Cooperación en redes vehiculares. Estado de la cuestión y propuesta de mecanismo basado en incentivos

Trabajo de Fin de Máster

Pablo Picazo Sánchez

Universidad Carlos III de Madrid
Especialidad: Sistemas distribuidos, multimedia y seguros

Agosto 2011

Cooperación en redes vehiculares. Estado de la cuestión y propuesta de mecanismo basado en incentivos

Cooperación en redes vehiculares. Estado de la cuestión y propuesta de mecanismo basado en incentivos

Especialidad: Sistemas distribuidos, multimedia y seguros

Dirigido por el profesor

Jose María de Fuentes García-Romero de Tejada

Universidad Carlos III de Madrid
Especialidad: Sistemas distribuidos, multimedia y seguros

Agosto 2011

A mis padres.

Los ordenadores son inútiles.
Sólo pueden darte respuestas.
Pablo Picasso

Agradecimientos

Primero aprende informática y toda la teoría. Después desarrolla un estilo de programación. Entonces, olvídalo todo y hackea

George Carrette

Ante todo, volver a resaltar a mis padres por estar siempre ahí para todo.

A Lara por aguantarnos mútuamente y confiar en mí.

Agradecer a Goyi todo lo que hace por mí siempre al igual que Jesús. Espero poder devolverlo algún día.

Ana, Ángeles y José Juan porque cuando voy con ellos parece como si no me hubiera ido.

A todos mis amigos que no puedo enumerar porque todos son igual de importantes.

A Chema, mi tutor por darme la oportunidad de trabajar juntos en esto.

A Marco Antonio y Pedro Pablo Gómez por compartir libremente TEXIS y hacer esta tarea más fácil.

Resumen

Cuando te inunde una enorme alegría, no prometas nada a nadie. Cuando te domine un gran enojo, no contestes ninguna carta.

Proverbio chino

Las redes vehiculares son un tipo de redes móviles que fueron diseñadas para mejorar la seguridad en los vehículos en la carretera, mejorar la conducción o el confort al volante.

Tradicionalmente, se ha asumido la cooperación entre nodos en una red de área local porque siempre existía un nodo central que hacía las labores de coordinación del resto de componentes de la red.

Las redes vehiculares son un tipo de redes móviles distribuidas donde esta afirmación no se puede realizar ya que en este tipo de redes Ad-Hoc, todos los nodos deberían ser capaces de cooperar entre sí sin la necesidad de que exista un nodo central.

Los vehículos que participan en las redes VANET (Vehicular Ad-Hoc Networks) están llamados a tener un comportamiento egoísta ya que tratarán de explotar los recursos de la red para un beneficio propio a expensas del resto de componentes del sistema.

Para evitar este mal comportamiento, actualmente se están investigando diferentes técnicas que sean capaces de fomentar la cooperación a la vez que introducen métodos de seguridad para conservar la privacidad y la consistencia tanto de los usuarios de la red como del propio sistema.

El objetivo de este trabajo es proponer un nuevo mecanismo que contribuya a mejorar la cooperación en redes vehiculares. Previamente al diseño de dicho mecanismo, se realiza un estudio del estado de la cuestión, identificando los aspectos que son susceptibles de mejora.

Palabras Clave

VANET, incentivos, cooperación

Abstract

Man is still the most extraordinary computer of all.

John F. Kennedy

Vehicular Ad-Hoc Network is a kind of Mobile Ad- Hoc Networks and is designed to improve safety, reliability, and management.

Traditionally, cooperation between nodes in a network area are assumed because there is a central node that coordinates the rest of all. In Vehicular Ad-Hoc Networks this assumption cannot be done because in these Ad-Hoc networks all of the nodes should be able to cooperate without a central node.

Each device on vehicles is controlled by a potentially selfish participant which will try to exploit the network at expense of others vehicles.

The purpose of this work is to propose a new schema to enforce cooperation in Vehicular Ad-Hoc Networks. Previously an overview of existing and proposed systems is made identifying those aspects that can be improved.

Keywords

VANET, Cooperation enforcement, incentives, pricing

Índice

Agradecimientos ix

Resumen xi

Abstract xiii

1. Introducción 1
- 1.1. Introducción . . . 1
- 1.2. ¿Qué son las redes Ad-Hoc? . . . 1
  - 1.2.1. Propiedades de las redes Ad-Hoc . . . 2
- 1.3. ¿Qué son las redes VANET? . . . 3
  - 1.3.1. La cooperación en entornos vehiculares . . . 3
- 1.4. Motivación . . . 3
  - 1.4.1. Mecanismos para fomentar la cooperación en VANET 4
- 1.5. Objetivos . . . 5
- 1.6. Organización del documento . . . 5

2. Estado del arte 7
- 2.1. Introducción . . . 7
- 2.2. Comportamientos deshonestos en las redes vehiculares . . . 10
- 2.3. Contramedidas aplicadas a comportamientos deshonestos . . . 11
  - 2.3.1. Esquemas basados en la confianza . . . 12
  - 2.3.2. Esquemas basados en incentivos . . . 12
- 2.4. Diseminación de información . . . 13
  - 2.4.1. Detección . . . 13
  - 2.4.2. Mitigación . . . 15
- 2.5. Encaminamiento de la información . . . 16
  - 2.5.1. Prevención . . . 17
  - 2.5.2. Mitigación . . . 18
- 2.6. Conclusiones . . . 25

3. Esquema basado en incentivos para el fomento de la coope-

ración en redes VANET. **29**
3.1. Introducción 29
3.2. Análisis de propuestas anteriores 31
3.2.1. Análisis de la función de beneficio 32
3.2.2. Limitaciones del esquema 33
3.3. Modelo del sistema 34
3.3.1. Modelo de entidades 34
3.3.2. Modelo de comunicaciones 35
3.3.3. Modelo de atacantes 36
3.4. Funcionamiento y análisis del esquema 36
3.4.1. Funcionamiento general del sistema 36
3.4.2. Función de beneficios 38
3.5. Evaluación 40
3.5.1. Resistencia a ataques 40
3.5.2. Gestión de los incentivos 41
3.5.3. Evaluación experimental 42
3.5.4. Discusión 44
3.6. Conclusiones 46

4. Líneas Futuras **47**
4.1. Líneas Futuras 47

5. Conclusiones **49**
5.1. Conclusiones 49

Bibliografía **51**

Índice de figuras

1.1. Esquema de una red Ad-Hoc 2

2.1. Esquema de comunicaciones en redes vehiculares 8
2.2. Esquema de comportamientos deshonestos 10
2.3. Sistema de recuento 17
2.4. Ilustración del esquema basado en reembolsos para dos nodos y un AP 19

3.1. Recompensa VS Distancia. $D_j = 3$ 39
3.2. Recompensa VS Tiempo 40
3.3. Recompensa que obtienen los nodos con respecto de la distancia 43
3.4. Recompensa que obtienen los nodos con respecto del tiempo . 44
3.5. Recompensa que obtienen los nodos con respecto del tiempo y de la distancia 44
3.6. Recompensa que obtienen los nodos con respecto del número de reenvíos 45
3.7. Recompensa que obtienen los nodos con respecto del tiempo y de la distancia en el artículo [12] 45

Índice de Tablas

2.1. Clasificación de comportamientos deshonestos 11

3.1. Ejemplo de valores de los pesos según el tipo de mensaje . . . 38

Capítulo 1

Introducción

Si abordas una situación como asunto de vida o muerte, morirás muchas veces

Adam Smith

Resumen: En este primer capítulo presentaremos qué son las redes Ad-Hoc y las redes VANET en particular. Nos centraremos en la cooperación entre vehículos explicando por qué es un problema y la necesidad de investigar y plantear soluciones en este ámbito en concreto.

1.1. Introducción

En esta sección se introducirán los conceptos más importantes que se usarán a lo largo de este trabajo. Una explicación de las redes Ad-Hoc así como sus principales características se hacen necesarias para comprender qué son las redes vehiculares (ya que son un tipo de redes Ad-Hoc). Posteriormente nos centraremos en la cooperación en este tipo de redes y po qué suponen un problema actualmente.

1.2. ¿Qué son las redes Ad-Hoc?

Una red Ad-Hoc es un tipo de red de comunicaciones compuesta por un conjunto de nodos capaces de comunicarse a través de una interfaz, generalmente inalámbrica, de manera descentralizada, es decir, donde cada nodo está capacitado para reenviar datos al resto de componentes. La decisión de retransmitir estos datos se toma de forma dinámica en función de la conectividad de la red. De esta manera, un nodo puede comunicarse con otro que se encuentre fuera de su rango de cobertura por medio de una comunicación

multisalto, es decir, se establece un puente entre origen y destino a través de nodos intermedios y la información se reenvía de nodo en nodo desde el emisor hasta el receptor.

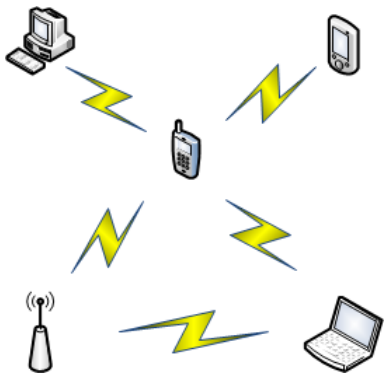

Figura 1.1: Esquema de una red Ad-Hoc

En la Fig. 1.1 se puede observar un posible esquema de red Ad-Hoc.

1.2.1. Propiedades de las redes Ad-Hoc

A continuación se detallan algunas de las principales características de las redes Ad-Hoc:

- Movilidad: Una de las características más importantes. Los nodos tienen la capacidad de ser móviles y no por ello perder la comunicación con el resto de sistema, siempre que no salgan del alcance radio de la propia red.
- Multisalto: Una red multisalto es una red donde el camino del nodo emisor al nodo receptor puede atravesar varios nodos intermedios.
- Conservación de la energía: Los nodos móviles, tienen una batería limitada y a no ser que dispongan de algún mecanismo de carga, no tienen capacidad de recarga, por tanto es muy importante conservar sus comunicaciones y sus cómputos para prolongar la autonomía de las baterías.
- Escalabilidad: En las redes distribuidas el número de nodos puede crecer hasta llegar a varios miles. Como no existe un punto de acceso concreto, la incorporación y descarte de nodos tiene que ser un proceso sencillo y transparente.
- Seguridad: Las redes inalámbricas son vulnerables a ataques, y las redes Ad-Hoc lo son especialmente. Pueden padecer tanto ataques activos como pasivos, el atacante puede emular a un nodo legítimo y capturar

paquetes de datos y control o destruir tablas de encaminamiento entre otros ataques.

1.3. ¿Qué son las redes VANET?

Las redes vehiculares (*Vehicular Ad-Hoc Networks*) son un tipo de redes Ad-Hoc formadas por dos tipos de nodos: estáticos y móviles.

Los nodos estáticos, son elementos fijos emplazados a lo largo de las carreteras llamados RSU (*Road-Side Unit*), cuya función es la de enviar, recibir y retransmitir paquetes para aumentar el rango de cobertura de la red pudiendo también ofrecer acceso a Internet.

Los nodos móviles son los vehículos equipados con un dispositivo electrónico llamado OBU (*On Board Unit*) para poder comunicarse con otros vehículos o con las RSU. Estos tipos de nodos tienen la capacidad de enviar, recibir y retransmitir mensajes entre ellos (*Vehicle-To-Vehicle*, V2V) o apoyándose de los nodos estáticos (*Vehicle-To-Infrastructure*, V2I).

1.3.1. La cooperación en entornos vehiculares

Las comunicaciones cooperativas se plantean como el próximo gran reto dentro del sector de la automoción y de los Sistemas Inteligentes de Transporte (ITS) ya que por sus características, son las comunicaciones encargadas de los servicios que demanden baja latencia y requisitos de tiempo real. Además, permitirán ampliar la cobertura y capacidad de redes inalámbricas tradicionales mediante el uso de los diferentes nodos como encaminadores de información. Es por esto que se requiere la participación de los nodos.

1.4. Motivación

En redes locales con varios elementos conectados siempre existe un nodo que hace las labores de coordinación del resto de componentes de la red. Sin embargo, en los sistemas distribuidos la cooperación entre los nodos es un problema ya que pueden existir procesos con relojes distintos, con arquitecturas distintas o características distintas. Una de las posibles soluciones a este problema de la coordinación es implementar algoritmos que elijan a un nodo que haga de coordinador del resto [7, 9].

En las redes vehiculares, al ser redes de tipo Ad-Hoc, la solución pasa por encontrar algún mecanismo que fomente la cooperación entre los componentes sin la existencia de un nodo central que ejerza de líder ya que, al contrario que las redes distribuidas estáticas, las redes vehiculares están en constante cambio y resultaría inviable ejecutar un algoritmo como los anteriores para encontrar un líder en un período de tiempo tan breve.

Así pues, la falta de cooperación y la falta de seguridad en esta cooperación en las redes vehiculares puede ser desastrosa ya que un nodo podría no reenviar un mensaje crucial para el funcionamiento de la red, como puede ser un mensaje de la llegada de una ambulancia para que los coches abran paso durante un atasco en una autovía producido por un accidente. También pudieran existir nodos que estuvieran tentados a introducir mensajes erróneos con el fin de conseguir un beneficio concreto, como enviar mensajes de accidentes inexistentes en una carretera concreta con el fin de poder viajar solo.

Es por estos motivos que se hace necesaria garantizar tanto la seguridad como una buena coordinación de los componentes de la red para que funcione correctamente y poder hacer frente a ataques como los citados anteriormente.

1.4.1. Mecanismos para fomentar la cooperación en VANET

Actualmente se emplean dos mecanismos para fomentar la cooperación en entornos vehiculares: sistemas basados en incentivos y sistemas basados en la confianza.

- Los sistemas basados en la confianza consisten en mantener las opiniones que los nodos realizan sobre otros nodos o sobre los mensajes que contienen información. Una opinión sobre un mensaje consiste en adjuntar a dicho mensaje que contiene la información (añadir más bits) correspondientes a si un nodo cree que esa información es veraz o no. En caso de que la opinión se haga sobre los nodos, entonces cada nodo debe mantener una cantidad de información correspondiente a la opinión que hagan sobre cada uno de los nodos que se vaya encontrando a lo largo de su historia para saber así, cuando reciba información de este nodo, si se puede fiar de que la información sea veraz o no [15].

  Uno de los principales problemas con los que los investigadores deben tener especial cuidado es que, en este tipo de sistemas se debe manejar una gran cantidad de información por lo que la eficiencia tiende a ser un problema ya que, en ocasiones, puede llegar a resultar inviable manejar tal cantidad de datos [19].

- Los sistemas basados en incentivos consisten en fomentar la cooperación a base de recompensar a los nodos por realizar reenvíos de los mensajes que les lleguen. Esta recompensa se realiza mediante el cálculo de algún algoritmo para poder otorgar los incentivos.

  Uno de los principales problemas con los que los investigadores deben tener especial cuidado es que, en este tipo de sistemas se tiende a fomentar el egoísmo debido a la competencia de los nodos por conseguir más recompensa que otros, por tanto la creación de una buena función

de beneficios (algoritmo para calcular las recompensas de cada nodo) ha de ser justa y no ha de fomentar el egoísmo [17, 16, 5, 4].

1.5. Objetivos

Los objetivos de este trabajo son dos:

1. Realizar un estado de la cuestión sobre la cooperación en las redes vehiculares.
2. Diseñar y evaluar un mecanismo basado en incentivos para la mejora de la cooperación en estas redes.

Para evaluar la propuesta, se van a analizar diferentes comportamientos:

- Cómo se comporta la función de beneficios propuesta. Para ello se mostrará gráficamente cuál es el rango de valores que la función puede generar, es decir, si otorga incentivos consecuentes y no recompensa a vehículos que no actúen de manera correcta.
- Gracias a las simulaciones realizadas, se podrá ver gráficamente cómo se comporta nuestro sistema de incentivos con respecto del tiempo y con respecto de la distancia.
- Así mismo, se analizará la propuesta con el modelo de atacantes descrito previamente.
- Se analizarán las propuestas en las que nos basamos, que tenían cierta falta de seguridad ante determinados comportamientos, enfrentándolas a nuestra propuesta.

1.6. Organización del documento

Este proyecto de Fin de Máster consta de cinco capítulos. En este primer capítulo se ha realiza una introducción a las redes vehiculares y al problema de la cooperación. En el capítulo dos, se muestra el estado del arte donde el lector podrá constatar en qué punto se encuentra la investigación. El tercer capítulo describe el mecanismo propuesto para fomentar la cooperación en este tipo de redes. En el cuarto capítulo se presentan unas líneas futuras mientras que el quinto y último capítulo se presentan las conclusiones de este proyecto.

Capítulo 2

Estado del arte

Los jóvenes hoy en día son unos tiranos. Contradicen a sus padres, devoran su comida, y le faltan al respeto a sus maestros.

Sócrates (470 AC-399 AC)

Resumen: Tradicionalmente, la cooperación entre nodos en un área local se ha asumido porque siempre existía un nodo central que hacía las labores de coordinación del resto de componentes de la red. En las redes vehiculares esta teoría no se puede asumir porque en este tipo de redes Ad-Hoc, todos los nodos[1] deberían de ser capaces de cooperar entre sí sin la existencia de un nodo central. Cada vehículo que participa en la red es controlado por un participante potencialmente egoísta que tratará de explotar los recursos de la red a expensas del resto de componentes del sistema. El propósito de este segundo capítulo es ofrecer al lector un estado del arte de los sistemas que existen actualmente para evitar los comportamientos maliciosos o deshonestos y fomentar la cooperación entre los vehículos.

2.1. Introducción

Hoy en día uno de los retos más importante en el mundo es mejorar la seguridad en las carreteras. En este escenario es donde tienen lugar las redes vehiculares. Las redes VANET fueron originalmente pensadas para reducir el alto número de accidentes en los coches, pero actualmente, hay una gran variedad de aplicaciones donde las redes VANET pueden ayudar, como la

[1] En este trabajo, los vehículos y los nodos son tratados de la misma manera

seguridad al volante, el bienestar del usuario o la eficiencia en la conducción entre muchas otras. Este tipo de redes Ad-Hoc son un componente importante de los Sistemas Inteligentes de Transporte (ITS).

Las redes vehiculares son un tipo de redes móviles (MANET) sin embargo tienen una diferencia importante respecto a éstas que resulta más complicado para implementarlas: la movilidad de sus componentes. Debido a esta gran rapidez de sus nodos, máximas de 120 Km/h en España, hacen que sea obligatorio tener una topología de red dinámica que se adapte a los cambios rápidamente o que sea capaz de renovarse cada vez que un nodo entre o salga de la red.

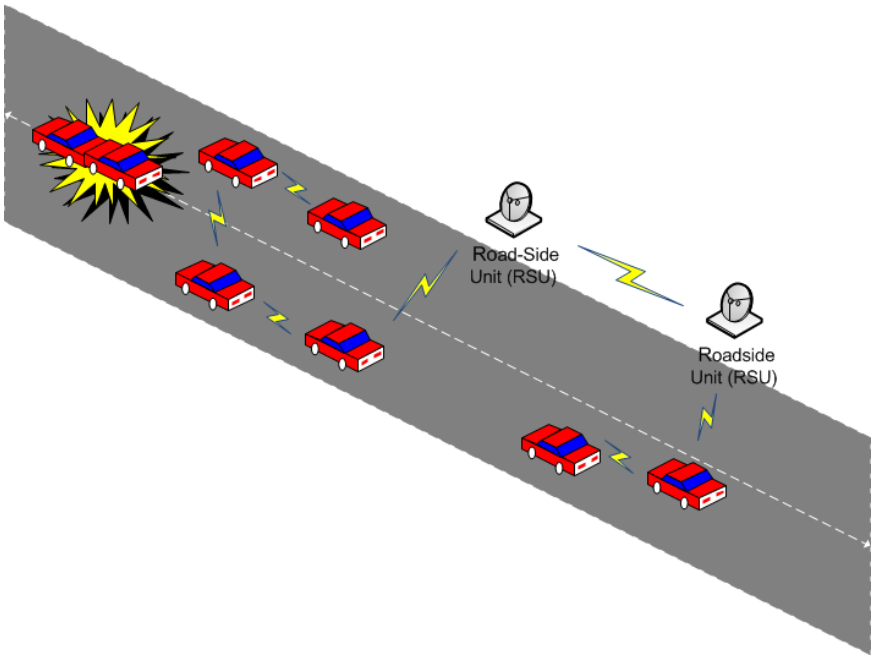

Figura 2.1: Esquema de comunicaciones en redes vehiculares

Otro de las dificultades que este tipo de redes poseen, son sus fuertes restricciones temporales, ya que resulta imprescindible que los mensajes que contienen información relevante sobre las condiciones del tráfico, lleguen a tantos vehículos como sea posible en el menor período de tiempo posible. Este intercambio de información se debe efectuar, generalmente, mediante el intercambio de mensajes entre los vehículos que componen la red en un momento determinado, entre los postes de comunicación que existen en las carreteras (RSU) o entre la combinación de todos estos.

Los vehículos, para poder establecer estas comunicaciones, están equipados con un dispositivo de comunicación inalámbrica de corto alcance llamado OBU. En la Fig. 2.1 se puede observar un esquema de comunicaciones en redes vehiculares.

Las redes VANET poseen múltiples cualidades que hacen que este tipo de redes sean el futuro en nuestros vehículos, sin embargo poseen todavía muchas cuestiones aun sin resolver. Uno de estos problemas es que cada coche pertenece a su dueño, como no puede ser de otra manera, y por tanto posee control total sobre todos los elementos que lo componen. Como consecuencia de esto, un usuario podría modificar los elementos que son necesarios para el buen funcionamiento de la red, esto es, puede alterar el software del coche o modificar los elementos de seguridad que forman parte de la red VANET que incluye cada coche para obtener un beneficio propio o para adaptarse mejor a sus propios propósitos [3]. Una posible solución a este problema sería asumir que la OBU es confiable, esto es, que resulta inaccesible ante cualquier tipo de ataques y emite mensajes correctos sin ningún tipo de información errónea, sin embargo esta asunción no se puede realizar ya que, por definición los canales de comunicaciones no son confiables y están sujetos a ataques.

Tradicionalmente, la cooperación entre los nodos en un área de red local se ha abordado a lo largo de la literatura proponiendo distintas aproximaciones para que uno de estos nodos actuara como coordinador del resto de los componentes de la red [7, 9]. Sin embargo, estas aproximaciones en las redes vehiculares no se pueden adoptar ya que, por definición, las redes VANET han de ser descentralizadas, con fuertes restricciones temporales y dinámicas y por tanto los componentes que forman las VANET han de poder coordinarse sin un nodo que dirija todas las acciones.

Actualmente existe un gran número de artículos de investigación que se centran en contrarrestar los comportamientos deshonestos de los nodos de la red VANET para fomentar la cooperación, sin embargo no se han recopilado y realizado un análisis y clasificación de todos ellos en un sólo artículo. Es por ello que un estado del arte de todas estas soluciones realizadas se hace necesario. El propósito de este segundo capítulo enmarcado dentro de este trabajo de Fin de Máster, es identificar los malos comportamientos en la cooperación de los vehículos así como las contramedidas adoptadas analizando para ello las contribuciones más representativas en este campo.

El resto de este capítulo está organizado de la siguiente manera: en la sección 2 los diferentes comportamientos deshonestos son explicados y clasificados. En la sección 3 se explican las contramedidas adoptadas y los mecanismos empleados para ello. La sección 4 trata la diseminación de datos erróneos, cómo hacer frente a ellos y mitigar sus efectos. En la sección 5 se muestran las anomalías que se pueden dar en el enrutamiento de la información y cómo poder reducir en la medida de lo posible la probabilidad de que ocurran estos problemas. Por último, este primer capítulo concluye con unas conclusiones.

2.2. Comportamientos deshonestos en las redes vehiculares

El envío de paquetes que contengan información falsa acerca de accidentes, retenciones, mensajes con información importante procedente de vehículos oficiales como las ambulancias, policías o bomberos, o con información sobre las condiciones meteorológicas que no se correspondan con la realidad pueden llegar a incrementar más aun los problemas en las carreteras pudiendo generar incluso, accidentes. Este problema de información errónea o falsa no siempre tiene que originarse por nodos maliciosos o nodos cuyo fin es atacar la red de comunicaciones en las VANET. Existen nodos que sencillamente pueden generar estos problemas sin intención debido a los propios sensores mal calibrados o que obtengan datos erróneos del entorno [18].

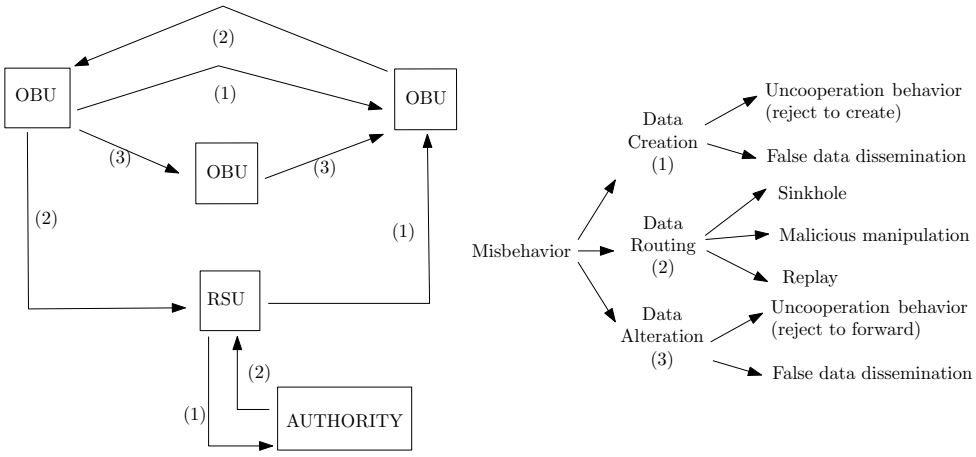

Figura 2.2: Esquema de comportamientos deshonestos

Por tanto, cada vehículo se puede decir que está controlado por participantes potencialmente egoístas [3] que tratarán de explotar la red a expensas de otros vehículos para obtener un mayor beneficio de esta. El egoísmo en estos entornos puede ser el origen de numerosas anomalías como pueden ser los *sinkhole attacks*, el problema de un mal enrutamiento de los paquetes, la alteración de los mensajes, o comportamientos que no fomenten la cooperación. Los *sinkhole attacks*, son un tipo de ataque a una red de comunicaciones donde los nodos tratan de atraer la mayoría de los mensajes de un área concreta para concentrar toda la información en un punto, generando así un "pozo de información". Los malos enrutamientos de la información se pueden originar de muchas maneras, no enviando paquetes, enviándoselos a un grupo selecto de vehículos excluyendo a otros, etc. Los vehículos también pueden introducir datos falsos en la red o modificar a su antojo la información que ya está circulando por ella o sencillamente dejar de cooperar en el reenvío de la información para no gastar sus propios recursos, porque

estén ocupados con otras operaciones o simplemente porque no quieran. En la Fig. 2.2 se puede observar una clasificación de los problemas asociados a los malos comportamientos que se pueden dar en un entorno de cooperación de las redes VANET.

Sin embargo, este egoísmo no siempre tiene que ser signo de un mal comportamiento de manera consciente, es decir, un nodo a veces se comporta de manera egoísta tan sólo para ahorrar energía, impidiendo por ejemplo la comunicación entre los distintos elementos que componen la red VANET, o para incrementar el ancho de banda para poder beneficiar así las comunicaciones entre otros nodos de la red o porque la red se encuentre sobrecargada. Aunque estos comportamientos no suelen ser lo habitual ya que los nodos tienden a consumir al máximo posible sus recursos para obtener así un mayor beneficio [27].

2.3. Contramedidas aplicadas a comportamientos deshonestos

Existen tres principales contramedidas actualmente para estos malos comportamientos de los vehículos en las redes VANET: la detección, la prevención y la mitigación. La detección consiste en averiguar cuándo se produce un comportamiento deshonesto. La prevención consiste en ser capaces de adelantarse estos malos comportamientos. Mientras que la mitigación es conseguir disminuir la probabilidad de que los comportamientos deshonestos puedan ocurrir.

	Detección	Prevención	Mitigación
Diseminación de datos	[1, 6, 18, 32]		[3, 32]
Anomalías en el enrutamiento		[16, 19]	[28, 21, 5, 12, 27, 14, 17]

Tabla 2.1: Clasificación de comportamientos deshonestos

Tanto para la detección (además de los *plausibility checks*), como para la prevención como para la mitigación se emplean mecanismos como los esquemas basados en incentivos (explicados en la subsección 2.3.1) o los sistemas basados en la confianza (explicados en la subsección 2.3.2).

En la tabla 2.1 se puede observar una clasificación de los diferentes artículos analizados organizados según problemas que abordan y las contramedidas adoptadas por los diferentes autores. La diseminación de datos es una categoría formada por la creación y la alteración de los datos ya que el problema

que tratan ambos y cómo lo abordan es muy similar.

2.3.1. Esquemas basados en la confianza

Una posible definición de confianza puede ser: *"La confianza (o de manera simétrica, la desconfianza) es un nivel particular de la probabilidad subjetiva con el cual un agente evalúa a otro agente o a un grupo de agentes que realizan una acción concreta, antes de que pueda controlar dicha acción (o de forma independiente o de su capacidad para ser capaz de controlarla) y en un contexto en el cual afecta a su propia acción* [8].

Así pues, y basándonos en la anterior definición, los sistemas basados en confianza son un tipo de sistemas de reputación en los cuales, cada miembro obtiene o pierde reputación basado en acciones sucedidas en el pasado (también llamadas generalmente creencias). En este tipo de sistemas la reputación de la información proviene de terceras partes, sin embargo, si se tiene unas creencias actuales sobre la información que se está tratando en ese momento, suele despreciarse el conocimiento pasado. Por tanto, puede ser que tan sólo con una creencia u opinión de un solo nodo pueda influir en la decisión de autorizar y evaluar, o no, la veracidad de la información [22].

Dentro de los sistemas basados en confianza existe un concepto denominado "*data-centric trust estabilsment*"para detectar los mensajes falsos, es decir un mecanismo basado en la confianza donde la confianza de los datos son analizados inicialmente de manera individual, posteriormente se combina la confianza de los datos analizados previamente para que, finalmente la confianza total de un mensaje sea inferida a partir de las confianzas anteriores usando sistemas de decisión para obtener la veracidad del mensaje final [26].

En las redes VANET, los sistemas basados en confianza tienen como finalidad ayudar a otros nodos a decidir cuándo comenzar un intercambio de información con otros nodos que son, hasta ese momento, desconocidos para ellos. En el artículo [15] se puede leer más acerca de este tipo de sistemas de reputación entrando más en detalle sobre su uso e implementación así como sus pros y sus contras.

2.3.2. Esquemas basados en incentivos

Los sistemas basados en incentivos son un tipo de sistemas de cooperación donde sus componentes son recompensados por realizar unas determinadas acciones. El núcleo de este tipo de sistemas es una función matemática que se encarga de otorgar las recompensas [17]. En entornos vehiculares donde se emplean los sistemas basados en incentivos, los nodos reciben recompensas cada vez que un nodo reenvía un paquete a otro u otros nodos. En este tipo de esquemas, el propósito principal es estimular a los nodos para que se involucren en la cooperación y reenvío de mensajes de la red VANET

estimulándolos por ello con un premio justo, es decir, un premio para ellos acorde al nivel de participación que hayan tenido.

Estos tipos de sistemas basados en incentivos poseen la capacidad de reconocer si un nodo está cooperando en el reenvío de paquetes o no y por tanto se puede penalizar, mediante algún elemento que haga de autoridad, a los nodos que no cooperen o tengan comportamientos deshonestos con el resto de los nodos o de la red en sí, como puede ser la no cooperación o el apagado del dispositivo de comunicación entre otros.

2.4. Diseminación de información

Existe una gran cantidad de información sobre acontecimientos en las carreteras o sobre las condiciones meteorológicas que pueden ser detectadas por los sensores que tienen incorporados los vehículos. Pero este tipo de información no siempre es veraz como dijimos anteriormente. Los sensores que usan los coches pueden estar calibrados de diferente manera, dependiendo por tanto de las propias marcas de los coches o sencillamente ir perdiendo fiabilidad con el tiempo o pueden ser, en el peor de los casos alterados por los propios usuarios.

Durante la fase de reenvío de paquetes existen otros problemas añadidos a los anteriores, y es que los usuarios deshonestos pueden alterar la información introduciendo así pues datos erróneos.

Es por esto, que para combatir los malos comportamientos a la hora de crear o diseminar datos se clasifican en las contramedidas explicadas anteriormente[2]: detección y mitigación.

2.4.1. Detección

En las redes vehiculares existen dos maneras para detectar los datos falsos: detectar los paquetes falsos o detectar a los nodos deshonestos.

En la detección de paquetes falsos, los sistemas basados en la confianza son usados en los propios mensajes, es decir, cada nodo adjunta su opinión en el mensaje indicando la veracidad del mismo [6, 18, 32].

En la detección de los nodos deshonestos, los sistemas basados en la confianza se emplean en la opinión de los propios vehículos, es decir, cada nodo posee una opinión del resto de vehículos [1].

Para detectar los mensajes que contienen información falsa, en [6] se propone una solución donde los nodos pueden generar tres tipos de opiniones distintas: *reputación directa*, *reputación indirecta* y una tercera llamada *reputación generada*. La reputación directa es la que se emite directamente sobre la veracidad de la información. La reputación indirecta es aquella que

[2]En la diseminación de información no existen artículos que adopten medidas de prevención. De ahí que no aparezca en una sección como la detección o la mitigación

se obtiene a partir de los nodos cuya reputación de la información es conocida, esto es, la reputación que los nodos han realizado sobre la veracidad de la información. Finalmente, la reputación generada se calcula a partir de la reputación directa, de la indirecta si el nodo es conocido, de las opiniones del resto o de una combinación de todas ellas.

También para detectar la información falsa, en [32], crean un mecanismo basado en un esquema de confianza denominado *Dynamic Trust-Token* (DTT). DTT utiliza tanto criptografía simétrica como criptografía asimétrica para proteger la integridad de la información. Su propósito principal es fomentar la cooperación en las redes VANET durante la diseminación de los paquetes en la red. Esta solución aseguran que tienen un beneficio, y es que no depende de la reputación que ha ido ganando o perdiendo cada nodo, DTT tiene la capacidad de establecer la reputación de cada nodo en tiempo de ejecución no teniendo que almacenar y mantener así la reputación histórica de los nodos. Con este mecanismo, los paquetes que contienen información incorrecta aseguran que no se propaga en ningún caso a través de la red.

Cada nodo en DTT juega tres roles diferentes según su estado: predecesor, intermediario y sucesor. Los nodos que se encuentran en la capa de los predecesores forman la primera parte de reenvío de la información y para generar los *trust-token*. Los nodos que están en la capa de intermediarios tienen la función de reenviar la información. Finalmente, los nodos que están en la capa de sucesores, son los responsables de aceptar o no los paquetes recibidos. El mecanismo DTT asegura que si alguna de las capas que forman el mecanismo fallara o alterara los mensajes, su mal comportamiento sería detectado por las capas del nivel superior y reportado a la capa de nivel inferior para que estos paquetes dejaran de ser propagados más.

En [18] al igual que los artículos anteriores, tratan de detectar los mensajes con información falsa empleando un sistema basado en confianza, sin embargo asumen que los sensores que poseen los coches son los que generan los eventos que mandan a un dispositivo llamado aplicación de tráfico seguro que es el que decide si enviar estos mensajes o no. Este dispositivo posee una tabla de eventos donde se almacenan todos los mensajes que recibe de los sensores del coche así como los mensajes que generan los vehículos de desconfianza sobre otros nodos. Todos los eventos que se almacenan en el dispositivo de tráfico seguro se inician a 0, es decir, poseen un contador que aumenta cada vez que se recibe el mismo evento generando así una tabla con valores que dan lugar a la reputación.

Este dispositivo posee dos parámetros que se han de configurar correctamente para un buen funcionamiento: el *umbral de reputación* y el *umbral de confidencia*. Para verificar la reputación de un evento, se calcula el número de veces que ha generado un evento (el contador) y si supera el umbral de la reputación establecido, entonces se asegura que ese evento existe y se está produciendo, tomándolo por tanto como real. En caso contrario, el evento no

existirá más. Si el número de ocurrencias de un evento supera el umbral de confidencia de un evento entonces significa que hay más vehículos que han detectado ese evento de tráfico y por tanto, la probabilidad de que sea real es mayor. Si un evento finalmente supera ambos umbrales se considera fiable y se envía al resto de los nodos.

Los tres anteriores artículos se basaban en detectar los mensajes que eran falsos. En [1] aun empleando un modelo basado en la confianza al igual que los anteriores, su principal característica es que se centra en las experiencias directas de cada nodo y no en un sistema de confianza donde las creencias de todos los nodos se usan para generar una opinión sobre un elemento en concreto, bien sea un nodo o un mensaje. Este sistema evalúa continuamente el rendimiento y la reputación de otros vehículos e incluyen una especie de resumen para aumentar el rendimiento del sistema propuesto y adaptar mejor los posibles cambios en los paquetes. Este esquema está basado principalmente en la asunción de que lo vehículos no siguen movimientos aleatorios sino que ellos, generalmente, hacen viajes regulares y pasan frecuentemente por unos sitios determinados.

En este esquema, exclusivamente las últimas recomendaciones que se hayan realizado sobre ese vehículo son las que se almacenarán. La recomendación de una fuente se basa en la creencia o en la no creencia de la opinión que el nodo que reenvía el mensaje genera. El nodo receptor del mensaje usa esta y otras opiniones recibidas de otros nodos para construir así su propia opinión sobre el mensaje que le ha llegado.

Finalmente, la confianza es el resultado de la fusión de tres componente principales: la *reputación*, la *predicción de los nodos* y la *competencia de los nodos*. Como hemos dicho ya anteriormente, la reputación es la opinión de otros nodos. La predicción de los nodos es cómo de bueno es un vehículo emitiendo juicios sobre la información que ha recibido de otros nodos. Por último, la competencia de los coches es la precisión de las opiniones vertidas, esto es, cuanto más preciso sean, más competentes son.

2.4.2. Mitigación

Para conseguir hacer disminuir la probabilidad de que los malos comportamientos ocurran en la creación o reenvío de los datos, se proponen dos sistemas principales: el uso de un dispositivo de seguridad en [3] o el uso de una técnica de seguridad llamada *watchdog* en [32].

En [3], se propuso una solución para redes MANET que hacía uso de un dispositivo hardware de seguridad en cada nodo de la red. Este dispositivo se asumía que era completamente seguro frente ataques de los adversarios, teniendo la capacidad de almacenar, manejar y distribuir las claves públicas y mantener a salvo en todo momento las claves privadas.

Bajo estas suposiciones, los autores propusieron un protocolo que re-

quería que los nodos que enviaran mensajes, éstos previamente tenían que pasar por este módulo de seguridad que mantenía un contador el cual decrecía cada vez que un paquete era generado para enviar por el nodo y se incrementaba cada vez que el nodo participaba en el reenvío de los mensajes que le llegaban de otros nodos de la red. El valor de este contador siempre ha de ser positivo, de esta manera, si un nodo quiere enviar un paquete previamente ha de haber cooperado en el reenvío de otros para que su contador sea mayor que uno. Este contador está siempre protegido frente a cualquier manipulación de los usuarios mediante el dispositivo de seguridad descrito anteriormente.

En el artículo [32] que analizamos previamente su propuesta basada en un mecanismo denominado DTT donde se detectaban los paquetes que contenían información falsa. A continuación veremos cómo su propuesta aseguran, bajo unas determinadas suposiciones, que también son capaces de disminuir la probabilidad de que ocurran estos malos comportamientos.

Los autores asumen que el primer nodo que genera un mensaje es confiable y que, como dijimos anteriormente emplean un mecanismo mitigación como es el *watchdog*. Este mecanismo, bien por software o bien por hardware, es un método por el cual se asegura que una acción se efectúa correctamente, esto es, una aplicación o una acción tarda un determinado tiempo en ejecutarse (ciclos de reloj) de manera correcta. Si pasado este tiempo, no se ha efectuado la acción que debería, entonces el *watchdog* se activa, ya que interpreta que algo va mal, y hace que todo comience de nuevo. Esta técnica requiere por tanto de un proceso o dispositivo seguro que controle todas las comunicaciones para así velar por la seguridad de ellas.

2.5. Encaminamiento de la información

Fomentar la cooperación en la redes VANET supone implementar un mecanismo por el cual los nodos de la red les compense retransmitir los mensajes que les llegan para que la información llegue a cuantos vehículos sea posible en un tiempo determinado. Sin embargo, se pueden dar problemas al igual que sucedía en la diseminación de la información, esto es, si los vehículos no tienen un incentivo por el cual retransmitir los mensajes les suponga un beneficio, podrían los nodos decidir no reenviar los mensajes para así crear un agujero de información y que los demás vehículos no obtengan esos mensajes, o que los nodos decidan no reenviar los mensajes para obtener así una mayor recompensa o justo lo contrario, evitar que el resto de nodos reciban premios por reenviar unos mensajes.

Es por esto, que para combatir los malos comportamientos a la hora de encaminar la información se clasifican en las contramedidas explicadas anteriormente[3]: prevención y mitigación.

[3]En el encaminamiento de información no existen artículos que adopten medidas de

2.5.1. Prevención

Para prevenir los malos comportamientos por parte de los nodos se emplean mecanismos basados en incentivos donde el uso de recibos o comprobantes así como el uso de diferentes elementos de la criptografía como los certificados o PKI [16, 19] parece prevenir en gran medida los malos comportamientos por parte de los nodos en el encaminamiento de la información.

En [16] los autores crean un nuevo esquema basado en incentivos llamado SSD. SSD es un método basado en recibos que emplea criptografía de clave pública para dotar de seguridad a los incentivos para la cooperación entre los nodos. Cuando un vehículo i reenvía un paquete a otro vehículo j, entonces j debería de dar a i un recibo o un comprobante de ese paquete que indica que no lo había recibido anteriormente y que por tanto el reenvío es válido. Todos los nodos que reenvían información pueden entonces reclamar un premio o un incentivo basado en el número de comprobantes que han cosechado a lo largo de la cooperación de ese mensaje.

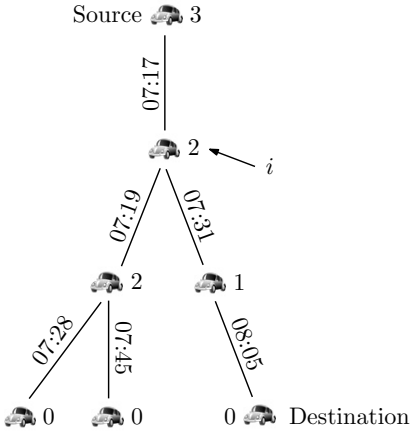

Figura 2.3: Sistema de recuento

Este método es muy flexible ya que cada nodo puede reclamar los recibos antes incluso de que los paquetes lleguen a su destino final. Sin embargo este método por esta misma cualidad de reclamar su premio antes de que llegue al final, tiene un problema de sobrecarga ya que el nodo fuente no puede saber en ningún caso la cantidad de beneficio que se va a originar durante el reenvío de un paquete concreto ya que no se puede saber a priori por cuántos nodos va a pasar la información [16].

Como se muestra en la Fig. 2.3, el nodo i obtiene 2 recibos, suponiendo que cada recibo posee un crédito virtual de 1, entonces ese nodo i obtendría un premio valorado en 2 unidades.

Otro sistema basado en incentivos para redes inalámbricas es el que los

detección. De ahí que no aparezca en una sección como la prevención o la mitigación

autores presentan en [19] basado también en el concepto de recibos. En este modelo los autores asumen que existen tres elementos bien diferenciados: centros de contabilidad (AC), nodos móviles y estaciones base. Los AC almacenan y administran la cuenta de crédito que los nodos móviles poseen, además de generar certificados de clave pública y su correspondiente clave privada para poder identificar y evitar problemas de seguridad para con los nodos. Los nodos móviles son los usuarios de la red, los que se encargan de enviar y de reenviar los mensajes. Las estaciones base, son puntos por los que se comunican los nodos, esto es puntos de acceso, puestos de Wi-Fi o puestos de comunicaciones 3G entre otros.

En este sistema existen tres principales retos o propósitos para mejorar la cooperación entre los nodos: 1) Desarrollar un modelo de pago para poder mejorar la implementación práctica de los micro-pagos a los nodos. 2) Proponer un nuevo sistema de incentivos para estimular así a los nodos a la cooperación. 3) Reducir el número de recibos o comprobantes para evitar por tanto la saturación en la red de comunicaciones.

En la fase de pagos, el certificado de un nodo le permite participar en el reenvío y por tanto puede recibir los comprobantes que acreditan que ha participado en la cooperación de los mensajes y que, por tanto, puede reclamar un premio o beneficio por ello. El AC es el que se encarga de verificar que ese comprobante es válido y en ese caso recompensará al nodo por haber cooperado.

El sistema de incentivos consiste principalmente en tres fases: 1) Comunicación. 2) Reclamar los incentivos. 3) La fase de pagos. Durante la fase de comunicación, los nodos que participan en la red reenvían los paquetes que le llegan de un nodo a otro para beneficio propio, pues obtendrán un premio, y para beneficio de la red. Durante la fase de reclamo de los incentivos, los nodos que han participado en la cooperación envían mediante las estaciones base, sus comprobantes como que han reenviado paquetes y que esperan una recompensa por ello. Por último, la fase de pagos, los AC que reciben esos comprobantes, verifican que son ciertos y que están correctamente y entonces aumentan el saldo de los nodos.

Finalmente, para reducir el número de comprobantes, los autores emplean el Hash de las firmas en vez de las propias firmas, reduciendo de manera significativa el tráfico de red.

2.5.2. Mitigación

Para conseguir disminuir la probabilidad de que se produzcan los malos comportamientos en el encaminamiento de la información, generalmente se emplean mecanismosbasados en incentivos con ciertas variantes como puede ser la inclusión de mecanismos aleatorios como la lotería en [21, 17], usando conceptos de teoría de juegos como en [5, 27], introduciendo funciones con-

vexas para el cálculo de los beneficios en [17, 12] o empleando unos contadores para controlar los mensajes que los nodos pueden o no mandar que son incrementados si se coopera y disminuidos si se envía información nueva como en [27, 14]. Aunque no siempre el uso de mecanismos basados en incentivos son los únicos empleados para disminuir la probabilidad de los comportamientos deshonestos en el encaminamiento de la información, en [28] se emplea un mecanismo de un esquema basado en reputación combinado con la tecnología de agentes móviles.

En [27], los autores extendieron el trabajo de [3] y diseñaron ese mismo esquema llevado redes inalámbricas Ad-Hoc. En este trabajo, el principal propósito es asegurarse que los puntos de acceso (AP) y los usuarios salen beneficiados de la colaboración. Así pues, los AP se encargan de quitar el crédito de los nodos que enviaban paquetes (creaban) y los nodos que se reenvían los paquetes (cooperan) se encargan de otorgarse crédito.

Inicialmente, los AP declaran un precio o un coste por un servicio que es elegido por él mismo. El concepto de servicio no es otro que la relación de la cantidad de datos que son transmitidos por el nodo. El nodo por tanto, si es capaz de asumir el coste de generar ese nuevo mensaje para introducirlo en la red, entonces se descuenta de su contador, en caso contrario no se puede generar el mensaje.

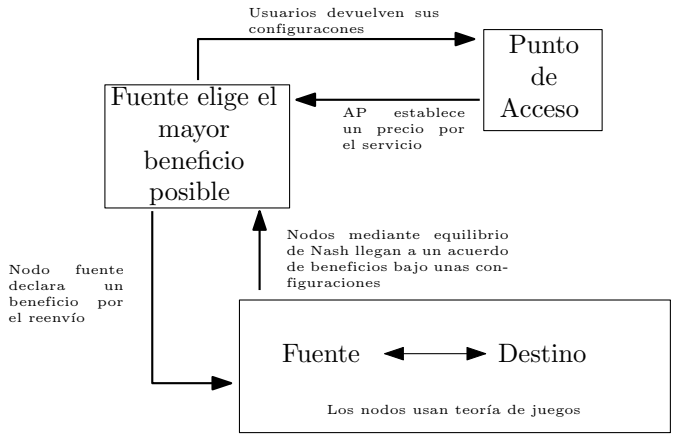

Figura 2.4: Ilustración del esquema basado en reembolsos para dos nodos y un AP

En la Fig. 2.4 se puede ver el esquema de este sistema basado en incentivos donde los usuarios son los responsables de elegir sus transmisiones y decidir si reenviar los mensajes o no. Entre los usuarios, existe un equilibrio de Nash ya que los nodos pueden elegir de manera unilateral si participar en el reenvío o no, sin embargo en caso de no hacerlo entonces ambos nodos perderían un beneficio común que alcanzarían en caso de que existiera una cooperación entre ellos.

Las principales ventajas del esquema propuesto por los autores tal y como indican ellos mismos, es que supone un esquema completamente distribuido y escalable, sin embargo el impacto o la gran ventaja de su trabajo es que es en redes de altas densidades o en redes donde los usuarios están organizados en grupos, donde el equilibrio de Nash tiene lugar, ya que tan sólo existe este equilibrio de teoría de juegos en redes geométricas donde los nodos están relativamente cerca unos de otros.

Otro artículo que extendió y mejoró los concepto introducidos por los autores en [3] y en [27] fue el artículo [14] que introdujeron una técnica para fomentar la cooperación para las redes VANET denominada 3CE, para un sistema que habían propuesto unos años antes en [13] llamado CLAS-S. Este sistema no mantenía los caminos que realizaban los mensajes en los encaminamientos de los paquetes para minimizar así el riesgo de que uno de esos caminos estuviera obsoleto o roto temporalmente. En CLAS-S las calles eran divididas en celdas donde en cada una de estas celdas operaba un router virtual que hacía las labores de encaminar los paquetes a través de enlaces virtuales. Por tanto cada vez que un paquete llegaba a cada uno de estos router virtuales, se creaba un nuevo enlace virtual a la siguiente celda hasta llegar a su destino

En CLAS-S es importante tener en cuenta que antes de que un nodo comience la transmisión de un paquete, la localización del destinatario de ese mensaje es requerida. Existen tres contadores que son actualizados gracias a un procedimiento que los autores denominan "procedimiento de actualización". Estos contadores son mantenidos por un dispositivo parecido al dispositivo de seguridad de [3] llamado módulo 3C.

Cuando un nodo comienza el procedimiento de descubrimiento de la localización (LD), consistente en un paquete llamado paquete LD, el módulo 3C del nodo inicial añade el paquete LD a su cabecera, como si se tratase de un modelo por capas como el modelo OSI. La cabecera del módulo 3C contiene entonces el valor de los tres contadores del nodo fuente. Basado en esta cabecera, los nodos vecinos del nodo inicial deciden entonces si reenviar el mensaje o no.

Si un nodo sospecha que el nodo fuente es deshonesto, entonces el nodo invoca un procedimiento de detección de malos comportamientos para verificar la cabecera del módulo 3C que contiene el paquete LD. Si este procedimiento identifica al nodo emisor como deshonesto, entonces los nodos vecinos penalizarán a este nodo no enviando los paquetes LD que éste genere.

Sin embargo, para que los nodos que han sido penalizados y sean tratados como nodos deshonestos, los módulos 3C de estos nodos podrán participar en el reenvío de los datos de la red para que, de esta manera, los nodos no se aíslen y no puedan formar parte nunca más de la red VANET. En este caso solo mediante la colaboración, podrán volver a ser capaces de generar

mensajes por sí mismos y que el resto de los nodos puedan reenviar estos mensajes, dándoles así la posibilidad de que vuelvan a actuar correctamente y por tanto participar en la red en plenitud de capacidades.

En el artículo [21] se muestra una solución basada en otorgar premios consecuentes según el mensaje reenviado e introducir un mecanismo de lotería. En este artículo, el premio que un nodo puede recibir se basa en la clasificación de los mensajes que se pueden enviar por la red VANET obteniendo mayor o menor beneficio en función del tipo de mensaje. Existen tres tipos principales: mensajes de seguridad de la carretera, mensajes de Internet y mensajes de advertencia. Los mensajes que contienen información sobre la seguridad en las carreteras proveen información prioritaria sobre acontecimientos graves como accidentes o retenciones en las carreteras. Los mensajes de Internet aportan, valga la redundancia, mensajes para poder acceder a Internet. Los mensajes de advertencia proveen información comercial sobre tiendas o estaciones de servicio que se puedan encontrar en un radio cercano a la posición del vehículo en un determinado instante.

En este artículo se agrupan además los vehículos que están conduciendo en el mismo sentido a velocidades parecidas. El grupo ha de tener un número mínimo de componentes y uno de los componentes ha de actuar como líder para controlar al resto. En este grupo, todos los nodos tienen una conexión directa con un nodo que hace las labores de coordinación y comparten además una clave secreta con él. Esta idea de los grupos permite reducir el número de paquetes que circulan por la red ya que es el líder de cada grupo el que toma las decisiones sobre un determinado paquete, es decir, si lo reenvía o no.

Bajo estas condiciones, en el caso de ser un paquete que contiene información sobre el tráfico, si un nodo decide no reenviarlo, entonces el grupo entero será castigado y penalizado por las autoridades que pueden observar este mal comportamiento y por tanto pagar un precio por este comportamiento deshonesto.

Los paquetes de Internet, en el esquema propuesto emplean seudónimos en la autenticación para firmar los mensajes para que así, la autoridad sepa en todo momento los nodos cooperativos y pueda por tanto premiarles o castigarles. Se hace esta distinción con respecto al resto de paquetes, porque son éstos los que a priori, la red VANET no tiene control sobre ellos y por tanto podría no identificar quién coopera en el reenvío de este tipo de mensajes.

En los paquetes con información comercial, cada pago o recompensa por reenviar este tipo de mensajes puede ser visto como una lotería. Una vez que los nodos reciben este tipo de paquetes, tanto el pagador (el comercio que distribuye el mensaje) como el ganador pueden determinar si es un boleto premiado o no. Este esquema permite a los proveedores determinar de antemano la cantidad de beneficio ofertado ya que de otra manera podrían existir problemas graves de sobrecarga.

Otra propuesta donde se emplea un componente de lotería es en [17]. En este artículo, los autores fueron de los primeros en emplear una función convexa para calcular el total de beneficio que un nodo puede obtener. Este sistema basado en incentivos para las redes VANET se llama FRAME y contiene dos componentes principales: una cantidad ponderada de beneficio y un componente aleatorio (lotería, como ellos lo denominan). Para calcular la cantidad ponderada se emplea la función convexa que se puede observar en la ecuación 2.1. El factor lotería se encarga de premiar de manera aleatoria a un número concreto de vehículos (los que les toque la lotería) que participan en la red VANET.

$$C_i = \alpha \cdot \Delta T_i + (1 - \alpha) \cdot K_i \tag{2.1}$$

En esta función convexa, la cantidad de contribución C_i para un nodo intermedio i que realiza las labores de reenvío de los paquetes, se calcula teniendo en cuenta dos parámetros: el tiempo que este nodo emplea para reenviar el mensaje a otro nodo ΔT_i y el número de reenvíos K_i que realiza este nodo a otros vehículos. La variable α es la que realiza el factor de balanceo y hace que esta función sea convexa entre estos dos parámetros.

El sistema FRAME está basado en [16] y como dijimos anteriormente, ese artículo posee un problema de sobrecarga, sin embargo los autores en FRAME consiguen solucionar ese problema estableciendo una cantidad total de premio que luego se repartirán los nodos de manera proporcional según los parámetros establecidos para calcular su beneficio.

La razón principal por lo que los autores introducen un componente aleatorio o de lotería es porque, cuando el árbol (compuesto por los nodos que reenvían los paquetes) crece a un determinado tamaño, entonces los nodos que son potencialmente aptos para reenviar los paquetes y no están dentro de ese árbol es muy probable que nunca puedan entrar en la dinámica para poder efectuar el reenvío de los paquetes de otros nodos. El motivo de esto es porque los nodos que ya están dentro del árbol de reenvíos, han acumulado una cantidad de contribuciones que hace muy complicado al resto de nodos participar en la cooperación ya que tan sólo ganarían una cantidad de premio muy pequeño, insuficiente comparado con el esfuerzo realizado por reenviar un mensaje. Es por ello que el componente de la lotería podría otorgar un beneficio a los nodos por cooperar y así verse recompensado su esfuerzo por haber participado en el reenvío de los paquetes a pesar de que, a priori, no le compensara.

Este sistema además, posee un componente extra: los vehículos podrían interactuar con una infraestructura adicional llamada autoridad de administración de reenvíos, esto es, un componente que se encarga de otorgar las firmas y los permisos necesarios para reenviar los paquetes. Esta autoridad es una tercera parte confiable que realiza las labores de juez y administrador del reembolso por la cooperación.

Sin embargo, tal y como indican en [12], en FRAME, los nodos egoístas pueden preferir mantener los paquetes en vez de reenviarlos para así obtener una mayor recompensa. Esto sucede cuando un nodo intermedio reenvía un paquete a un nodo que no es el nodo final, ya que es en ese momento cuando la recompensa se ve dividida en la parte proporcional a su colaboración entre ambos nodos. En este mismo artículo ([12]) los autores presentan este problema y proponen una nueva función convexa (fórmula 2.5) donde se tienen en cuenta tres parámetros: el tiempo que un nodo retiene un mensaje, el número de reenvíos y la distancia a la cual la información del mensaje deja de tener valor.

El factor del tiempo viene dado por la fórmula de Stokes (ver ecuación 2.2) la cual tiene como característica su comportamiento asintótico. Esta función está pensada para que, un nodo i almacene un paquete el mínimo tiempo posible t_{ij}, esto es, cuanto menos tiempo retenga un mensaje, más beneficio obtendrá. La fórmula también tiene en cuenta que un mensaje se considera interesante dentro de un tiempo concreto de tiempo T_j establecido por el nodo inicial.

$$\alpha_1 T_j(1 - e^{t_{ij}}) \tag{2.2}$$

El número de reenvíos viene dado por la fórmula 2.3, donde se premia que un nodo realice cuantos más envíos de un mensaje mejor. Posee, como se puede ver un comportamiento lineal creciente.

$$\alpha_2 f_{ij} \tag{2.3}$$

La distancia viene representada por la fórmula 2.4. La idea es que la información se considera interesante dentro de un radio concreto D_j, ya que no tendría sentido mandar un mensaje de un accidente en una carretera de Madrid a unos coches que circulan por Barcelona. Bajo este supuesto, la fórmula 2.4 otorga una mayor recompensa cuando el mensaje está dentro de una distancia concreta establecida por el nodo emisor, siendo d_{ij} la distancia a la que se encuentra el nodo i en un determinado instante.

$$\alpha_3(\text{-}D_j(1\text{-}e^{-d_{ij}})+D_j) \tag{2.4}$$

La fórmula final que los autores propusieron se deriva todas las anteriores y forman una nueva (ecuación 2.5) donde sus componentes son los descritos anteriormente y, además se introducen unos factores $\alpha_1, \alpha_2, \alpha_3$, donde $\sum \alpha_i = 1$. Factores que son establecidos por el nodo inicial para atribuir más o menos importancia a cada uno de los componentes (tiempo, distancia, número de reenvíos).

$$C_{ij} = \alpha_1 T_j(1 - e^{-t_{ij}}) + \alpha_2 f_{ij} + \alpha_3(-D_j(1 - e^{-d_{ij}}) + D_j) \tag{2.5}$$

Un enfoque basado en teoría de juegos es propuesto en [5] donde los autores se apoyan también de un sistema basado en incentivos para las redes VANET. Este artículo está basado principalmente en [17], sin embargo en [5] consideran que los incentivos deberían ser para todos los nodos, incluyendo los nodos emisores, para garantizar así una cooperación bajo su propio análisis teórico.

En teoría de juegos, se necesitan al menos dos jugadores o dos grupos de los mismos, por lo que los autores realizan la correspondencia directa con los vehículos de la red VANET. Cuando los jugadores deciden cooperar, entonces se le denomina coalición. El principal propósito de este artículo es asegurar que, sea cual sea el escenario, un mensaje que necesita ser reenviado debe involucrar a los nodos y por ello han de ser recompensados por formar una coalición.

Para realizar el esquema de manera mucho más eficiente, una aproximación ultra-ligera es propuesta y hace que sean los propios nodos los que decidan sobre un paquete, es decir si les compensa reenviarlo o no debido a la recompensa que pueden llegar a obtener.

Todos los vehículos que componen la red poseen un dispositivo en el propio coche que maneja el crédito virtual, al igual que en [16], que emplea certificados para cada vehículo y cada vez que un nodo reenvía mensajes obtiene un comprobante. Cuando los coches están próximos a las infraestructuras de comunicación (RSUs, APs . . .) entonces ellos se conectan al centro de crédito virtual (VCC) para intercambiar los datos y poder reclamar los beneficios que han obtenido por cooperar en el reenvío de los mensajes. Este esquema además posee la ventaja de que los coches no tienen que estar conectándose continuamente al VCC sino que lo pueden hacer eventualmente, teniendo la seguridad de que podrán recibir los premios y no caducarán.

Finalmente y rompiendo la tendencia, un sistema de reputación empleando agentes móviles es propuesto en [28]. Un agente móvil es una entidad software con características como la autonomía, la habilidad social (capacidad para comunicarse con el resto de agentes), capacidad de aprendizaje o su capacidad de adaptarse al medio en el que se encuentre entre muchas otras. Sin embargo, la característica que más importancia tiene este tipo de software es la capacidad de migrar de un ordenador o un dispositivo a otro y ser capaz de continuar con su ejecución en el mismo punto en el que se encontraba previamente [30]. Este artículo está basado en un protocolo de encaminamiento donde existe un mecanismo de monitorización como en [32]. Este mecanismo ayuda a encontrar el valor de la reputación que poseen los vecinos de un nodo en concreto. Los autores además diferencian dos partes principales en su esquema: la búsqueda de la mejor ruta y el reenvío de los mensajes.

En esta primera parte del protocolo, la de la búsqueda de la mejor ruta, cuando un nodo quiere mandar un nuevo mensaje a otro, un agente

móvil se encarga de buscar el mejor camino a través de los nodos que mejor reputación tengan, realizando una lista por donde el mensaje pasará posteriormente, asegurándose a priori que van a reenviar el mensaje. Si el agente móvil reconociera el nodo, como el nodo final al que le ha de llegar el mensaje, entonces es cuando comenzaría la segunda parte del protocolo.

En la segunda fase del protocolo, la del reenvío de los paquetes, debido a que la ruta ya ha sido encontrada previamente por el agente móvil, éste ha de regresar al nodo inicial para indicarle cuál es la mejor ruta para que el paquete llegue a su destino. Durante este viaje de vuelta, es cuando el agente anotará de manera definitiva la reputación de los nodos en su lista.

2.6. Conclusiones

En este capítulo se ha realizado un estado del arte sobre la cooperación en entornos vehiculares. Se han analizado y clasificado una gran variedad de artículos según los problemas que tratan (diseminación de datos o encaminamiento de datos) y las contramedidas que se adoptan para hacer frente a esos problemas (detección, prevención y mitigación).

Se puede observar la tendencia que siguen los artículos dentro de la diseminación de datos es optar por emplear un mecanismo basado en un esquema de reputación.

Los sistemas basados en reputación son un método clásico para mejorar la calidad de información o para evitar que se diseminen paquetes erróneos o con contenidos falsos en un área de red. Sin embargo, tal y como citan en [19] y en [4], este método tiene cinco problemas graves que hacen que esta práctica sea inviable para este tipo de redes Ad-Hoc:

1. Para monitorizar la transmisión de sus vecinos, un nodo de red generalmente trabaja en modo promiscuo pero eso en las redes VANET no es eficiente y hay que evitar ese comportamiento en la medida de los posible [19].

2. Los sistemas basados en reputación no alcanza la justicia, esto es, si un nodo contribuye a reenviar muchos paquetes, su esfuerzo no se ve recompensado de manera proporcional a su esfuerzo con respecto a otro que haya reenviado tan solo un paquete. Además, los nodos que son penalizados cuando no cooperan no se tiene en cuenta si ellos previamente han reenviado todos los mensajes o que en un momento dado, un nodo esté ocupado y no pueda reenviar un mensaje aislado [19].

3. Estos sistemas sufren de una detección de nodos egoístas mediocre o incluso, a veces, nula. Además las acusaciones falsas de nodos deshonestos hacia otro nodos honestos son difíciles de diferenciar [19].

4. Los sistemas de reputación no pueden ser considerados una posibilidad para estas redes porque los nodos egoístas pueden formar coaliciones con otros nodos para así mejorar su reputación y poder seguir actuando de manera deshonesta [19].

5. En las redes VANET, por definición, cada vehículo posee una gran movilidad lo cual implica que mantener un histórico de las reputaciones de los coches que se van encontrando a lo largo de la vida de un vehículo es inviable ya que en un corto período de tiempo un vehículo puede relacionarse con una gran cantidad de ellos [4].

Además, en [22] los autores añadieron algunas cuestiones más a las citadas aquí, acerca de los sistemas de reputación mostrando algunas medidas para solucionarlos.

Dentro del problema del encaminamiento de la información, la mayoría de artículos optan por emplear mecanimos de sistemas basados en incentivos tanto para la detección, como para la prevención como para la mitigiación. Los sistemas basados en incentivos son una solución clásica para mejorar los problemas de encaminamiento y fomentar la cooperación en redes VANET entre otros motivos porque son capaces de detectar y penalizar los comportamientos deshonestos y egoístas. También poseen la capacidad de recuperar a los nodos que han sido penalizados por no cooperar, dándoles la oportunidad de volver a entrar en la red y poder ser recompensados por un comportamiento correcto en vez de dejarles aislados.

Sin embargo, este tipo de mecanismo basado en incentivos posee cuestiones abiertas que supone que aún los investigadores tengan que emplear más tiempo en desarrollar nuevos algoritmos para mejorar estos sistemas. Alguna de las características que hay que tener en cuenta a la hora de implementar un nuevo sistema de este tipo son:

1. Hay que tener algún sistema de seguridad como la criptografía de clave pública empleada en [16, 17, 5], o el uso de seudónimos en [10, 21], o tener un dispositivo de seguridad hardware en cada nodo como hacen en [10, 3]. etc ...

2. El método de reenvío para motivar a los usuarios a cooperar es el núcleo de cualquier sistema basado en incentivos [17].

3. Hay que crear mecanismos para evitar la posibilidad de que existan nodos egoístas o deshonestos en los vehículos, o que existan nodos que exageren sus contribuciones para obtener así una mayor recompensa que la que realmente deberían de obtener [4].

4. Este tipo de mecanismo es muy propenso a crear problemas de sobrecarga a la hora de obtener la recompensa, por lo tanto hay que hacer un protocolo que sea capaz de evitar este problema [4].

En este segundo capítulo del trabajo de Fin de Máster se ha realizado una recopilación de los artículos más representativos en el campo de la cooperación en entornos vehiculares. El propósito principal ha sido analizar y clasificar el gran número de artículos de investigación que se centran en contrarrestar el comportamiento deshonesto de los nodos de la red VANET para fomentar la cooperación entre ellos.

Capítulo 3

Esquema basado en incentivos para el fomento de la cooperación en redes VANET.

La mejor estructura no garantizará los resultados ni el rendimiento. Pero la estructura equivocada es una garantía de fracaso.

Peter Drucker

Resumen: Las redes vehiculares son un tipo de redes móviles diseñadas para mejorar la seguridad, el manejo y la fiabilidad al volante de los automóviles. Tradicionalmente se ha asumido la cooperación entre los nodos en un entorno distribuido porque siempre existe un nodo central encargado de coordinar al resto de componentes de la red. En las redes vehiculares esta asunción no se puede realizar porque cada componente puede actuar de manera deshonesta y decidir no tomar parte en la cooperación de reenvío de mensajes para obtener un beneficio propio. En este capítulo se introduce una nueva propuesta basada en cómo motivar o incentivar a los nodos para fomentar la cooperación en el reenvío de paquetes en este tipo de redes Ad-Hoc.

3.1. Introducción

Hoy en día uno de los retos más importante a nivel global es mejorar la seguridad en las carreteras. Es, en este escenario, donde las redes vehiculares entran en escena. Las redes VANET se originaron principalmente para evitar

el gran número de accidentes en los coches, pero actualmente la potencia de este tipo de redes ha hecho que el número de aplicaciones crezca significativamente: aplicaciones para mejorar la seguridad de los usuarios, el confort, la eficiencia en la conducción y aplicaciones comerciales entre otras muchas.

Las redes VANET son un subtipo de las redes móviles MANET pero con ciertas características que las hacen más difíciles de implementar, siendo la gran velocidad de cambio su mayor problema. Debida a esta gran movilidad (velocidades máximas de 120Km/h en España) de sus nodos móviles hacen que esta red posea una topología totalmente dinámica y sujeta a cambios continuos ya que la red se tiene que modificar o adaptar cada vez que un coche entre o salga de la red de un área concreta.

La comunicación se efectúa siempre mediante intercambio de mensajes entre los nodos de la red, ya sea entre vehículos, o entre postes existentes a lo largo de las carreteras (RSU) o entre la combinación de estos elementos. La comunicación entre los vehículos se establece gracias a la incorporación de un dispositivo de comunicación *wireless* corto alcance llamado OBU.

La comunicación en las redes VANET está basada en envíos de mensajes con información de la carretera entre los componentes de la red. Cada componente puede generar o reenviar los mensajes en beneficio común de la red. Pero existe un problema, y es que se asume que cada nodo va a colaborar y va a actuar en beneficio de la red, pero no siempre es así ya que pueden existir nodos que en vez de colaborar en el reenvío de los mensajes, deciden despreciarlos o no encaminarlos para un beneficio propio.

Para evitar comportamientos como los citados, en las redes VANET se decide estimular a los nodos para que se involucren en la tarea de reenvío de mensajes y de cooperación. Existen principalmente dos tipos de esquemas o de métodos para incentivar la cooperación entre nodos: los sistemas basados en confianza y los sistemas basados en incentivos [19, 27].

Los sistemas basados en la confianza son un tipo de sistemas de reputación donde sus miembros ganan o pierden una reputación basada en comportamientos anteriores (también llamado creencias u opiniones). Se puede obtener más información sobre sistemas basados en confianza en [6, 14, 1].

Sin embargo, en este artículo nos centraremos únicamente en los sistemas basados en incentivos. Se pueden encontrar muchos artículos donde el esquema que se emplea son los incentivos como se puede ver en [12, 19, 14, 16, 17]. En estos sistemas basados en incentivos, un nodo recibe un premio o un incentivo cada vez que este nodo realiza acciones en beneficio de la red, en nuestro caso, reenviar mensajes a otros nodos. En estos esquemas, el principal propósito es estimular a los nodos intermedios a contribuir en el reenvío de mensajes incentivándoles a ello mediante un premio o una recompensa, el cual es el núcleo de un esquema basado en incentivos [17], acorde a su nivel de contribución.

Algunas de las propuestas que emplean este tipo de esquemas tienen

la capacidad de reconocer si un nodo está actuando como debería, es decir, reenviando los mensajes que le llegan o si está obrando de manera deshonesta y por tanto el sistema puede penalizarle por ello.

Actualmente fomentar la cooperación entre nodos supone un reto para los investigadores. Existe una gran cantidad de artículos sobre cómo fomentar la cooperación entre nodos empleando sistemas basados en incentivos pero aún sigue siendo una cuestión sin solución. Artículos como [16] y [17] poseen problemas reconocidos de sobrecarga en la función de beneficios, es decir, en el cálculo del premio para cada nodo en [16] o problemas más importantes como el egoísmo en [17] debido a que un nodo prefiere no reenviar un paquete a un nodo porque así su premio es mayor ya que no tiene que compartirlo con un número de nodos que crece rápidamente con cada mensaje reenviado.

En el artículo [12] los autores identificaron estos problemas y propusieron una nueva función de beneficios para evitar los problemas mencionados anteriormente, sin embargo con esta nueva propuesta los autores no dan solución a tres problemas esenciales entre otros que detallaremos en las siguientes secciones: no existe una tercera parte confiable que administre los incentivos de manera segura; dos nodos se pueden reenviar los mensajes entre ellos y luego obtener un beneficio por ello; no se puede comprobar si un nodo dice la verdad a la hora de calcular sus incentivos.

En este capítulo presentamos una nueva función de beneficio que calcule los incentivos para cada nodo y para fomentar la cooperación entre ellos evitando que los nodos egoístas obtengan beneficio alguno y solucionando los problemas que [12] tienen. Evaluaremos nuestros resultados mediante los datos obtenidos de la simulación.

El resto del capítulo está organizado de la siguiente manera: en la sección 2 realizamos un estudio de los artículos en los cuales nos basamos. En la sección 3 introducimos el modelo de nuestro sistema bajo el cual nuestro supuesto tiene lugar. La sección 4 supone el núcleo de nuestra propuesta. Los resultados de la simulación se muestran en la sección 5 y acabamos finalmente en la sección 6 con las conclusiones.

3.2. Análisis de propuestas anteriores

Debido a que nuestro trabajo está basado principalmente en [12] en esta sección vamos a discutir las propuestas que se adoptaron en este artículo y mostraremos los problemas o limitaciones que hemos encontrado.

Hay que destacar que, inicialmente [12] está basado en el artículo [17] donde los autores fueron los primeros en tener en cuenta que la función de beneficio se puede calcular con una función lineal convexa con un factor de balanceo (donde la variable α supone el factor de balanceo de la función convexa), con parámetros como el número de reenvíos, representado por f_i y otro parámetro que representa el tiempo que un paquete es almacenado

por un nodo, representado por t_i. En este artículo, cada uno de los nodos computa su propia contribución C_i mediante la fórmula 3.1.

$$C_i = \alpha t_i + (1 - \alpha) f_i \tag{3.1}$$

Pero esta solución posee un problema de sobrecarga debido a que el nodo inicial no puede adivinar en un principio el total de reembolso o beneficio que los nodos van a obtener debido a que no se puede predecir el número de nodos que van a formar parte en el reenvío de ese mensaje. Así pues, Hernández et al. en su artículo [12] crearon una posible solución a este problema manteniendo constante el número total de beneficio y calculando el beneficio asociado a cada nodo intermedio mediante R_i una sencilla fórmula (ver fórmula 3.2) después de que el paquete llegara a su destino.

$$R_i = \frac{R \cdot C_i}{C} \qquad donde \quad C = \sum_i C_i \tag{3.2}$$

Sin embargo, los autores crearon finalmente una nueva función de beneficios (ver fórmula 3.3) donde se tuvieran en cuenta tres parámetros: la distancia, el tiempo y el número de reenvíos. Una función convexa con los parámetros descritos a continuación:

- Factor de balanceo de la función representado por α_i: donde $\sum \alpha_i = 1$.
- Tiempo máximo de vida del mensaje representado por T_j.
- Período t_{ij} en el cual un paquete j es almacenado por el nodo i.
- Número de reenvíos f_{ij} del paquete j por el nodo i antes del tiempo máximo de vida T_j.
- Distancia d_{ij} entre el nodo inicial y los nodos finales cuando el paquete j reenviado por el nodo i.
- Máxima distancia D_j donde la información del mensaje j se considera interesante por los receptores.

$$C_{ij} = \alpha_1 T_j (1 - e^{-t_{ij}}) + \alpha_2 f_{ij} + \alpha_3 (-D_j (1 - e^{-d_{ij}}) + D_j) \tag{3.3}$$

3.2.1. Análisis de la función de beneficio

Los parámetros T_j y D_j son establecidos por el nodo inicial así como la importancia que le quiere dar a cada factor de la fórmula asignando los valores de los α_i sabiendo que $\sum \alpha_i = 1$. Por tanto veamos cómo se comportan cada uno de los componentes de la fórmula descrita anteriormente de manera individual, es decir, asignando valores canónicos al conjunto de los α_i .

- $\alpha_1 = 1$, $\alpha_2 = 0$,$\alpha_3 = 0 : \lim_{x\to\infty} \alpha_1(T_j(1 - e^{-x})) = T_j$. En este caso un nodo obtendrá un beneficio de este factor dependiendo únicamente del factor del tiempo, donde el beneficio máximo que podrá obtener será como máximo T_j, asignado por el nodo inicial.

- $\alpha_1 = 0$, $\alpha_2 = 1$,$\alpha_3 = 0 : \lim_{x\to\infty} \alpha_2 x = \infty$. En este caso un nodo obtendrá de este factor un beneficio indeterminado cuyo límite es infinito pero en un tiempo máximo T_j, asignado por el nodo inicial. Es decir, el beneficio será tanto como la capacidad de un nodo para reenviar mensajes en un tiempo T_j.

- $\alpha_1 = 0$, $\alpha_2 = 0$,$\alpha_3 = 1 : \lim_{x\to\infty} \alpha_3(-D_j(1 - e^{-x}) + D_j) = 0$. En este caso, un nodo dejará de obtener beneficio de este factor cuando llegue a la distancia máxima D_j fijada por el nodo inicial.

3.2.2. Limitaciones del esquema

En este esquema basado en incentivos, cada nodo es recompensando en función de su nivel de participación en el proceso de reenvío de los mensajes de la red. Sin embargo existen ciertas cuestiones abiertas, a las cuales el artículo no da respuesta, que analizaremos a continuación.

3.2.2.1. Generación y manejo de los incentivos

Los autores no mencionan cuándo se otorgan los premios. Se supone, puesto que en la función de beneficios se incluye un parámetro temporal y otro donde se tiene en cuenta el número total de reenvíos realizados, que los incentivos se otorgan pasado un tiempo concreto el cual no se estipula en el artículo. aun así, podríamos suponer que el tiempo correspondería con el valor de T_j establecido por el nodo inicial.

Bajo este supuesto, podría darse el caso en el que el coche inicial A vaya en un sentido y otro nodo B en el sentido opuesto y pasado el tiempo T_j ambos nodos no estén bajo el mismo radio de conexión. En esta situación, el nodo B parece que no recibiría su premio ya que no está en el radio de comunicación del nodo A, habiendo llevado a cabo una tarea y un consumo (cómputo, de red, etc.) que no tiene asociado ningún beneficio para el nodo B.

En caso de no suponer que el reparto de incentivos se hace pasado un tiempo T_j, sino que se realiza de manera instantánea, no parece tener sentido alguno la inclusión de los parámetros del tiempo y del número de reenvíos en un tiempo máximo T_j en la fórmula del cálculo de beneficios ya que el nodo obtendría una recompensa por cada reenvío de los mensajes, que serían tratados por tanto de manera individual.

3.2.2.2. Reclamo de incentivos y sobrecarga de la red

No existe ningún mecanismo para saber si lo que dice un nodo a la hora de calcular su recompensa es o no cierto. Para saber si se está diciendo la verdad sobre una determinada acción, en este caso el premio obtenido por cada nodo, deberían de existir al menos dos opiniones sobre un hecho, o que alguna de las partes sea confiable [23]. Por tanto parece poco probable averiguar la fiabilidad de un nodo cuando calcula su recompensa a través de la función de beneficios en el escenario que han supuesto los autores.

En el artículo los autores no tienen en cuenta que se puede dar el caso en el que un mensaje esté continuamente mandándose entre una serie de nodos concretos. En el modelo del sistema aseguran que un nodo recibe una sola vez el mensaje, sin embargo a la hora de calcular la recompensa mediante la función de beneficios hemos visto que se tiene en cuenta el número de reenvíos realizados en un tiempo máximo T_j. No hace distinción entre quiénes, ni si lo han recibido ya anteriormente. Por tanto, se pueden formar coaliciones entre dos nodos cualesquiera mandándose el mismo mensaje rápidamente con el fin de obtener una recompensa muy alta.

Existe también una posibilidad de que el nodo inicial A le mande un mensaje a un nodo B y éste a su vez permanezca reenviando ese mismo mensaje al nodo A de manera continuada. Transcurrido un tiempo T_j, el nodo B va a reclamar una recompensa por su cooperación en el reenvío de ese mensaje, debido a que no se tiene en cuenta en ningún momento a quién se lo manda sino cuántas veces se manda un mensaje en el menor tiempo posible y en un radio determinado.

3.3. Modelo del sistema

El modelo de nuestro sistema está dividido en 3 categorías principales: modelo de entidades, modelo de atacantes y modelo de comunicaciones. A continuación se detallarán cada una de ellas.

3.3.1. Modelo de entidades

Nuestro modelo del sistema está basado en la idea que los autores proponen en [19]. El modelo gira, principalmente, en torno a dos elementos: bancos y nodos móviles.

Los bancos juegan el papel de terceras partes confiables para poder llevar a cabo una transacción de pagos entre las entidades de la red, ya que sin él no sería posible tal y como se explica en [23]. Estos bancos poseen la capacidad de emitir certificados digitales [25] como si se trataran de autoridades de certificación (CA), que son unos certificados que los vehículos emplean para probar la identidad frente a otros componentes que forman parte de la red.

Estos certificados generalmente están generados con una PKI (criptografía de clave pública) y su correspondiente clave privada.

Dentro de los nodos móviles hacemos dos clasificaciones de acuerdo a su comportamiento: nodos honestos y nodos deshonestos. Los nodos honestos son aquellos que actúan de manera correcta, es decir que cumplen con el protocolo de comunicaciones correspondiente y se comportan como es debido. Los nodos deshonestos son exactamente lo contrario a los honestos, son aquellos nodos que no se comportan como se espera según dicta el protocolo.

Los vehículos, a su vez tendrán un dispositivo de seguridad (HSM, del inglés Hardware Security Module). Este dispositivo posee la capacidad de generar claves criptográficas, almacenarlas, protegerlas de manera totalmente segura y distribuirlas en un momento determinado. Si este módulo fuera foco de ataques físicos para poder obtener las claves privadas que almacena, entonces la protección física de la unidad posee un mecanismo por el cual borraría toda la información susceptible de ser extraída de manera ilegítima. En resumen, el módulo HSM es la base de la seguridad y la confianza, ya que sin él las claves privadas podrían verse comprometidas [24].

En nuestro esquema, al igual que en la vida real pueden existir ambos tipos de nodos, asumimos que pueden existir también en nuestro esquema.

3.3.2. Modelo de comunicaciones

Los vehículos poseen una OBU para conectar los nodos móviles a los bancos nuestro modelo contempla la posibilidad de hacerlo mediante cualquier tecnología de comunicación *wireless* como Wi-Fi, 3G, o mediante los puntos de acceso colocados a través de la carretera (RSU). Son gracias a estas tecnologías de comunicación, a través de las cuales los nodos se conectarán con los CA o con los bancos para realizar operaciones como renovación de certificados, cobros, cambiar crédito obtenido gracias a la cooperación por dinero real o descuentos en establecimientos comerciales como en [16].

El reenvío de los mensajes a los nodos les supone un coste (computacional, de recursos, etc. . .) como es lógico, por tanto un nodo siempre valorará si le compensa o no reenviar un mensaje, teniendo en cuenta que el nodo puede calcular en todo momento el beneficio que obtendrá por cooperar. Es por ello, que el beneficio que obtenga un nodo siempre ha de ser mayor que el coste que le suponga reenviarlo, ya que, de lo contrario no cooperará.

En nuestro modelo, los mensajes que se reenvían en la red VANET están clasificados según la importancia de la información que posean. En la literatura existen numerosos artículos en los que asignan diferentes prioridades a los mensajes para actuar de una u otra manera según la relevancia de los mismos [29, 2, 20].

3.3.3. Modelo de atacantes

Dentro de los nodos deshonestos, bajo nuestro entorno de colaboración, podemos hacer dos clasificaciones: los nodos egoístas y los nodos maliciosos. El egoísmo en un entorno de incentivos como el nuestro es un comportamiento por el cual los nodos tratan de maximizar su recompensa a costa, por ejemplo, de minimizar su comunicación con el entorno y su consumo. Los nodos maliciosos por el contrario, son aquellos vehículos que realizan ataques de manera activa o pasiva a la red, como denegación de Servicio (DoS), suplantación o escuchas no autorizadas del canal de comunicación entre otros, sin ningún beneficio aparente. En este trabajo nos centraremos en los nodos egoístas pues son los que interfieren directamente en el problema de la cooperación.

Uno de los ataques típicos en este tipo de redes son los *sybil attacks*. Este tipo de ataques, como los autores indican en [11] son ataques que se pueden producir siempre que no exista una lógica centralizada como es el caso de las redes VANET. Sin embargo indican que una forma de evitar estos ataques es emplear técnicas criptográficas de clave pública y unas entidades confiables que emitan certificados seguros. En nuestro caso, ambas soluciones están adoptadas, por tanto este tipo de ataques están prevenidos en nuestro modelo gracias al uso de dispositivos HSM que posee cada coche y al uso de certificados digitales.

Existen numerosos ataques realizados por nodos irracionales, es decir nodos que atacan a la red sin esperar nada a cambio, tan solo por el placer de romper la seguridad de la red sin embargo este tipo de ataques se alejan del propósito de este artículo. Nuestro trabajo se centra en combatir a otro tipo de nodos que realizan ataques con algún propósito concreto, es decir con ataques de nodos racionales.

Los nodos racionales son aquellos que tratan de obtener algún beneficio a través de ataques activos o pasivos. Los principales problemas que pueden acarrear los nodos maliciosos racionales en el ámbito de la cooperación son, por ejemplo, suplantar identidades para conseguir más recompensas o intentar obtener más beneficio mediante un cálculo distinto de la función de beneficios entre otros. A lo largo de la propuesta se irán dando solución a estos problemas o ataques citados anteriormente.

3.4. Funcionamiento y análisis del esquema

3.4.1. Funcionamiento general del sistema

En nuestro modelo, como en [19], existen tres fases bien definidas: registro, transferencias y pagos. Para explicar de manera más sencilla el funcionamiento de nuestro sistema, vamos a apoyarnos en un ejemplo donde a un nodo A le llega un mensaje que a su vez quiere reenviárselo a un nodo B.

Para que un nodo pueda participar, y por tanto obtener un beneficio de la red, lo primero que deberá hacer es registrarse en la VANET para poder empezar a reenviar mensajes y obtener un beneficio por ello. En este momento, el banco genera un certificado temporal que el nodo tiene que renovar cada cierto tiempo. Sólo con este certificado expedido por una tercera parte confiable el nodo ya puede participar en la red, solucionando así el problema de suplantación de identidades ya que cada nodo está identificado frente a las autoridades y a los propios nodos por estos certificados. Queda claro que si a un nodo le llegara un mensaje de un nodo que no posee un certificado expedido por la CA, rechazará el mensaje automáticamente.

A continuación los nodos generan mensajes y los reenvían entre ellos, siendo ésta la fase de transferencia. El nodo A, que reenvía el mensaje a B, calcula el beneficio que obtiene a través de la función de beneficios y lo almacena para enviárselo posteriormente al banco. Este cálculo no tendría validez para el banco a no ser que el nodo B se comunique con el banco y le diga que A le ha hecho llegar este mensaje bajo unas condiciones concretas. Estas acciones se pueden realizar cuando los nodos renueven su certificado como muy tarde.

Es en este momento cuando el banco valida la transferencia (verificando que el cálculo de A es correcto bajo las condiciones descritas) y por tanto el nodo A estaría dispuesto a recibir su recompensa por haber cooperado en el reenvío del mensaje. Sin embargo, si alguno de los nodos remitiera datos distintos sobre un mismo hecho, entonces el banco penalizaría a los dos nodos.

Los mensajes idénticos que han llegado a un nodo por otro camino son despreciados, por tanto el nodo emisor no recibirá recompensa por esa transferencia, creando así una necesidad de rapidez a los nodos ya que cuanto más tiempo tarden en encaminar un mensaje la probabilidad de que le llegue ese mismo mensaje al nodo a través de otros participantes de la red crece exponencialmente.

Si el nodo B recibiera un mensaje de A y alegara que ya lo ha recibido por otros nodos para dejar al nodo A sin recompensa y luego decidiera reenviarlo, el banco detectaría este mal comportamiento y podría tomar medidas contra el nodo B, ya no solo penalizándolo sino expulsándolo de la red VANET o medidas más fuertes que involucren a las autoridades policíacas.

Los mensajes que se transmiten en la red deben poseer información añadida para el cálculo de la función de beneficios, esto es, información de cuándo se creó el mensaje y de dónde se creó para calcular la distancia y el tiempo que ha transcurrido desde su creación. Estos campos están firmados y por tanto cualquier modificación por parte de algún nodo sería detectada y penalizada.

Los valores de los factores de balanceo α_i empleados en nuestra función de beneficios así como la distancia D_j y el tiempo T_j por el cual la información

Tipo de mensajes	α_1	α_2	D_j	T_j
Información Tráfico	0.6	0.4	3 Km	60s
Información Comercial	0.4	0.6	0.5 Km	20s

Tabla 3.1: Ejemplo de valores de los pesos según el tipo de mensaje

de un mensaje tiene interés para los nodos vienen dados por el tipo de los mensajes, siendo la propia red VANET la que otorga valores a los mensajes dependiendo de su categoría y evitando por tanto que sean los propios nodos los que asignen estos valores. Un ejemplo de unos posibles valores se pueden observar en la Tabla 3.1, para dos tipos de mensajes distintos: información de tráfico e información comercial.

Si un nodo está fuera del radio de acción de un mensaje, esto es, a una distancia en la cual la información del mensaje carece de interés entonces el beneficio que un nodo pueda obtener deberá ser inferior en cualquier caso al coste que le genera reenviar un mensaje.

3.4.2. Función de beneficios

El núcleo de nuestro esquema basado en incentivos consta de dos parámetros a tener en cuenta para calcular el beneficio de un nodo (fórmula 3.4): la distancia y el tiempo. El parámetro correspondiente al número de reenvíos que se tiene en cuenta en [12] ha sido suprimido de nuestra fórmula del cálculo de beneficios aunque, como ya explicamos anteriormente, cuantos más reenvíos haga un nodo más beneficio obtendrá por tanto ese parámetro que hemos eliminado de la fórmula sigue latente en el sistema.

Definimos la distancia como la diferencia entre el punto donde se creó el mensaje (origen) y el punto donde se encuentra en un momento en el tiempo determinado.

El tiempo lo definimos como la diferencia entre el instante actual y el instante en que fue creado en el origen.

Tal y como definimos anteriormente, estos parámetros permanecen invariables en el mensaje por lo que los nodos acceden a estos valores para calcular la función de beneficios por cada mensaje enviado. Por tanto una acción de reenviar un mensaje de un nodo A a un nodo B puede ser visto como una conversación independiente en un instante t entre dos participantes.

$$R_i = \alpha_1(-D_j(1 - e^{-d_{ij}}) + D_j) + \alpha_2 \frac{e^{-\frac{t_{ij}}{2}}}{2} T_j \qquad siendo\, t_{ij} > 0 \qquad (3.4)$$

En las siguientes subsecciones cada una de los componentes de la función de beneficios se explicarán y justificarán de manera independiente.

3.4.2.1. Distancia

La distancia constituye el primer parámetro de la función de beneficios (fórmula 3.5). Cuando algún acontecimiento ha sucedido en un lugar concreto es importante que esta información llegue a cuantos más vehículos mejor para poder actuar de manera consecuente en la carretera.

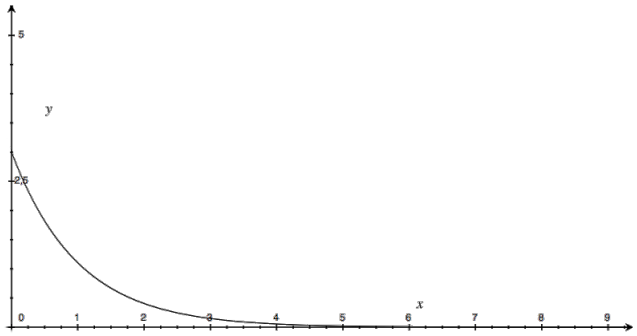

Figura 3.1: Recompensa VS Distancia. $D_j = 3$

Para evitar que un vehículo obtenga siempre una recompensa cuando se sale de un radio de actuación en el cual un mensaje deja de tener importancia, esta función debe tender a cero cuanto más lejos esté del origen. El comportamiento de esta función se puede observar en la Fig. 3.1

$$(-D_j(1 - e^{-d_{ij}}) + D_j) \tag{3.5}$$

Esta función es la misma que los autores contemplan en su función de beneficios en [12] correspondiente con la fórmula de Stokes. Donde d_{ij} corresponde a la distancia entre el nodo i que reenvía el paquete j del foco del mensaje y el parámetro D_j es la distancia máxima donde la información del mensaje j se considera interesante por los receptores.

En nuestro esquema, el parámetro D_j es establecido según el tipo de mensaje que sea en vez de ser el nodo inicial el que establezca ese parámetro impidiendo así a un nodo deshonesto a actuar de alguna manera que no sea óptima para nuestro esquema de cooperación.

3.4.2.2. Tiempo

El tiempo representa un parámetro especialmente crítico en la función de beneficios siendo el responsable de un comportamiento egoísta debido principalmente a que un nodo podría preferir no reenviar un mensaje a los demás nodos de la red para obtener así un mayor beneficio y no tener que compartirlo con nadie más [12].

Debido a que en nuestro modelo, los nodos tan sólo se ven recompensados por el número de reenvíos satisfactorios de los mensajes a otros componentes de la red este problema queda solventado (entendiendo como mensaje satisfactorio a todo aquel mensaje que ha sido reenviado de un nodo A a un nodo B y dicho mensaje no había llegado a B mediante otros nodos de la red).

Sin embargo hemos introducido como segundo componente de la función de beneficios un factor temporal para que no haya lugar a dudas y los nodos no estén tentados a mantener los mensajes para intentar beneficiar a otros nodos de la red y para que genere, aún más, una competencia para obtener mayor recompensa (fórmula 3.6).

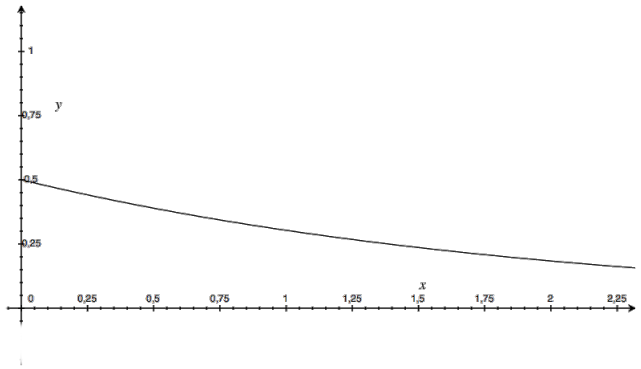

Figura 3.2: Recompensa VS Tiempo

Este parámetro es un caso concreto de la función gamma con unos valores establecidos de $\lambda = \frac{1}{2}$ y $k = 1$. Esta función, al igual que sucede con el parámetro de la distancia, debe tender a cero cuanto más tiempo pase desde la creación del mensaje en el origen. Al resultado final se le multiplica por la constante T_j que, recordemos, es el tiempo máximo por el cual un mensaje se considera interesante para los nodos.

$$\lambda e^{-\lambda d_{ij}} \frac{(\lambda d_{ij})^{k-1}}{\Gamma(k)} \longrightarrow \frac{e^{-\frac{t_{ij}}{2}}}{2} T_j \tag{3.6}$$

Esta función posee un comportamiento asintótico y tiende a 0 a medida que sucede el tiempo como se puede observar en la Fig. 3.2

3.5. Evaluación

3.5.1. Resistencia a ataques

Uno de los ataques típicos en las redes de cooperación tal y como describimos en nuestro modelo de atacantes son los *sybil attacks*. Sin embargo, en nuestro modelo se emplean certificados digitales y los nodos se identifican

mediante su clave pública y su correspondiente clave privada. Estos mecanismos de certificados digitales y criptografía pública es la solución que los autores indican en [11] para este tipo de ataques.

Otro de los ataques típicos en estos entornos de cooperación basada en incentivos, es que los nodos intenten suplantar la identidad de otros para conseguir así unas recompensas que no les corresponden. Sin embargo, en nuestro modelo, gracias al uso de certificados digitales y PKI para identificar a los componentes de la red sin que su privacidad se vea amenazada.

Pueden existir usuarios que intenten alterar los datos correspondientes a los datos de los mensajes para calcular su función de beneficios, sin embargo estos campos en los mensajes vienen firmados por lo que cualquier alteración sería detectada y el mensaje se dejaría de retransmitir entre los nodos ya que éstos no obtendrían recompensa y por tanto no les interesaría gastar unos recursos que luego no se van a ver recompensados.

Los nodos egoístas que intenten retener el mensaje para que otros nodos no obtengan un beneficio tan alto como él no conseguirá tampoco un beneficio tan alto como si lo reenviase lo más rápido posible debido a la fórmula del cálculo de beneficios.

3.5.2. Gestión de los incentivos

A continuación veremos cómo a través de nuestra nueva propuesta, se solucionan tres de los factores más importantes que en [12] no parecen tener solución que son: 1) Evitar que un mensaje se reenvíe de un nodo a otro continuamente y reciban un beneficio por ello; 2) Comprobar que un nodo está diciendo la verdad a la hora de reclamar sus incentivos; 3) Otorgar los incentivos de manera segura.

Para solucionar el primero de los problemas se emplea el uso de unos comprobantes entre los vehículos donde queda constancia que un mensaje se ha enviado de un nodo A a un nodo B en un instante determinado. Estos comprobantes aseguran que existan dos versiones sobre un mismo hecho. En caso de que un nodo reenvía el mismo mensaje a un nodo un número determinada de veces, la CA identificará que tan sólo el primer comprobante correspondiente a la primera retransmisión realizada tendrá validez descartando todos los anteriores evitando también los problemas que existían en [16].

El uso de comprobantes también se emplea para resolver el segundo de los problemas, es decir, cómo saber si un nodo está o no diciendo la verdad a la hora de reclamar sus incentivos. Se pueden dar 3 casos distintos:

1. El nodo receptor no suba el comprobante como que se ha efectuado una retransmisión. Si el nodo A, que reenvía el mensaje a B y este nodo B no se comunica con el banco y le dice que A le ha hecho llegar este mensaje bajo unas condiciones concretas, entonces B no puede

reenviar ese mensaje a otros nodos para obtener un beneficio de este mensaje ya que sería detectado automáticamente por las autoridades y penalizado consecuentemente.

2. Dos nodos envíen hechos distintos sobre la misma retransmisión. Cuando el banco valida la transferencia (verificando que el cálculo de A es correcto bajo las condiciones descritas) y por tanto el nodo A estaría dispuesto a recibir su recompensa por haber cooperado en el reenvío del mensaje. Sin embargo, si alguno de los nodos remitiera datos distintos sobre un mismo hecho, entonces el banco penalizaría a los dos nodos (pues el banco no sabe quién está diciendo la verdad).

3. Que el nodo B recibiera un mensaje de A y alegara que ya lo ha recibido previamente y luego intentara sacar partido de su retransmisión. Si el nodo B alegase que ya ha recibido previamente un mensaje por otros nodos para dejar al nodo A sin recompensa y luego decidiera reenviarlo, el banco detectaría este mal comportamiento y podría tomar medidas contra el nodo B.

Para solucionar el tercer gran problema, es decir, que los incentivos se otorguen de manera segura, tal y como indican los autores en [23], se necesita que exista una tercera parte confiable para poder realizar las transacciones seguras entre las entidades de la red. En nuestro esquema empleamos el concepto de bancos, que también pueden hacer las labores de CA, como tercera parte confiable para poder realizar el pago de los incentivos.

3.5.3. Evaluación experimental

Para validar nuestra propuesta, se han realizado numerosas simulaciones en el entorno de simulación de eventos discretos para entornos vehiculares llamado NS-2. Para ello, se han introducido una serie de valores para poder llevar a cabo la simulación:

- Número de nodos: 15.
- Extensión donde tiene lugar la simulación: 800m x 800m.
- Rango de acción de cada nodo: 100m.
- Movimientos de los nodos: aleatorio.
- Posición inicial de los nodos: aleatorio.
- Parámetros empleados de D_j y de T_j se corresponde con un paquete de información de tráfico (ver parámetros en la Tabla 3.1)

Se escoge un nodo A que envía uno y sólo un mensaje a los nodos que tiene dentro de su radio de acción. En ese momento, los vehículos que vayan recibiendo este primer mensaje se dispondrán a reenviarlo a todos los vehículos que se vayan encontrando (cuantos más, más beneficios obtendrán).

Cabe destacar también, que la posición de los nodos inicial influye en gran parte de los resultados aquí obtenidos. En nuestro caso, los nodos se encuentran en su gran mayoría cerca unos de otros (dentro de su radio de acción), sin embargo, si las simulaciones se realizaran en entornos donde los vehículos están separados unos de otros, estos resultados variarían considerablemente.

En la figura 3.3 se puede observar la relación que existe entre el beneficio que obtienen los vehículo de media con respecto de la distancia al punto donde se ha generado el primer mensaje. Como resulta lógico, los primeros nodos que reciben los mensajes obtendrán mayor beneficio ya que disponen de más tiempo y más nodos a los que mandar el mensaje además de que cuanto más se alejen del punto del origen, menos recompensa obtendrán. Tal y como debe actuar nuestro modelo, los últimos vehículos en recibir los mensajes, no tendrán más vehículos a los que reenviar el mensaje de manera única ya que lo habrán recibido previamente mediante otros vehículos.

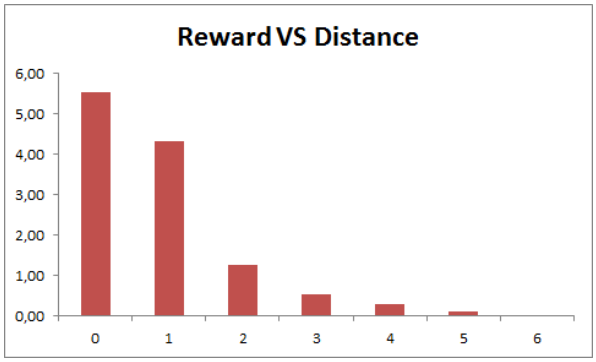

Figura 3.3: Recompensa que obtienen los nodos con respecto de la distancia

En la figura 3.4 se puede observar la relación que existe entre el tiempo y el beneficio que tiene cada vehículo de media. Como resulta lógico, a medida que pasa el tiempo, el beneficio que obtiene cada vehículo es menor (tiende a 0). Sin embargo, merece la pena destacar cómo crece y decrece el beneficio que obtienen los nodos ya que, hay que recordar que es la función de beneficios es la suma ponderada de dos parámetros y que cuantos más reenvíos realicen, más ganarán.

Finalmente, en la figura 3.5 se puede observar cómo evoluciona nuestra función de beneficios en función del tiempo y de la distancia. En esta gráfica se puede observar que el comportamiento de las gráficas anteriores responden a un comportamiento completamente normal (el número de reenvíos no hace más que aumentar o disminuir la escala de la gráfica). El eje x se corresponde

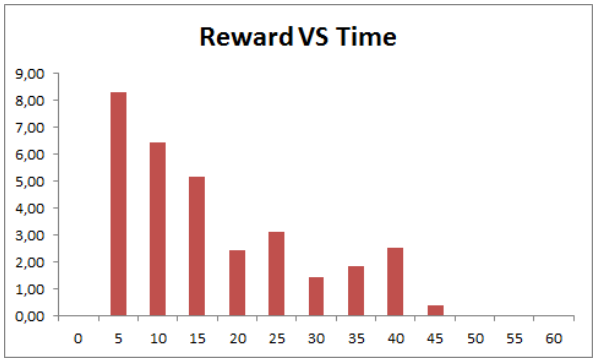

Figura 3.4: Recompensa que obtienen los nodos con respecto del tiempo

con la distancia, el eje y se corresponde con el tiempo y finalmente, el eje z se corresponde con la cantidad de reembolso que ha obtenido.

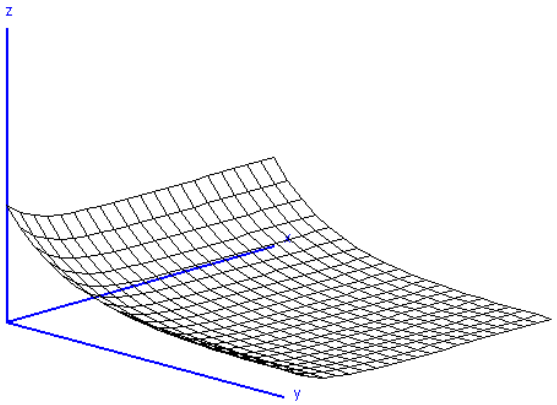

Figura 3.5: Recompensa que obtienen los nodos con respecto del tiempo y de la distancia

3.5.4. Discusión

En esta sección se compara directamente la propuesta que realizaron en [12] con con la planteada aquí con el fin de contrastar los resultados y observar la mejoría de nuestra propuesta (al margen de solucionar los problemas de seguridad que citamos en las secciones previas) con respecto al artículo sobre el que nos basamos.

Esta comparación entre las propuestas resulta muy complicada de realizar ya que en el artículo [12] no muestran con qué datos se ha realizado la simulación, sin embargo existe un resultado que revela un comportamiento muy importante. Parece lógico pensar que si un nodo no reenvía un mensaje,

entonces dicho nodo no debe recibir recompensa alguna. En la Fig. 3.6 se muestran los resultados obtenidos en [12] de enfrentar los incentivos que obtienen los vehículos con respecto del número de reenvíos.

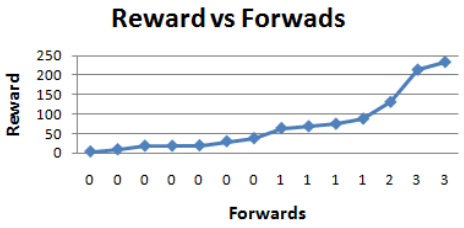

Figura 3.6: Recompensa que obtienen los nodos con respecto del número de reenvíos

Esta gráfica es significativa ya que aquí no interviene tanto los parámetros de la función de beneficios como el comportamiento del sistema. Se puede observar claramente que, a pesar de no haber reenviado ningún mensaje, el sistema otorga una serie de incentivos a lo vehículos. Esto es debido a que en el cálculo de los incentivos existen tres componentes como ya hemos mencionado anteriormente: la distancia, el tiempo y el número de reenvíos. Si se suprime el número de reenvíos, aún existen dos parámetros más para calcular el beneficio a pesar de no efectuar retransmisión alguna.

Este comportamiento se puede observar claramente mediante la representación gráfica de su función de beneficios en la Fig. 3.7. Siendo el eje OX el correspondiente a la distancia, el eje OY el correspondiente al tiempo y el eje OZ el correspondiente a los incentivos. Para ello, los valores que se han dado han sido: $D_j = 2$, $T_j = 3$ y $f_{ij} = 0$

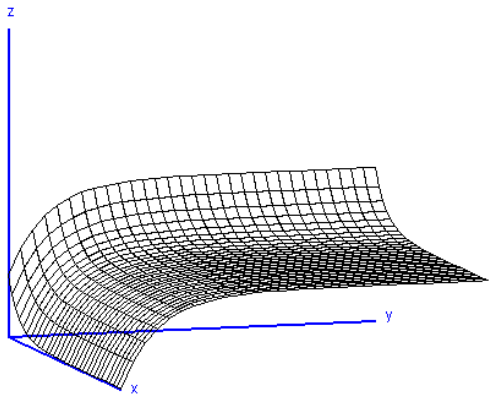

Figura 3.7: Recompensa que obtienen los nodos con respecto del tiempo y de la distancia en el artículo [12]

En esta gráfica se puede observar también que su función de beneficios,

no tiende a 0 nunca por mucho que pase el tiempo o la distancia, sino que llega un punto en el que se mantiene constante pero siempre recibiendo un incentivo.

En nuestro sistema propuesto, estos casos no pueden darse en ninguna circunstancia. Para el primer problema, se necesitan los comprobantes de los dos nodos que han participado en el reenvío de un mensaje y la posterior verificación de una tercera parte confiable, en nuestro caso, el AC. Si un nodo no retransmite mensaje alguno, entonces no recibe ningún premio. Mientras que cada retransmisión satisfactoria (bajo las condiciones descritas en nuestro modelo), conlleva un incentivo, por tanto a más retransmisiones más incentivos (las retransmisiones son tratadas de manera independiente).

En el segundo problema podemos observar en la Fig. 3.5 que el dominio de nuestra función sí tiende a 0 impidiendo por tanto que los nodos reciban un incentivo una vez superado el tiempo o el radio de acción de un mensaje.

3.6. Conclusiones

En este capítulo se ha realizado una nueva propuesta basada en incentivos para fomentar la cooperación en las redes vehiculares. En esta propuesta, se ha adaptado la función para calcular los beneficios que los autores crearon en [12] para que obtenga unos resultados que mejoraran a los iniciales y que solucionen los problemas que poseía este artículo como se han podido ver en la evaluación de nuestra propuesta.

Capítulo 4

Líneas Futuras

Si es bueno vivir, todavía es mejor
soñar, y lo mejor de todo, despertar.
Antonio Machado

Resumen: En este capítulo se detallan unas cuestiones abiertas para la propuesta que se detalló en el capítulo anterior. Se describe una nueva tecnología y por qué su unión con la tecnología de redes vehiculares se hace más que interesante.

4.1. Líneas Futuras

En las redes VANET existen numerosos vehículos que, constantemente están intercambiando información. Uno de los elementos software que mejor se adaptan a este tipo de tecnologías son los agentes móviles ya que son capaces de adaptarse al entorno y proseguir sus ejecuciones en diferentes dispositivos, tan sólo necesita que tengan una plataforma especial software para dar soporte a este tipo de software [30]. En este mismo artículo, se hace especial hincapié en la unión en ambas tecnologías, enfrentando los problemas y los beneficios que acarrearía esta unión.

Los agentes móviles pueden ser en un futuro no muy lejano una solución muy buena para las redes VANET debido, como ya dijimos anteriormente a su rápida capacidad para adaptarse. Sin embargo, tal y como dicen los autores en [30] existen dos principales retos que actualmente no tienen solución en las redes VANET que con agentes móviles se resolvería de manera trivial: que el reenvío de los mensajes sea haga en un tiempo concreto y que los destinatarios de esos mensajes sean los correctos.

El principal problema que posee la tecnología de agentes móviles es que actualmente, requieren que exista un nodo central que los coordine. Esto

obviamente choca con una de las principales problemas de los entornos distribuidos móviles y es que es complicado hacer que un nodo coordine al resto y por tanto se ha de prescindir de un coordinador centralizado. Debido a esto, parece razonable que la implementación de agentes móviles requiere de una pequeña remodelación para poder adaptarse a este nuevo entorno [31].

Otra de las cuestiones que aún están por resolver en este campo es garantizar la seguridad cuando un agente quiere saltar de un dispositivo a otro ya que este agente debe estar encriptado para evitar problemas como la privacidad, la de poder realizar un seguimiento a los vehículos, etc... Por tanto se debe establecer una confianza mutua entre el agente y el coche que va a dar soporte al agente. En el artículo [31] muestran más dificultades que existen en los agentes móviles y las redes VANET.

Por tanto, tal y como dicen en el artículo [30], una de las tecnologías a tener en cuenta en el futuro es la inclusión de agentes móviles en las redes vehiculares. Es un área completamente inexplorada que está llamada a ser una nueva línea donde focalizar los esfuerzos por parte de los investigadores.

Como trabajos futuros para nuestra propuesta, existen varias líneas donde el uso de agentes móviles podría ser una buena opción:

- Sustituir el uso de comprobantes por esta opción para ver cómo se comporta mejor, si con los agentes móviles o con los comprobantes.
- Usar agentes móviles para realizar las labores de los bancos, esto es, agentes móviles confiables que fueran de coche en coche, renovando los certificados temporales ya que puede haber zonas donde no exista una conexión con un banco como las zonas rurales.
- Emplear agentes móviles para saltar de manera aleatoria entre los vehículos y verificar que un nodo está actuando correctamente. Es decir, como si se tratase de un control policial donde se observase *in situ* al nodo trabajando

Así mismo, como trabajo futuro, queda simular nuestra propuesta en diferentes situaciones de tráfico, esto es, en autopistas, en ciudades reales con retenciones o en pueblos rurales donde existe un número pequeño de nodos entre otros para obtener así conclusiones que indiquen en qué situaciones se comporta peor o se comporta mejor nuestra solución.

Capítulo 5

Conclusiones

5.1. Conclusiones

En este trabajo de Fin de Máster se ha comenzado en el capítulo 1 introduciendo los elementos esenciales para comprender qué es una red vehicular, qué supone la cooperación en estos entornos y por qué supone un problema. En el capítulo 2 se ha realizado una recopilación y análisis correspondiente al estado del arte de la cooperación en entornos vehiculares.

Posteriormente y una vez comprendidas las debilidades de las propuestas que los autores habían realizado en este campo, nos hemos basado en el artículos [12] cuya idea carecía de elementos para comprobar la veracidad del cálculo de la recompensa de cada nodo así como tampoco se contemplaba la posibilidad de que un mensaje estuviera reenviándose entre unos nodos continuamente y por ello recibir un gran incentivo para realizar una nueva aportación en el capítulo 3 basándonos en un sistema de incentivos para fomentar la cooperación donde se solucionasen esos problemas y se introdujera una tercera parte confiable para poder realizar los pagos ya que sin él, no se podría.

Finalmente en el capítulo 4 se muestran unas líneas futuras sobre las que trabajar para expandir y mejorar nuestra propuesta.

Bibliografía

[1] W. Bamberger, J. Schlittenlacher, and K. Diepold. A Trust Model for Intervehicular Communication Based on Belief Theory. *2010 IEEE Second International Conference on Social Computing*, pages 73–80, Aug. 2010.

[2] M. S. Bouassida and M. Shawky. A cooperative congestion control approach within vanets: formal verification and performance evaluation. *EURASIP J. Wirel. Commun. Netw.*, 2010:11:1–11:12, April 2010.

[3] L. Buttyán and J. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Kluwer Academic Publishers, Mobile Networks and Applications*, 8(5):579–592, 2003.

[4] P. Caballero-Gil, J. Molina-Gil, and C. Stimulating cooperation in self-organized vehicular networks. *2009 IEEE, APCC 2009.*, 2010.

[5] T. Chen, F. Wu, and S. Zhong. Stimulating Cooperation in Vehicular Ad Hoc Networks: A Coalitional Game Theoretic Approach. *Vehicular Technology, IEEE Transactions on*, (99):1–1, 2010.

[6] F. Dotzer, L. Fischer, and P. Magiera. VARS: A Vehicle Ad-Hoc Network Reputation System. *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, (1):454–456.

[7] R. Franklin. On an improved algorithm for decentralized extrema finding in circular configurations of processors. *Commun. ACM*, 25:336–337, May 1982.

[8] D. Gambetta. Can we trust trust? In D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, chapter 13, pages 213–237. Published Online, 2000.

[9] H. Garcia-Molina. Elections in a distributed computing system. *IEEE Trans. Comput.*, 31:48–59, January 1982.

[10] G. Guette and C. Bryce. Using tpms to secure vehicular ad-hoc networks (vanets). In J. Onieva, D. Sauveron, S. Chaumette, D. Gollmann, and

K. Markantonakis, editors, *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, volume 5019 of *Lecture Notes in Computer Science*, pages 106–116. Springer Berlin / Heidelberg, 2008.

[11] G. Guette and B. Ducourthial. On the sybil attack detection in vanet. *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 0:1–6, 2007.

[12] C. Hernández-Goya, P. Caballero-Gil, J. Molina-Gil, and C. Caballero-Gil. Cooperation enforcement schemes in vehicular ad-hoc networks. In R. Moreno-Diaz, F. Pichler, and A. Quesada-Arencibia, editors, *Computer Aided Systems Theory - EUROCAST 2009*, volume 5717 of *Lecture Notes in Computer Science*, pages 429–436. Springer Berlin / Heidelberg, 2009.

[13] A. H. Ho, Y. H. Ho, and K. A. Hua. Adapting connectionless approach to ad-hoc networks in urban environments. pages 532–538, 2005.

[14] Y. H. Ho, A. H. Ho, G. L. Hamza-Lup, and K. a. Hua. Cooperation Enforcement in Vehicular Networks. *2008 IEEE International Conference on Communication Theory, Reliability, and Quality of Service*, pages 7–12, June 2008.

[15] a. Josang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644, Mar. 2007.

[16] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu. Secure incentives for commercial ad dissemination in vehicular networks. *ACM Press*, page 150, 2007.

[17] F. Li and J. Wu. FRAME: an innovative incentive scheme in vehicular networks. *Communications, 2009. ICC'09. IEEE International*, pages 1–6, June 2009.

[18] N.-W. Lo and H.-C. Tsai. A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks. *EURasiP Journal on Wireless Communications and Networking*, 2009:1–11, Sept. 2009.

[19] M. E. Mahmoud and X. Shen. Pis: A practical incentive system for multi-hop wireless networks. *Vehicular Technology IEEE Transactions on*, 59(8):1, 2010.

[20] F. Martinez, M. Fogue, M. Coll, J.-C. Cano, C. Calafate, and P. Manzoni. Evaluating the impact of a novel warning message dissemination scheme for vanets using real city maps. In M. Crovella, L. Feeney,

D. Rubenstein, and S. Raghavan, editors, *NETWORKING 2010*, volume 6091 of *Lecture Notes in Computer Science*, pages 265–276. Springer Berlin / Heidelberg, 2010.

[21] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil. A vision of cooperation tools for vanets. *IEEE Computer Society*, pages 1–4, 2010.

[22] S. MOLONEY and P. GINZBOORG. Security for interactions in pervasive networks: Applicability of recommendation systems. *Lecture notes in computer science*, pages 95–106.

[23] H. Pagnia and F. C. Gartner. On the impossibility of fair exchange without a trusted third party. *Darmstadt University of Technology Department of Computer Science Technical Report TUDBS199902*, 1999.

[24] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11):100–109, 2008.

[25] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. pierre Hubaux. Certificate revocation in vehicular networks. Technical report, Technical Report LCA-Report-2006-006, 2006.

[26] M. Raya, P. Papadimitratos, V. D. Gligor, and J. pierre Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *IEEE Conference on Computer Communications*, pages 1238–1246, 2008.

[27] N. Shastry and R. Adve. Stimulating Cooperative Diversity in Wireless Ad Hoc Networks through Pricing. *2006 IEEE International Conference on Communications*, pages 3747–3752, June 2006.

[28] S. Sukumaran and V. Jaganathan. Reputation based on demand routing protocol using mobile agent in mobile ad-hoc networks. *2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC)*, pages 1–4, Jan. 2010.

[29] C. Suthaputchakun and A. Ganz. *Priority Based Inter-Vehicle Communication in Vehicular Ad-Hoc Networks using IEEE 802.11e*, pages 2595–2599. IEEE, 2007.

[30] O. Urra, S. Ilarri, T. Delot, and E. Mena. Mobile agents in vehicular networks: Taking a first ride. *Springer Berlin / Heidelberg*, 70:119–124, 2010.

[31] O. Urra, S. Ilarri, R. Trilo, and E. Mena. Mobile agents and mobile devices: friendship or difficult relationship? *Journal of Physical Agents*, 3:27–37, May 2009.

[32] Z. Wang and C. Chigan. Countermeasure Uncooperative Behaviors with Dynamic Trust-Token in VANETs. *2007 IEEE International Conference on Communications*, pages 3959–3964, June 2007.