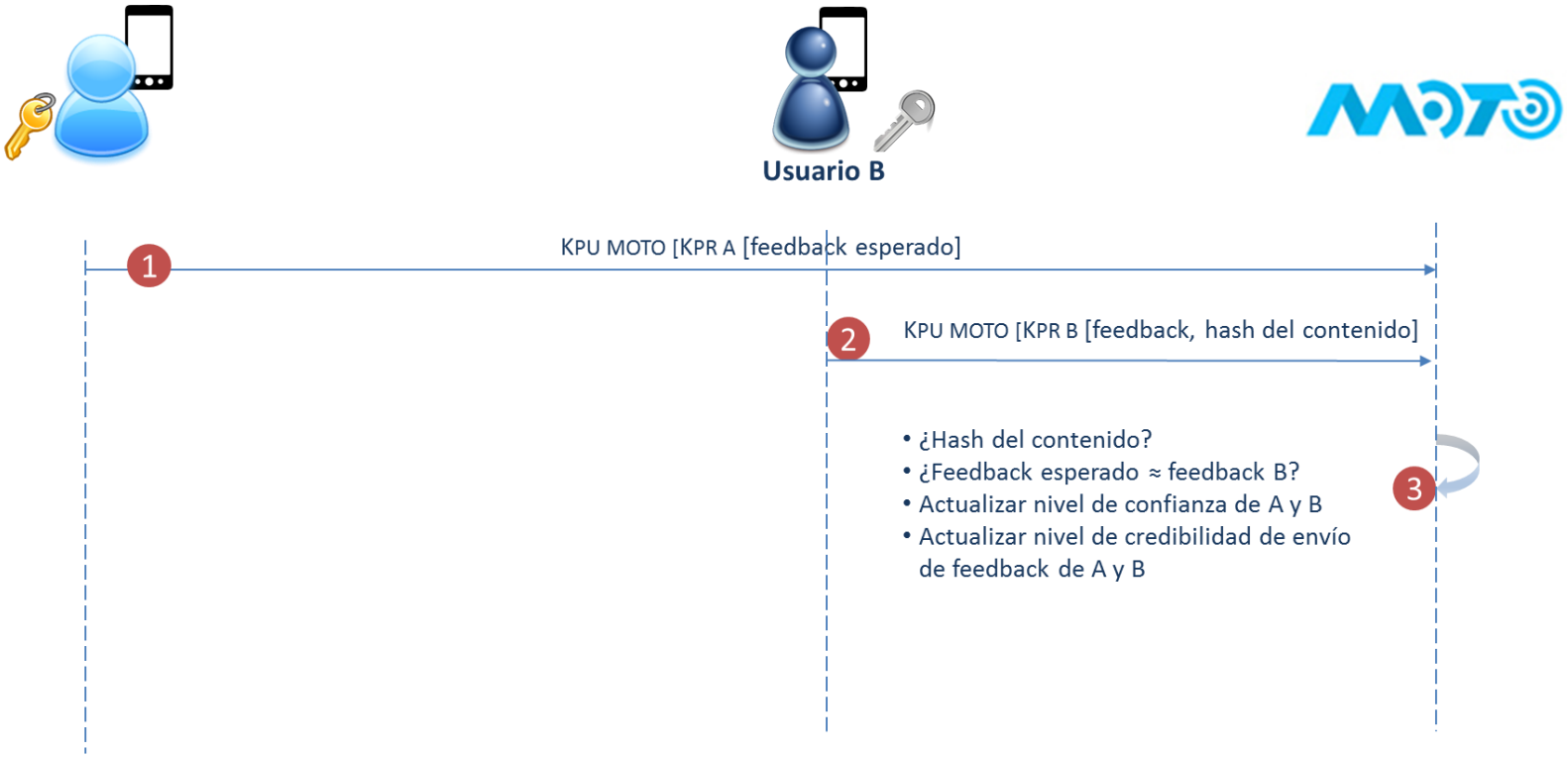


Ilustración 14: envío de "trust"

En la Ilustración 14 se muestran los mensajes enviados cuando el usuario B, es decir el usuario final, ha recibido el contenido. En esta comunicación al igual que en el caso anterior toman parte el usuario A que es el "seed", el usuario B que es el usuario destinatario del contenido y la plataforma MOTO. Cabe comentar que las comunicaciones de los usuarios con la plataforma MOTO son a través de WiFi o LTE. En este caso las claves utilizadas son las claves asimétricas de MOTO y las claves asimétricas y los seudónimos enviados por la plataforma MOTO a los usuarios en el proceso de autenticación.

En primer lugar, una vez se ha finalizado el envío el usuario "seed" envía a MOTO el feedback que espera recibir del usuario B cifrado con su clave privada y posteriormente con la clave pública de MOTO para poder garantizar que confidencialidad e integridad a ese feedback. Por otro lado, en cuanto el usuario B obtiene el contenido y comprueba si es correcto o no, obtiene un feedback en base a como ha sido el envío. A continuación, el usuario B envía ese feedback junto con un hash del contenido firmado con la clave de sesión para que MOTO pueda comprobar a que envío se refiere.

Una vez comprueba los feedbacks recibidos y basándose en la fiabilidad que la plataforma tiene sobre cada nodo se actualizan los niveles de confianza y de fiabilidad de ambos nodos.

12. Metodología y pruebas

En este apartado se va a describir la metodología seguida para llevar a cabo el TFM que se ha ido detallando a lo largo de los anteriores apartados.

12.1. Pasos previos

El primer paso para llevar a cabo este TFM ha sido la definición de objetivos, los cuales están detallados en su correspondiente apartado dentro de este documento. Así como analizar el estado del arte y el estado actual de las redes oportunistas y las comunicaciones D2D

12.2. Definición de la solución de seguridad

A continuación se ha definido la solución de seguridad. Para llevar a cabo esta tarea se ha analizado la plataforma a securizar y se han estudiado las principales amenazas en la principal tecnología empleada dentro de la misma, es decir, las redes oportunistas. Se han definido los objetivos de seguridad y se ha detallado la solución de seguridad. Estos objetivos de seguridad como se ha comentado anteriormente son confidencialidad, autenticidad e integridad de los datos transmitidos. Así como el anonimato de los usuarios que usan la plataforma y servicios de gestión de la confianza.

Una vez definida la solución de seguridad ha sido necesario llevar a cabo simulaciones con el fin de conocer la viabilidad de la misma para su posterior implementación. Para poder desarrollar las simulaciones ha sido necesario en primer lugar definir y poner en marcha el escenario que se va a utilizar para simular y con el que se van a obtener los resultados para analizar el rendimiento de la solución. Para poner en marcha el escenario se ha partido de un escenario previamente diseñado y configurado, en el cual se han realizado pruebas de rendimiento de diferentes estrategias de offloading.

12.3. Plan de pruebas en un entorno simulado

En este apartado se detallan las simulaciones llevadas a cabo con el fin de validar la viabilidad de la solución de seguridad propuesta. El objetivo de estas simulaciones es evaluar el impacto de aplicar la solución de seguridad a los algoritmos de offloading.

Como se ha comentado anteriormente este TFM es parte de un proyecto más grande y los resultados de las simulaciones completas están en el entregable 5.2 [32] (disponible en la página del proyecto [6]) que se ha enviado a la comisión europea por parte de todos los miembros del consorcio encargados de las simulaciones.

12.3.1. Entorno de simulación

Para llevar a cabo las simulaciones se ha empleado la plataforma iTETRIS [33] la cual se compone del simulador de eventos discretos NS-3 y del simulador de tráfico SUMO. Para la interoperabilidad entre ambos simuladores se hace uso de un framework desarrollado por el consorcio de empresas que desarrollaron el proyecto iTETRIS. Cabe comentar que en este TFM no se ha hecho uso de la plataforma SUMO ya que las pruebas no se han realizado en una ubicación real y los usuarios son peatones que se desplazan por una zona cuadrada.

12.3.2. Objetivo de las simulaciones

Las simulaciones de seguridad llevadas a cabo en este TFM están dedicadas a analizar los tres aspectos principales de la solución de seguridad propuesta. En primer lugar se han llevado a cabo simulaciones de Monte Carlo para comprobar la eficiencia de la distribución de claves y seudónimos. En estas simulaciones, se mide el tiempo que tarda la red en estabilizarse, es decir el tiempo necesario para refrescar las claves y seudónimos, con el fin de poder realizar nuevas comunicaciones permitiendo a los usuarios cambiar sus identificadores. En segundo lugar se llevan a cabo simulaciones de eventos para medir el retardo adicional introducido por los mensajes de establecimiento de conexión que se intercambian previamente al envío del contenido. Por último se llevan a cabo simulaciones para medir el impacto debido a la implementación de los mecanismos de confianza. Por lo tanto los objetivos de las simulaciones son:

- **Cuantificar el tiempo necesario para la diseminación de las claves y los seudónimos**: este tiempo se quiere que sea mínimo ya que durante este tiempo la red estará parada, es decir, sin poder establecerse relaciones oportunistas para reenviar contenido.
- **Cuantificar el retardo de los intercambios previo de autenticación**: se quiere comprobar si este retardo es asumible.
- **Cuantificar el impacto del esquema de confianza propuesto**: se quiere comprobar si el retardo adicional debido a este esquema compensa con la información que aporta el envío del trust.

12.3.3. Descripción y diseño de las simulaciones

Los tres tipos de simulaciones definidos en la sección anterior se han llevado a cabo en el mismo escenario, un área cuadrada de 100 m^2 (10m x 10m). A continuación se muestra una imagen que ilustra la topología de red definida en las simulaciones.

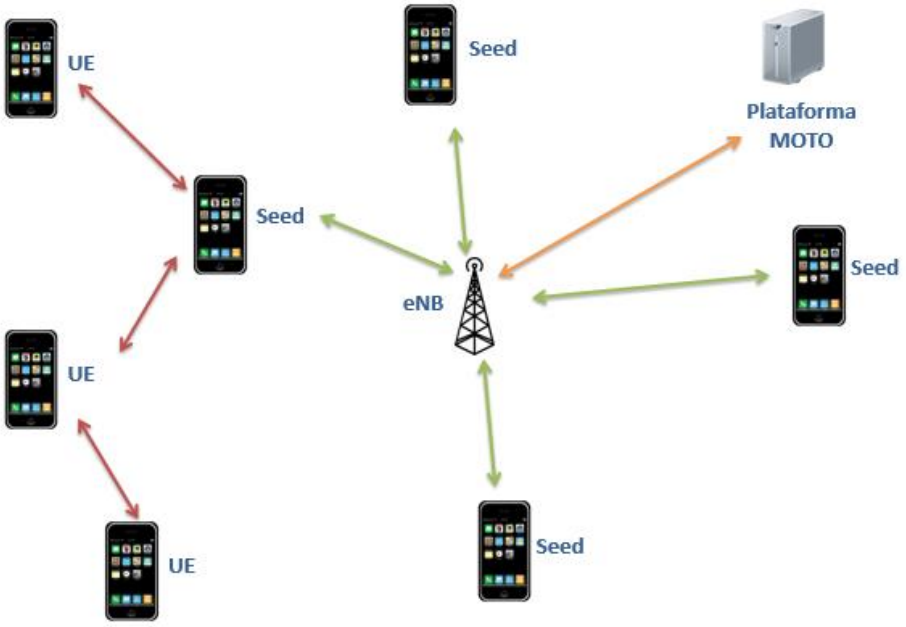


Ilustración 15: escenario de simulación

La topología de red se compone de un nodo eNB, es decir, un eNodeB el cual se encarga de enviar la información que le llega de la plataforma MOTO a través de la tecnología LTE. La plataforma MOTO que es la encargada de enviar tanto las claves y los seudónimos, a todos los nodos mediante LTE, como los datos solicitados a un proveedor de contenidos a los seed, mediante LTE para que se pueda reenviar por la red al resto de nodos destinatarios.

El nodo eNB se ha posicionado en el centro del cuadrado, es decir, en la coordenada X=5, Y=5. Los demás nodos (seeds y UEs) se han distribuido de forma aleatoria a través del área de simulación. El ancho de banda asignado a la plataforma MOTO es el 50% del ancho de banda disponible con el fin de permitir que otras comunicaciones puedan llevarse a cabo, como por ejemplo llamadas de voz. Sobre este escenario se han establecido las tres tandas de simulaciones:

- La primera tanda de simulaciones se ha realizado con la intención de comprobar la estabilización de la red, es decir, el tiempo que pasa desde que la plataforma MOTO ejecuta el refresco del par de claves y seudónimos, y el tiempo en el que todos los nodos han recibido sus nuevas claves y seudónimos. Los mensajes que se envían para distribuir las claves y seudónimos se envían sobre la red LTE del operador. Se han llevado a cabo simulaciones con diferentes longitudes de mensajes para poder evaluar si es viable enviar, en una misma tanda de refresco varios pares de claves y seudónimos, con el objetivo de retardar lo menos posible el resto de las comunicaciones.

- La segunda tanda de simulaciones mide el tiempo pasado desde que la plataforma MOTO envía el contenido a distribuir, y el tiempo en el que todos los nodos destinatarios tienen el paquete. Este tiempo incluye la distribución del contenido, así como los mensajes punto a punto intercambiados relacionados con la seguridad (autenticación, autorización, etc. de los usuarios) para las comunicaciones entre UEs.
- La tercera tanda de simulaciones consiste en evaluar el retardo introducido por el mecanismo de confianza, teniendo en cuenta que los feedbacks transmitidos tienen que ser generados por el UE, transmitidos a la plataforma MOTO y procesados por la plataforma MOTO

12.3.4. Resultados esperados

Las simulaciones llevadas a cabo tienen el objetivo de mantener la viabilidad de la solución de seguridad propuesta por el entrono MOTO. Por supuesto, se espera que introduciendo los mecanismos de seguridad se aprecie un impacto en el rendimiento y algunos retardos adicionales. La forma en la que más se degradan las comunicaciones es mediante el retardo y la pérdida de paquetes por lo tanto se van a tomar ambos parámetros como principales métricas. Se esperan obtener los siguientes resultados:

1. En relación a la primera tanda de simulaciones, es decir, a la cuantificación del tiempo de estabilización de la red se espera que este retardo sea el más bajo posible ya que durante este tiempo de refresco de claves y seudónimos los nodos no van a ser capaces de enviar o recibir datos. Además se espera que este tiempo dependa de la densidad de nodos.
2. En relación al tiempo necesario para intercambiar el contenido introduciendo las medidas de seguridad se espera que la implementación de la seguridad no introduzca un retardo excesivamente alto y que los nodos que tengan que volver a solicitar el contenido por haber entrado en la zona de pánico sean los mínimos posibles. Al igual que en el caso anterior se espera que estos datos a medir sean mayores cuanto mayor sea la densidad de los nodos.
3. En relación al envío del trust se espera que el retardo introducido sea mínimo al igual que los nodos que entran en la zona de pánico. Se espera que el impacto de implementar esta medida de seguridad sea prácticamente despreciable.

12.3.5. Parámetros de configuración de la simulación

En este apartado se presentan los principales parámetros establecidos en la herramienta de simulación con el fin de llevar a cabo las simulaciones anteriormente citadas. Los parámetros configurables en las simulaciones son:

- **Número de UEs**: hace referencia a la cantidad de usuarios conectados a la plataforma MOTO.
- **Número de seeds**: hace referencia a la cantidad de usuarios que la plataforma MOTO selecciona como "seed" para la retransmisión de contenido.
- **Número de eNBs**: hace referencia a la cantidad de eNodeB disponibles en la plataforma.
- **Tipo de contenido**: hace referencia al tipo de contenido que se intercambia, es decir, texto, foto, video, etc.
- **Tamaño del contenido**: hace referencia a la longitud de los datos intercambiados.
- **Tiempo de vida de los mensajes**: tiempo durante el cual el mensaje puede ser reenviado entre los nodos hasta llegar al nodo destino.
- **Tiempo para entrar en la zona de pánico**: la zona de pánico es un estado en el que entra el nodo si en un tiempo especificado por este parámetro no ha recibido la información solicitada. En caso de entrar en la zona de pánico el nodo solicita a la plataforma MOTO de nuevo la información previamente solicitada y la plataforma MOTO se la envía en esta ocasión por la conexión LTE en vez de mediante técnicas de offloading.
- **Patrones de movilidad de los nodos**: hace referencia a como se mueven los nodos, es decir, estático (no se mueven), lineal o aleatorio.
- **Número de inyecciones periódicas**: este parámetro hace referencia a cada cuanto se inyecta tráfico en el caso de que se quiera enviar una misma información cada cierto periodo de tiempo.
- **Tiempo para la primera inyección de tráfico**: este parámetro es necesario para determinar cuánto tiempo pasa desde que se inicia la simulación hasta que se pone en marcha el envío. Este tiempo es necesario para que los nodos consigan mediante DHCP la IP en el simulador y se ponga en funcionamiento la plataforma con el fin de que no haya errores derivados de falta de conexión de los nodos.
- **Habilitado el envío de la posición**: este parámetro permite determinar si se desea que se envíe la posición del nodo periódicamente o no.
- **Tiempo de simulación**: tiempo total que se simula incluyendo el tiempo para la primera inyección.
- **Número de nodos maliciosos**: porcentaje de nodos del total de los UEs que tienen un comportamiento incorrecto. En este TFM se ha simulado que son nodos egoístas que no distribuyen el tráfico cuando les llega.
- **Estrategia de los seudónimos**: este parámetro hace referencia a si los seudónimos cambian o no durante la simulación.

La tabla que se muestra a continuación contiene los parámetros de la primera tanda de simulaciones:

Parámetro	Variable/fijo	Unidades	Mínimo	Máximo
Número de UEs	Variable	Número	10	150
Número de seeds	Fijo	Porcentaje	10%	
Número de eNBs	Fijo	Número	1	
Tipo de contenido	Fijo	Video/Foto/Texto	Texto	
Tamaño del contenido	Variable	Bits	320	600
Tiempo de vida de los mensajes	Fijo	Segundos	2	
Tiempo para entrar en la zona de pánico	Variable	Segundos	3	8
Patrones de movilidad de los nodos	Fijo	Lineal, aleatorio o estático	Aleatorio	
Tiempo para la primera inyección de tráfico	Fijo	Segundos	1	
Habilitado el envío de la posición	Fijo	Si/No	Si	
Tiempo de simulación	Fijo	Segundos	10	
Parámetros específicos de seguridad				
Estrategia de los seudónimos	Fijo	Estático, variable, variable para diferentes nodos	Variable para diferentes nodos	

Tabla 6: parámetros de la primera tanda de simulaciones.

La tabla que se muestra a continuación contiene los parámetros de la segunda y tercera tanda de simulaciones:

Parámetro	Variable/fijo	Unidades	Mínimo	Máximo
Número de UEs	Variable	Número	10	150
Número de seeds	Fijo	Porcentaje	10%	
Número de eNBs	Fijo	Número	1	
Tamaño del contenido	Fijo	Bytes	40 (paquetes de control) 30 k (paquetes de datos)	
Tiempo de vida de los mensajes	Fijo	Segundos	6	
Tiempo para entrar en la zona de pánico	Fijo	Segundos	7	
Patrones de movilidad de los nodos	Fijo	Lineal, aleatorio o estático	Aleatorio	
Número de inyecciones periódicas	Fijo	Número	1	
Tiempo para la primera inyección de tráfico	Fijo	Segundos	1	
Habilitado el envío de la posición	Fijo	Si/No	Si	
Tiempo de simulación	Fijo	Segundos	15	
Parámetros específicos de seguridad				
Número de nodos maliciosos	Fijo	Porcentaje	5%	

Estrategia de los seudónimos	Fijo	Estático, variable, variable para diferentes nodos	Variable para diferentes nodos

Tabla 7: parámetros de la segunda y tercera tanda de simulaciones.

La principal diferencia entre la segunda y tercera tanda de simulaciones es que en la tercera se incluye además de las comunicaciones de la segunda tanda el envío de la información de confianza.

12.3.6. Parámetros a medir

Como se ha comentado anteriormente las principales métricas son el retardo extremo a extremo y la pérdida de paquetes. La pérdida de paquetes se evalúa mediante el número de nodos que entran en la zona de pánico, ya que como se ha comentado anteriormente la zona de pánico es un estado al que pasan los nodos si pasado un tiempo configurado no reciben la información solicitada.

En todas las simulaciones se mide el retardo extremo a extremo. Sin embargo, la pérdida de paquetes se evalúa únicamente en la segunda y tercera tanda de simulaciones debido a que es cuando se envía tráfico mediante técnicas de offloading.

12.3.7. Resultados de las simulaciones

A continuación, se muestran los resultados de las pruebas de simulación detalladas en este apartado.

Primera tanda de simulaciones

En las dos siguientes tablas (referencias) se muestran los retardos medios para la primera tanda de simulaciones, es decir, se muestra el tiempo que la red debería estar parada para que todos los nodos hayan recibido la nueva tanda de claves y seudónimos con lo que poder comunicarse. Este tiempo se ha denominado tiempo de estabilización de la red. Los retardos mostrados en las siguientes tablas son en milisegundos. La primera tabla es para enviar un par de claves y un seudónimo (320 bits) y la segunda para enviar estos datos para dos intervalos de tiempo (640 bits), es decir, dos pares de claves con sus correspondientes seudónimos.

Nº NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	12,986	0,567	13,996	8,546
15	16,863	0,372	17,494	14,132
50	52,504	0,296	52,987	49,915
150	127,524	0,378	127,990	124,807

Tabla 8: Resultados de envío de un par de claves y seudónimos (320 bits).

Nº NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	14,680	0,606	15,498	9,610
15	17,880	0,379	18,498	15,016
50	61,731	0,352	62,451	60,494
150	148,174	0,509	148,957	146,483

Tabla 9: Resultados de envío de un par de claves y seudónimos (640 bits).

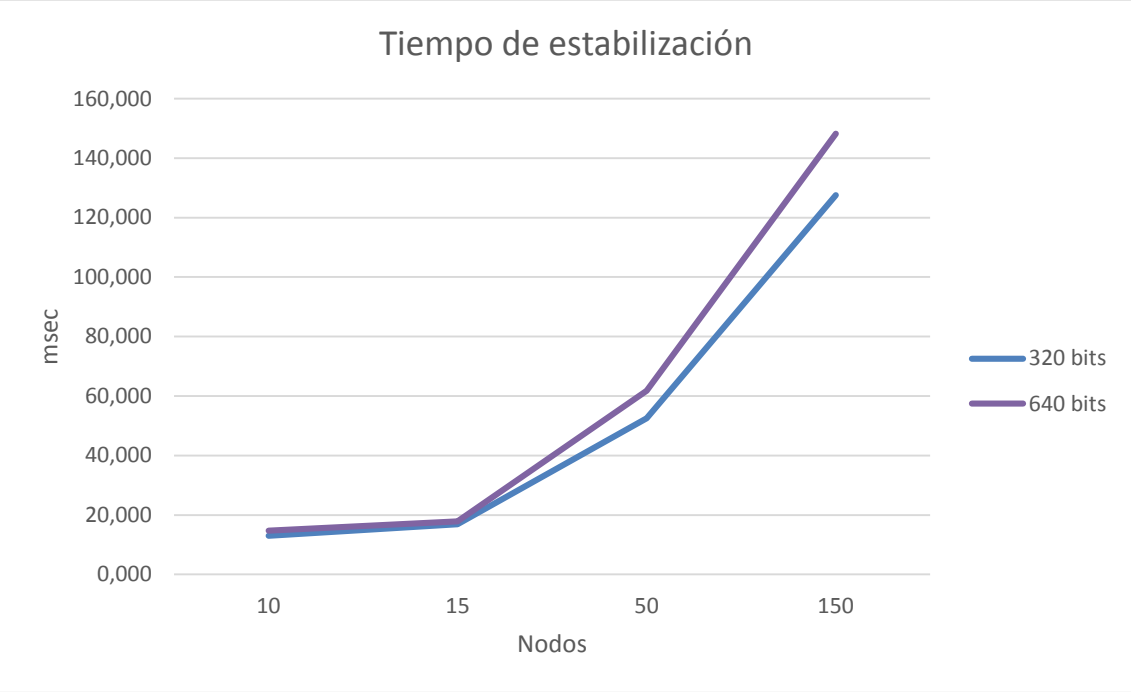


Ilustración 16: Gráfica que compara resultados de tiempo de estabilización.

Como se puede observar en los resultados, el tiempo que supone reenviar las claves y seudónimos actualizados es bastante reducido por lo que este proceso no dejaría la red parada un tiempo excesivo. Además se puede observar que es mejor enviar dos pares de claves-seudonimos cada vez ya que esto permite tener que para la red menos ocasiones para reiniciar estos parámetros y la diferencia de tiempo es mínima.

Segunda tanda de simulaciones

En la siguientes tabla (referencias) se muestran los retardos medios para la segunda tanda de simulaciones, es decir, se muestra el tiempo que tarda en llegar el contenido a los nodos destinatarios mediante relaciones oportunistas. Para poder comprobar el retardo introducido debido a la seguridad se han realizado dos tipos de simulaciones, sin seguridad (color azul en la tabla) y con seguridad (color blanco en la tabla). Los resultados que se muestran en la siguiente taba son en milisegundos.

NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	150,72	1,40	152,91	148,08
	515,11	2,42	547,79	490,07
15	247,09	3,07	249,35	241,57
	796,59	9,35	855,58	733,35
50	1367,39	3,09	1371,17	1363,30
	3003,10	9,72	2855,38	3164,65
150	3329,92	1,06	3331,71	3327,92
	8025,04	7,38	8252,45	7735,52

Tabla 10: Comparación de resultados con seguridad y sin seguridad.

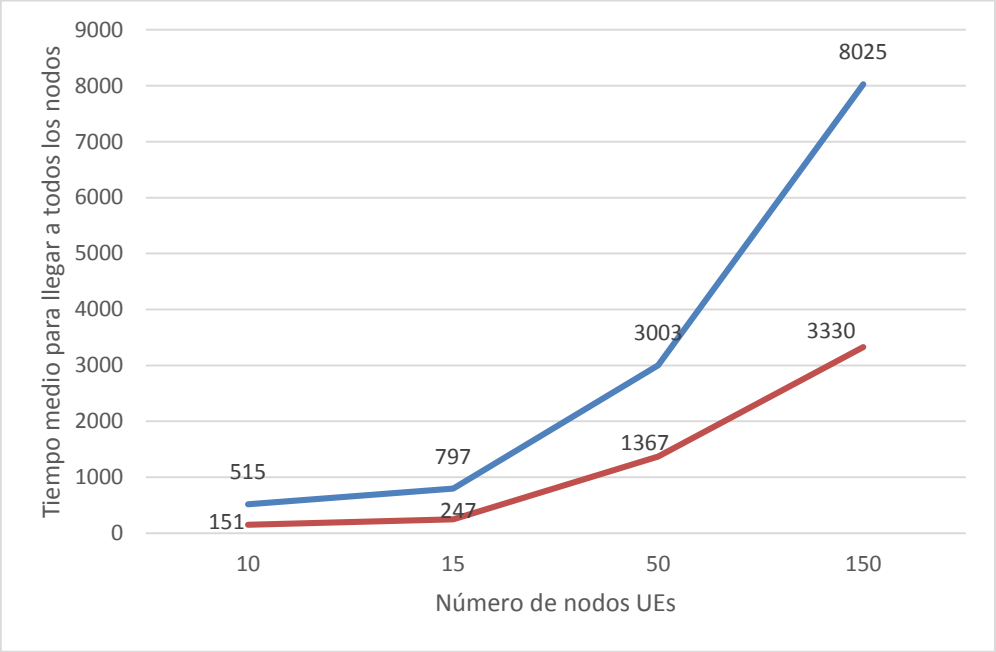


Ilustración 17: Gráfica que compara el retardo sin seguridad y con seguridad.

Como se puede observar para 150 nodos el retardo extra que se incluye debido a seguridad es bastante grande en comparación con el resto de casos, pero aun así solo se trata de una diferencia de 5 segundos de espera. Para este caso debería plantearse escoger más nodos que hagan la función de "seed" que en este caso si se quiere bajar este valor. Para el resto de concentraciones de usuarios los valores son bastante aceptables debido a que tampoco son valores demasiado grandes.

En esta misma tanda de simulaciones se han medido la pérdida de paquetes. Cabe comentar que como se ha comentado antes este parámetro se mide con los usuarios que entran en la denominada zona de pánico, es decir que pasado un tiempo desde la solicitud no han recibido los datos.

Los resultados se muestran en la siguiente tabla:

NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	0,13	0,12	1	0
	0,30	0,22	1	0
15	0,23	0,25	2	0
	0,58	0,57	2	0
50	1,08	0,70	4	0
	1,54	0,90	4	0
150	2,57	1,40	5	0
	3,46	1,80	5	0

Tabla 11: Nodos que entran en la "zona de pánico" con seguridad y sin seguridad.

Como se puede observar en estos resultados con el incremento de nodos y por consiguiente con el incremento de los paquetes que circulan por la red cada vez es mayor el número de nodos que entran en la zona de pánico y, por lo tanto, tienen que solicitar de nuevo el contenido vía LTE. Esto se podría solucionar incrementando el tiempo para entrar en la zona de pánico con el número de nodos de tal forma que cuantos más nodos haya este parámetro se mantenga más o menos estable.

Tercera tanda de simulaciones

En la siguientes tabla (referencias) se muestran los retardos medios para la tercera tanda de simulaciones, es decir, se muestra el tiempo que tarda en llegar el contenido a los nodos destinatarios mediante relaciones oportunistas (tiempo medido anteriormente) sumado al tiempo que tarda MOTO en recibir el trust de los nodos involucrados en la comunicación. La necesidad de medir este retardo es comprobar si el tiempo extra que requiere enviar el trust compensa con la información que aporta. Para poder comprobar el retardo introducido debido al trust se han realizado dos tipos de simulaciones, sin trust (color azul en la tabla), con trust (color blanco en la tabla). Los resultados que se muestran en la siguiente taba son en milisegundos.

NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	150,72	1,40	152,91	148,08
	515,11	2,42	547,79	490,07
15	247,09	3,07	249,35	241,57
	796,59	9,35	855,58	733,35
50	1367,39	3,09	1371,17	1363,30
	3003,10	9,72	2855,38	3164,65
150	3329,92	1,06	3331,71	3327,92
	8025,04	7,38	8252,45	7735,52

Tabla 12: Comparación de resultados con trust y sin trust.

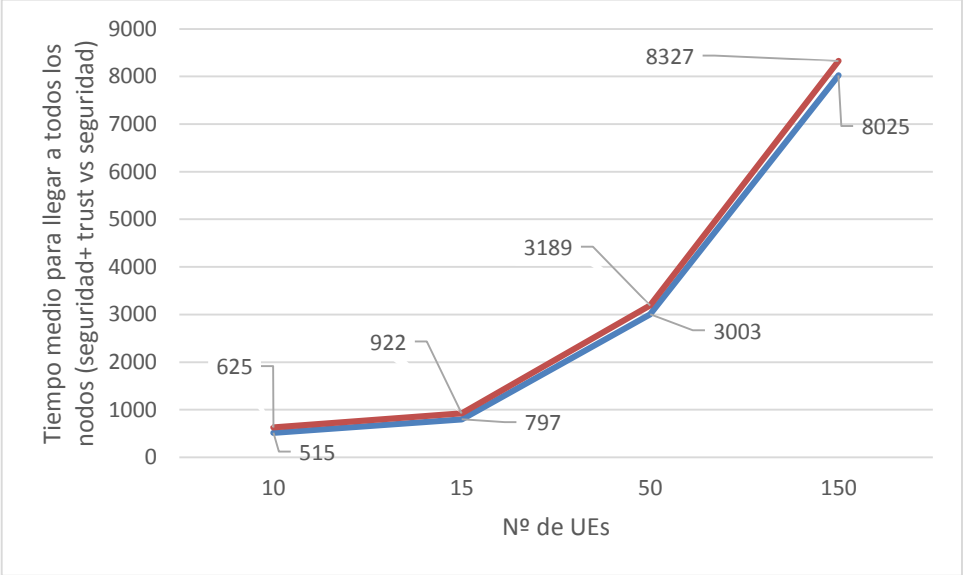


Ilustración 18: Gráfica que compara el retardo sin trust y con trust.

Como se puede observar para todos los casos de concentraciones de usuarios los valores son bastante aceptables debido a que el máximo retardo que incluye el envío del trust son 300 milisegundos y los datos que aporta para poder localizar a nodos malintencionados es muy importante.

En esta misma tanda de simulaciones se han medido la pérdida de paquetes. Cabe comentar que como se ha comentado antes este parámetro se mide con los usuarios que entran en la denominada zona de pánico, es decir que pasado un tiempo desde la solicitud no han recibido los datos. Los resultados se muestran en la siguiente tabla:

NODOS	MEDIA	VARIANZA	MÁXIMO	MÍNIMO
10	0,30	0,22	1	0
	0,33	0,23	1	0
15	0,58	0,57	2	0
	0,61	0,59	2	0
50	1,54	0,90	4	0
	1,63	1,05	5	1
150	3,46	1,80	5	0
	4,17	1,93	6	1

Tabla 13: Nodos que entran en la "zona de pánico" con trust y sin trust.

Como se puede observar en estos resultados con el incremento de nodos y al haber introducido el envío del trust el número de nodos que entran en la zona de pánico y, por lo tanto, tienen que solicitar de nuevo el contenido vía LTE no varía en gran medida con respecto al caso anterior.

12.4. Plan de pruebas en un entorno real

Una vez analizado el rendimiento de la solución de seguridad en un entorno simulado se va a analizar la seguridad que proporciona la solución en un entorno real. Para poder llevar a cabo estas simulaciones se ha desarrollado un framework de seguridad que tiene como objetivo asegurar la integridad y confidencialidad del contenido, así como la privacidad del usuario durante el proceso de transmisión del contenido, principalmente sin comprometer el rendimiento y la eficiencia del sistema. Cabe comentar que los módulos no relacionados con la seguridad se encuentran en el documento D5.3 [34] disponible en la web del proyecto [6].

12.4.1. Descripción del prototipo

Se han implementado los siguientes módulos para alcanzar los objetivos de seguridad citados anteriormente:

- Módulo de Login: Este módulo se encarga de la autorización y autenticación durante el proceso de acceso a la aplicación. Además de usar el método convencional de usuario y contraseña, esta información de Login está cifrada con el algoritmo SHA1. De esta forma, se evitan los posibles intentos de robo de identidad. Por último, en el servidor de seguridad se mantiene un fichero de log con todos los accesos a la plataforma.
- Módulo de firma de fichero: Este módulo se encarga de asegurar la integridad del contenido, así como la autenticación del nodo que reenvía el fichero, bien cuando MOTO lo distribuye a través de la plataforma a los receptores o mediante comunicaciones D2D. El servidor de seguridad es el responsable de generar la clave pública y privada de MOTO mediante el algoritmo RSA-SHA1, el cual es un método de criptografía asimétrica para verificar que el fichero es exactamente lo que pretende ser. A partir de este momento el servidor de seguridad puede firmar sus ficheros con la clave privada de MOTO con tiempo de uso limitado y a continuación, la firma digital puede ser compartida por una llamada REST, tan pronto como el terminal de usuario termine de descargarse el contenido. Una vez ha terminado la descarga, los receptores pueden verificar la firma con la clave pública de MOTO correspondiente obtenida en el proceso de Login anterior.
- Módulo de cifrado y descifrado: Como este módulo es para prevenir que se inyecte modifique el contenido solicitado por contenido erróneo o modificado, su uso es opcional si el canal de transmisión está asegurado, por ejemplo, con HTTPS. De todas formas, el servidor de seguridad puede cifrar el fichero con la clave de cifrado de MOTO. A continuación, los receptores Android verifican la firma del fichero y descifran el fichero cifrado para conseguir el fichero original.

Como parte del prototipo de MOTO, la propuesta de seguridad se tiene que poder integrar sin problemas con la plataforma MOTO con el fin de asegurar el funcionamiento eficiente y exitoso del resto de servicios MOTO. Para ello, el flujo de trabajo de integración de seguridad se establece en el siguiente diagrama secuencial.

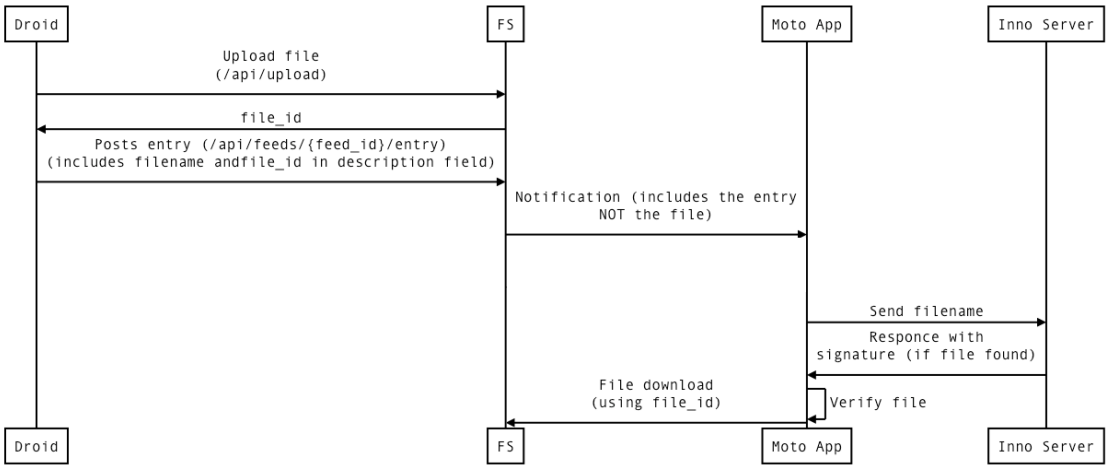


Ilustración 19: Flujo de trabajo de integración de seguridad.

Como se puede ver en el flujo, el servidor de seguridad (INNO Server) está separado del servidor web, para proteger los datos privados y sensibles, como las contraseñas de los usuarios, con una capa extra de control de acceso. Por otro lado, el servidor de seguridad solo se comunica con la app MOTO una vez durante el proceso de transmisión de fichero. Además, el módulo de verificación se ejecuta localmente en el dispositivo móvil. De esta forma, se interfiere lo mínimo posible con los demás servicios MOTO. Debido a que el canal seguro sobre HTTPS se ha establecido entre la plataforma MOTO y la app MOTO, el módulo de cifrado y descifrado se puede sustituir por el servicio de cifrado bidireccional que ofrece HTTPS.

12.4.2. Escenarios de pruebas

El escenario desplegado para las pruebas se ha implementado con una configuración WI-FI. Consiste en una red WI-FI integrada con la plataforma MOTO y accesible a través de Internet.

En las primeras versiones del prototipo, las comunicaciones D2D se establecieron mediante el uso de WiFi en modo adhoc. Aunque no está soportado oficialmente, en anteriores versiones de Android (2.4 e inferiores), era posible establecer la interfaz WiFi en ese modo. Sin embargo, esta funcionalidad se eliminó debido a características de seguridad. Usando dispositivos antiguos con la versión de Android 2.4 las pruebas no fueron aceptables debido a que la versión es demasiado obsoleta y la falta de soporte LTE.

En el momento de realizar las pruebas no estaban disponibles tecnologías de capa inferior adecuadas para el transporte de comunicaciones D2D. Por ejemplo, Bluetooth o WiFi

direct requieren un emparejamiento entre dispositivos previo al intercambio de contenido y este hecho no es aceptable para diseminación de contenido basado en un enfoque oportunista, principalmente por el retardo y la información de señalización que se introduce en el proceso de emparejamiento. Además, este hecho impide escalar el número de dispositivos involucrados en la diseminación porque se considera un modelo maestro-esclavo evitando las comunicaciones multisalto. El proceso de descubrimiento de nodos vecinos también está limitado por estas deficiencias. Adicionalmente, WiFi direct en realidad está emulando un punto de acceso WiFi en el dispositivo que entrega los datos. Por lo tanto, es algo similar a usar un punto de acceso como un realy.

Debido a las limitaciones comentadas, se ha decidido utilizar un punto de acceso WiFi como un relay para encargarse de las comunicaciones D2D con el prototipo, lo cual es similar al escenario "locally routed" definido en la versión 13 de funcionalidades ProSe del 3GPP. Esta se considera la mejor opción hasta que las tecnologías de comunicaciones D2D estén disponibles, por ejemplo, con la estandarización del 3GPP. Será entonces cuando se incluyan capacidades reales D2D en el prototipo actual.

12.4.3. Plan de pruebas

Las pruebas detalladas a continuación cubren la validación de las funcionalidades de seguridad implementadas en el prototipo.

La primera prueba tiene como objetivo validar que el usuario es capaz de autenticarse mediante la app MOTO en la plataforma y así poder empezar a usar los servicios de MOTO. Para llevar a cabo esta prueba la plataforma MOTO debe estar accesible por el UE, es decir, debe estar en el rango de cobertura. El procedimiento para realizar esta prueba es el siguiente:

- El usuario MOTO realiza una petición HTTPS a la plataforma MOTO para acceder a los servicios.
- La plataforma MOTO solicitará las credenciales.
- El UE se autenticará ante la plataforma.
- La plataforma MOTO permitirá al usuario participar.

La segunda prueba tiene como objetivo verificar que la plataforma MOTO es capaz de firmar el contenido y que la aplicación MOTO es capaz de verificar la firma. Para poder realizar esta prueba el nodo debe estar dentro del rango de cobertura de MOTO y estar autenticado con el paso anterior. El procedimiento para llevar a cabo esta prueba es el siguiente:

- El usuario MOTO envía una petición HTTPS a la plataforma MOTO pidiéndole algún contenido.
- La plataforma MOTO va a firmar el contenido con la firma de MOTO.
- El UE recibe el contenido ye s capaz de verificar la firma de MOTO.

La tercera y última prueba llevada a cabo tiene como objetivo verificar que la plataforma MOTO es capaz de cifrar el contenido antes de enviarlo a los usuarios y que los usuarios son capaces de descifrarlo. Como en el caso anterior para poder realizar esta prueba el nodo debe estar dentro del rango de cobertura de MOTO y estar autenticado. El procedimiento para realizar esta prueba es el siguiente:

- El usuario MOTO realiza una petición HTTP a la plataforma MOTO para pedir el contenido.
- La plataforma MOTO cifra el contenido antes de enviárselo al usuario.
- El UE recibe el contenido cifrado y lo descifra para poder leer el contenido real.

12.4.4. Resultados obtenidos

Una vez realizadas las pruebas cabe comentar que las tres han sido exitosas en entornos aislados, es decir, sin integrar con la app MOTO. Esto es, para la realización de las pruebas se ha empleado un terminal móvil y un servidor que únicamente implementan las funciones de seguridad, es decir, que contiene los tres módulos explicados anteriormente los cuales son el objeto del análisis.

Una vez analizados los dos tipos de pruebas se puede concluir que la solución propuesta es una solución segura y eficiente ya que los resultados de simulación han proporcionado unos resultados en cuanto a retardos satisfactorios y los módulos evaluados en las pruebas en maqueta han cerciorado que la solución es segura.

Como futura línea de investigación se propone la integración del módulo de seguridad con la app MOTO completa con el fin de conocer cómo se comporta la solución de seguridad en términos de rendimiento en un entorno real.

13. Descripción de tareas

En este apartado se detalla la planificación que se ha llevado a cabo para la realización de este TFM, incluyendo las tareas y los hitos. A continuación, se detallan los paquetes de trabajo en los que se ha dividido el TFM:

- **Definición de objetivos y requisitos:** En este paquete de trabajo se han definido los objetivos y requisitos que se quieren alcanzar con este TFM. Este paquete de trabajo a su vez consta de dos tareas que son definir los objetivos y definir los requisitos.
- **Diseño de la solución de seguridad con estudio de alternativas:** En este paquete de trabajo se ha definido la solución de seguridad para la topología de red definida. Este paquete de trabajo a su vez consta de tres tareas que son el análisis de la topología de red definida, análisis del estado del arte de las soluciones disponibles y definición de la solución de seguridad.
- **Diseño y realización de pruebas mediante simulaciones:** en este paquete de trabajo se han definido y llevado a cabo las pruebas en el entorno simulado anteriormente detallado. Este paquete de trabajo consta a su vez de cuatro tareas que son identificación de parámetros a medir, definición y puesta en marcha del escenario, diseño del plan de pruebas y desarrollo de mediciones.
- **Diseño y despliegue de pruebas en entorno real:** en este paquete de trabajo se han definido y llevado a cabo las pruebas reales. Este paquete de trabajo consta a su vez de cuatro tareas que son identificación de parámetros a medir, definición y puesta en marcha del escenario, diseño del plan de pruebas y desarrollo de mediciones.
- **Análisis y valoración de resultados:** este paquete de trabajo consta de dos tareas que son analizar y valorar los resultados de las simulaciones y por otro lado analizar y valorar los resultados de las pruebas en entorno real.
- **Documentación del TFM:** En este paquete de trabajo se ha documentado debidamente el estudio que se ha realizado.
- **Gestión del desarrollo del TFM:** Este paquete de trabajo tiene la duración del trabajo completo y en él se gestionan todos los aspectos relacionados con el trabajo.

Los hitos más importantes de este TFM son el inicio del TFM (28 de septiembre de 2015), entrega de los correspondientes informes al finalizar cada paquete de trabajo (30 de septiembre de 2015, 17 de noviembre de 2015, 29 de enero de 2016, 5 de febrero de 2016, 4 de abril de 2016 y 8 de abril de 2016) y por último la finalización del TFM (3 de junio de 2016).

A continuación, se muestran tres imágenes que recogen el diagrama de Gantt (paquetes de trabajo, tareas e hitos) del TFM que se ha explicado en este apartado. La primera muestra el diagrama Gantt completo de todo el proyecto y las otras tres imágenes muestran el proyecto por paquetes de trabajo.

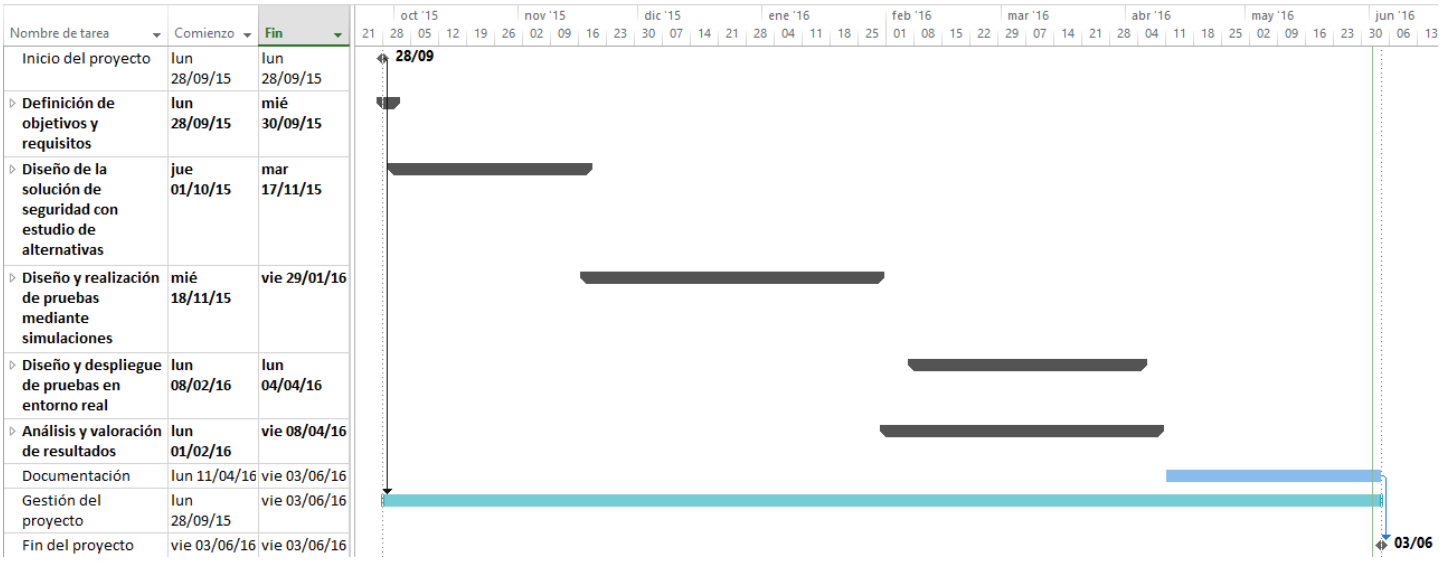


Ilustración 20: Gantt del proyecto completo.

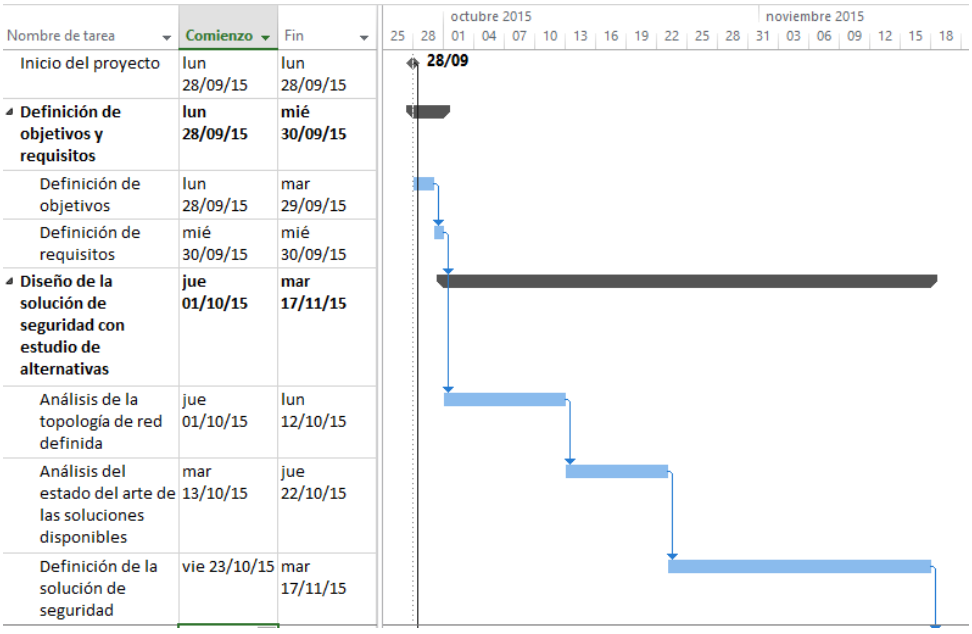
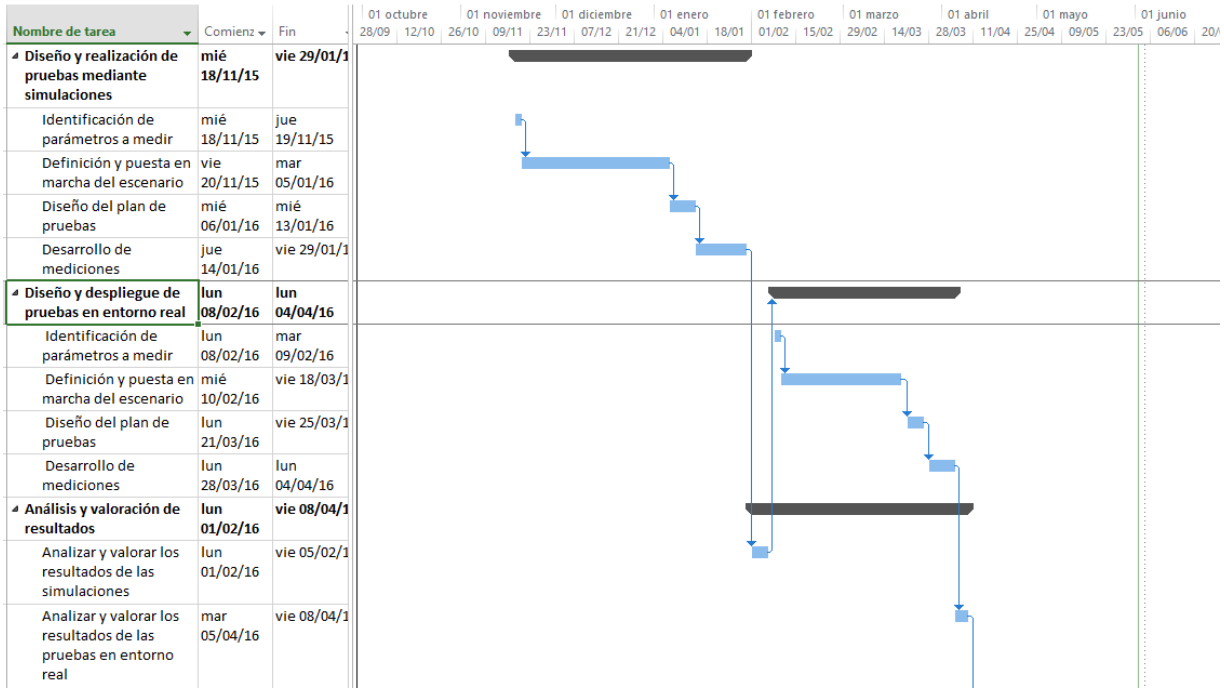


Ilustración 21: Gantt de los paquetes de trabajo "Definición de objetivos y requisitos" y "Diseño de la solución de seguridad con estudio de alternativa".



Nombre de tarea	Comienz	Fin
Diseño y realización de pruebas mediante simulaciones	**mié 18/11/15**	**vie 29/01/1**
Identificación de parámetros a medir	mié 18/11/15	jue 19/11/15
Definición y puesta en marcha del escenario	vie 20/11/15	mar 05/01/16
Diseño del plan de pruebas	mié 06/01/16	mié 13/01/16
Desarrollo de mediciones	jue 14/01/16	vie 29/01/1
Diseño y despliegue de pruebas en entorno real	**lun 08/02/16**	**lun 04/04/16**
Identificación de parámetros a medir	lun 08/02/16	mar 09/02/16
Definición y puesta en marcha del escenario	mié 10/02/16	vie 18/03/1
Diseño del plan de pruebas	lun 21/03/16	vie 25/03/1
Desarrollo de mediciones	lun 28/03/16	lun 04/04/16
Análisis y valoración de resultados	**lun 01/02/16**	**vie 08/04/1**
Analizar y valorar los resultados de las simulaciones	lun 01/02/16	vie 05/02/1
Analizar y valorar los resultados de las pruebas en entorno real	mar 05/04/16	vie 08/04/1

Ilustración 22: Gantt del paquete de trabajo "Diseño y realización de pruebas mediante simulaciones", "Diseño y despliegue de pruebas en entorno real" y "Análisis y valoración de resultados".

Este TFM tiene una duración de aproximadamente 8 meses (180 días laborables), con una carga de trabajo diaria de 4 horas lo que resulta en un total de 720 horas.

14. Costes

En este apartado se van a presentar los costes que han supuesto la realización de este estudio de forma detallada.

14.1. Horas internas

Para la realización de este TFM han sido necesarios un ingeniero superior y un ingeniero junior como recursos humanos. La tasa horaria de cada uno de ellos es:

Acrónimo	Nombre	Responsabilidad	Tasa Horaria
Is	Mariví Higuero	Ingeniera Senior	50€/h
Ij	Maitane Chaves	Ingeniera Junior	20€/h

Tabla 14: Tasa horaria de horas internas.

A continuación, se detallan las horas trabajadas por persona a lo largo del proyecto para cada paquete de trabajo:

Paquete de trabajo	Responsable	Horas	Tasa horaria	Coste
Definición de objetivos y requisitos	Ij	12 h	20€/h	240 €
Diseño de la solución de seguridad con estudio de alternativas	Ij	136 h	20€/h	2.720 €
Diseño y realización de pruebas mediante simulaciones	Ij	204 h	20€/h	4.080 €
Diseño y despliegue de pruebas en entorno real	Ij	164 h	20€/h	3.280 €
Análisis y valoración de resultados	Ij	36 h	20€/h	720 €
Documentación del TFM	Ij	160 h	20€/h	3.200 €
Gestión del desarrollo del TFM	Ij	40 h	20€/h	800 €
Supervisión	Is	125 h	50€/h	6.250 €
TOTAL				**21.290 €**

Tabla 15: Coste total de horas internas.

El coste total de horas internas asciende a 21.290 €.

14.2. Amortizaciones

En este TFM solo existen las siguientes amortizaciones que corresponden al uso del equipo con el que se ha realizado el análisis y la documentación, el terminal móvil usado para las pruebas del prototipo y el servidor empleado para implementar el servidor de seguridad MOTO.

Equipo	Valor inicial	Valor residual	Vida útil	Tiempo de utilización	Coste
Equipo con el que se ha realizado el análisis	800 €	100 €	3 años (36 meses)	8 meses	155,55 €
Terminal móvil	200 €	50 €	2 años (24 meses)	2 meses	12,50 €
Servidor	750 €	100€	3 años (36 meses)	2 meses	36,11 €
TOTAL					**204,16 €**

Tabla 16: Coste total de amortizaciones.

El coste total de amortizaciones asciende a 204,16 €.

14.3. Gastos

Además de las horas internas y las amortizaciones, han de incluirse gastos de materiales no reutilizables.

Descripción	Coste
Electricidad	60 €
Conectividad a Internet	250 €
Material de oficina	50 €
TOTAL	**360 €**

Tabla 17: Coste total de gastos.

El coste total de gastos asciende a 360 €.

14.4. Coste total del proyecto

El coste total del proyecto supone la suma de los totales de cada subapartado, es decir, horas internas, amortizaciones y gastos, ya que en este proyecto no ha sido necesario realizar ninguna subcontratación o inversión.

Descripción	Coste
Horas internas	21.290,00 €
Amortizaciones	204,16 €
Gastos	360,00 €
TOTAL	**21.854,16 €**

Tabla 18: Coste total del proyecto.

El coste total que supone la realización del TFM "Definición y análisis de una solución de seguridad en entornos D2D oportunistas multioperador" es de 21.854,16 €.

15. Conclusiones y resultados de difusión

En primer lugar es importante indicar que los objetivos que se habían planteado para este proyecto se han cubierto de forma satisfactoria, ya que se ha conseguido definir y analizar una solución de seguridad en entornos D2D oportunistas multioperador de forma adecuada y en los plazos establecidos.

Debido a que actualmente las redes oportunistas se están posicionando como una solución a los problemas de capacidad de las operadoras, se ha considerado oportuno definir y analizar una solución de seguridad de una topología de red que hace uso de estas tecnologías D2D, ya que precisamente esta forma de funcionar plantea problemas de seguridad que ponen en riesgo el éxito de este tipo de soluciones, para así, poder conocer cómo se comporta dicha solución de seguridad para una red oportunista ante diferentes cantidades de tráfico, más o menos usuarios, etc.

Una vez definida la solución se ha diseñado e implementado el plan de pruebas y se han llevado a cabo las medidas. Observando los resultados obtenidos de las medidas, concretamente el retardo, vemos que en este escenario los valores del mismo son muy buenos ya que nos encontramos con un retardo extra debido a la seguridad por debajo de los 5 segundos, lo cual es imperceptible para descargas de contenido multimedia.

Por lo tanto, se puede concluir que esta solución de seguridad cumple con los requisitos iniciales que se han planteado y que puede servir de base para futuras investigaciones en esta línea de investigación.

Por último cabe comentar que como resultado de este trabajo se han realizado dos publicaciones. La primera de ellas ya publicada es un artículo presentado en el congreso de la XXX Simposium Nacional de la Unión Científica Internacional de Radio celebrado en la Universidad de Pamplona que tiene como título “Seguridad en Entornos de Comunicaciones D2D Oportunistas Multioperador”. La segunda de ellas se trata de un libro de seguridad en redes oportunistas que aún está en desarrollo que tiene como título “*Introduction to opportunistic networks, their main features and which security challenges they pose*”.

16. Bibliografía

[1] F. Rebecchi, M. Dias de Amorim, V. Conan, «DROiD: Adapting to Individual Mobility Pays Off in Mobile Data Offloading,» Trondheim, Norway, Junio 2014.

[2] Filippo Rebecchi, Marcelo Dias De Amorim, Vania Conan, Andrea Passarella, Raffaele Bruno, «Data Offloading Techniques in Cellular Networks: A Survey,» *Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers (IEEE),* pp. 1-25, 2014.

[3] M.J. Yang, S.Y. Lim, H.J. Park y N.H. Park, «Solving the data overload: Device-to-Device bearer control aechitecture for cellular data offloading,» *IEEE Vehicular Technology Magazine,* vol. 8, nº 1, pp. 31-39, Marzo 2013.

[4] Coll-Perales, B.; Gozalvez, J.; O. Lazaro & M.Sepulcre, «Opportunistic Multi-Hop Cellular Networking for Energy-Efficient Provision of Mobile Delay Tolerant Services,» *IEEE Vehicular Technology Magazine,* 2015.

[5] B.Coll-Perales & J. Gozalvez, «Experimental Evaluation of Multihop Cellular Networks Using Mobile Relays,» *IEEE Communications Magazine,* vol. 51, nº 7, pp. 122-129, 2013.

[6] M. Consortium, «MOTO,» [En línea]. Available: http://www.fp7-moto.eu/.

[7] Aijaz, A.; Aghvami, H. & Amani, M., «A survey on mobile data offloading: technical and business perspectives.,» *IEEE Wireless Communications,* pp. 104-112, 2013.

[8] Martin, A., Smith, J. & Koethe, M., «A platform independent model and threat analysis for mobile ad hoc networks.,» de *SDR Forum Technical Conference.*, 2007.

[9] Min, Z. & Jiliu, Z., «Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks.,» de *International Symposium on Information Engineering and Electronic Commerce.*, 2009.

[10] Gerla, M., Tang, K. & Bagrodia, R., « TCP Performance in Wireless Multi-Hop Networks,» de *Proceedings of IEEE WMCSA*, 1999, pp. 41-50.

[11] B.S. Manoj, Ram Murthy, Ad hoc Wireless Networks: arquitecture and protocols, Jane Bonnell, 2004.

[12] Hongsong, Chen; Zhenzhou, Ji; Mingzeng, Hu, «Design and performance evaluation of multi-agent based dynamic lifetime security scheme for AODV routing protocol,» *Journal of Network and Computer Applications,* pp. 145-166, 2007.

[13] Hongmei, Deng; Wei, Li; Dharma, Agrawal, «Routing security in wireless ad hoc networks,» *IEEE Communications Magazine,* pp. 70-75, 2002.

[14] Solomon Abel, Vikas, «Survey of Attacks on AdhocWireless Networks,» *International Journal on Computer Science and Engineering (IJCSE),* vol. 3, nº 2, pp. 826-829, 2011.

[15] Manikandan, K.P.; Satyaprasad, R.; Rajasekhararao, R., «A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks,» *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 2, nº 3, pp. 7-12, 2011.

[16] Hu, Y.; Perrig, A.; Johnson, D. B., «Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,» *Proceedings of the ACM Workshop on Wireless Security,* pp. 30-40, 2003.

[17] Awerbuch, B.; Holmer, D.; Nita-Rotaru, C.; Rubens, H., «An On-Demand Secure Routing Protocol Resilient to Byzantine Failures,» *Proceedings of the ACM Workshop on Wireless Security,* pp. 21-30, 2002.

[18] V. S. Abel, «Survey of Attacks on Mobile Adhoc Wireless Networks,» *International Journal on Computer Science and Engineering,* vol. 3, nº 2, pp. 826-829, Feb 2011.

[19] L. Hu y D.Evans, «Using Directional Antennas to Prevent Wormhole Attacks,» *VA IJCSNS International Journal of Computer Science and Network Security,* vol. 8, nº 7, Julio 2008.

[20] W. Wang y B.Bhargava., «Visualization of wormholes in sensor networks,» *Proceedings of the 2004 ACM workshop on Wireless Security,* pp. 51-60, 2004.

[21] K. Win, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay, «Analysis of Detecting Wormhole Attack in Wireless networks,» *World Academy of Science, Engineering and Technology 48,* 2008.

[22] E. Mohammed y L. Oakland Dargin, «Routing Protocols Security in Ad Hoc Networks,» *University School of Computer Science and Engineering CSE 681 Information Security.*

[23] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman, «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.,» *Commun. ACM 21,* pp. 120-126, 1978.

[24] S. Yi, P. Naldurg, and R. Kravets , «Security-Aware Ad Hoc Routing for Wireless Networks,» *Proceedings of ACM MOBIHOC 2001,* pp. 299-302, Octubre 2001.

[25] C. E. Perkins y E. M. Royer, «Ad Hoc On-Demand Distance Vector Routing,» *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications,* pp. 90-100, Febrero 1999.

[26] Y. Hu, D. B. Johnson, y A. Perrig, «SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,» *Proceedings of IEEE WMCSA 2002,* pp. 3-13, Junio 2002.

[27] Charles E. Perkings IBM y T.J. Watson Reseach Center Hawthorne, «Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,» de *Nueva York*.

[28] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, y E. M.B. Royer, «A Secure Routing Protocol for Ad Hoc Networks,» *Proceedings of IEEE ICNP 2002,* pp. 778-87, Noviembre 2002.

[29] A. Perig, R. Canetti, D. Tygar y D. Song, «The tesla broadcast authentication protocol,» 2002.

[30] C. Boldrini, M. Conti, A. Passarella, «Exploiting users' social relations to forward data in opportunistic networks: the HiBOp solution,» *Elsevier Pervasive and Mobile Computing,* vol. 4, nº 5, pp. 633-657, Octubre 2008.

[31] Adrian Leung, Chris Mitchell, Royal Holloway, «A service discovery threat model for ad hoc networks,» de *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2006)*, Setubal, 2006.

[32] M. Consortium, «D5.2: Evaluation of offloading strategies based on simulations,» 2015.

[33] iTETRIS Consortium, «iTETRIS,» 2010. [En línea]. Available: http://www.ict-itetris.eu/simulator/introduction.htm.

[34] M. Consortium, «D5.3. Evaluation of offloading strategies based on experimentation,» 2015.