Modelo de confianza evolutivo para lograr cooperación emergente en redes ad-hoc a través de algoritmos genéticos

Diego Alejandro Vega Vega

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial
Bogotá D.C., Colombia
2021

Modelo de confianza evolutivo para lograr cooperación emergente en redes ad-hoc a través de algoritmos genéticos

Diego Alejandro Vega Vega

Tesis presentada como requisito parcial para optar al título de:
Magister en Ingeniería de Sistemas y Computación

Director(a):
Ph.D. Jorge Eduardo Ortiz Triviño

Línea de Investigación:
Computación aplicada
Grupo de Investigación:
TLÖN - Grupo de Investigación en Redes de Telecomunicaciones Dinámicas y Lenguajes de Programación Distribuidos

Universidad Nacional de Colombia
Facultad de Ingeniería, Departamento de Ingeniería de Sistemas e Industrial
Bogotá D.C., Colombia
2021

Dedicatoria

A mis padres y todos mis amigos que me acompañaron en el proceso de desarrollo de esta tesis.

Agradecimientos

En primer lugar, a mi familia que me apoyó durante toda mi trayectoria académica, tanto en la parte económica como en la parte anímica.

Al profesor Jorge Eduardo Ortiz Triviño por recibirme en su grupo de investigación y compartir conmigo sus enseñanzas a lo largo de este trabajo de maestría.

Al profesor Juan Pablo Ospina por su paciencia y consejos, que son los que me han llevado a lograr este documento y este logro académico.

Finalmente, a todos mis amigos que me brindan su apoyo y que me recuerdan que en la vida es importante el desarrollo académico y personal en la misma medida.

Resumen

Modelo de confianza evolutivo para lograr cooperación emergente en redes ad-hoc a través de algoritmos genéticos

En esta tesis, se propone un modelo evolutivo para interacciones de agentes en redes ad-hoc. Para esto, primero se hizo una revisión general sobre los diferentes tipos de modelos existentes en la literatura, con el fin de elegir un modelo en función de su pertinencia. El modelo escogido utiliza algoritmos genéticos complementados con juegos estocásticos, que se espera que ofrezcan un comportamiento adaptativo y dinámico. A continuación, se diseñaron las simulaciones con el fin de involucrar la naturaleza de las redes ad-hoc, donde se demostró que los algoritmos genéticos son capaces de adaptarse a la red, pero el proceso toma 1.000 interacciones para alcanzar indicadores favorables. En consecuencia, se propuso la inclusión de juegos estocásticos, los cuales alcanzan los mismos indicadores con solo 250 interacciones. Este resultado evidencia las ventajas del modelo propuesto. Finalmente, se realizó la implementación de una prueba piloto sobre una red ad-hoc real, validando el comportamiento de las simulaciones. La principal contribución de este trabajo es el modelo adaptativo, que además presenta una mejora en la velocidad de adaptación en entornos adversos en comparación con trabajos encontrados en la literatura.

Palabras clave: Auto-organización, cooperación, confianza, adaptación, redes ad-hoc.

Abstract

Evolutionary trust model to achieve emergent cooperation in ad-hoc networks through genetic algorithms

This thesis proposes an evolutional model for agent interactions in ad-hoc networks. For this purpose, an overview is presented of the different types of existing models in the literature, in order to choose a model based on its relevance to the objective. The choosen model uses genetic algorithms improved by including stochastic games that are expected to offer an adaptative and dynamic behavior. After defining the model to be studied, the simulations were designed to involve the nature of ad-hoc networks. The simulations show that the genetic algorithms are able to adapt to the network, but the process takes 1.000 interactions to reach favorable indicators. In consecuence, the inclusion of stochastic games is proposed. With this improvement, the algorithm reaches the same indicators with only 250 interactions. This result evidences the advantages of the model proposed. Finally, the implementation in a real ad-hoc network showed results that validate the behavior observed in the simulations. The main contribution of this work is the adaptative model that also presents an improvement in the velocity of adaptation in adverse environments in comparison with previous works in the literature.

Keywords: Self-organization, cooperation, trust, adaptation, ad-hoc networks

Esta tesis de maestría se sustentó el 15 de Septiembre de 2021 a las 10:00 am,
y fue evaluada por los siguientes jurados:

Luis Fernando Niño Vásquez (Ph.D.)
Universidad Nacional de Colombia
Departamento de ingeniería de sistemas e industrial

Jeisson Andrés Vergara Vargas (Ph.D.)
Universidad Nacional de Colombia
Departamento de ingeniería de sistemas e industrial

Contenido

Lista de símbolos

En esta capítulo se definen las abreviaciones usadas en el documento y los símbolos utilizados en las ecuaciones descritas, especialmente en el capítulo 4 en donde se define el modelo principal.

Símbolos con letras latinas

Símbolo	**Término**	**Unidad SI**	**Definición**
C	Confianza en la red	%	*Porcentaje*
p_i	Resultado del envío numero i	1	*Binario*
$NC_{a,b}(t)$	Nivel de confianza en una interacción t	1	*Entero*
$fitness_a$	Puntaje del agente a	1	*Entero*
e	Error no controlado del sistema	1	*Porcentaje*
H_k	Entropía del evento k	1	*Real*
H_{env}	Entropía de un envío	1	*Real*
H	Entropía del sistema	1	*Real*

Símbolos con letras griegas

Símbolo	**Término**	**Unidad SI**	**Definición**
$\beta_{a,b}(t)$	Resultado una interacción	1	*Binario*
$\Phi(a)$	Probabilidad de escoger el agente a	1	*Porcentaje*
λ_m	Probabilidad de cruce	1	*Porcentaje*
θ_j	Probabilidad de obtener la salida j	1	*Porcentaje*

Subíndices

Subíndice	Término
a	Agente
b	Agente
t	Número de interacción
k	Evento en la red: resultado interacción de dos agentes
env	Envío
j	Salida de un proceso (Éxito o fallo)

Abreviaturas

Abreviatura	Término
AGT	*Algorithmic Game Theory*
C	Cooperación en una interacción
CONFIDANT	*Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks*
MANET	*Mobile Ad-hoc Network*
R	Rechazo de una interacción
SORI	*Secure and Objective Reputation-based Incentive*
VANET	*Vehicular Ad-hoc Network*

1 Introducción

Las redes ad-hoc también conocidas como MANETs (por sus siglas en inglés: *Mobile Ad-Hoc Networks*) son redes distribuidas para ambientes de computación que, en comparación con las redes más utilizadas, como la WIFI, tienen una ventaja en términos de robustez, ya que no dependen de una jerarquía específica que garantice el funcionamiento de la red. Las redes ad-hoc tienen una estructura distribuida, lo que quiere decir que todos los participantes pueden actuar como clientes y como servidores. Esta estructura distribuida ofrece estabilidad, ya que cuando algún integrante de la red falla o se sale de esta, no afecta su funcionamiento. Por otro lado, otra cualidad importante de las redes ad-hoc es la autonomía de cada integrante de la red para tomar decisiones sobre su participación en los diferentes procesos que se llevan a cabo en la red. Este trabajo está enmarcado en el proyecto del grupo de investigación TLÖN, el cual desarrolla una red ad-hoc social-inspirada, es decir, que se modelan todos los mecanismos de la red de manera análoga a la forma en que las sociedades humanas se organizan a sí mismas.

Dentro de las redes ad-hoc, se tiene un flujo de información constante, debido a que los participantes de la red necesitan comunicarse y enviar documentos a través de la red. Para esto, es necesario definir los mecanismos de interacción entre los participantes de la red, particularmente en el caso de esta tesis se trabajará sobre el sistema multi-agente, donde conviven e interactúan todos los agentes. Estas interacciones no son siempre exitosas, pueden fallar por varias razones, como una falla de la conectividad, falta de recursos disponibles o por la presencia de integrantes egoístas en la red. Estos últimos son aquellos que buscan aprovecharse de la red y en este proceso pueden afectar el desempeño global de la red en términos de efectividad de la comunicación. De esta manera, se hace necesario proponer un mecanismo de interacción de los agentes que le permita a la red adaptarse a las condiciones expuestas y obtener unos indicadores favorables independientes de la presencia de integrantes egoístas, falta de recursos o fallas no controlables de la conexión.

El objetivo principal esta tesis es diseñar un modelo de confianza evolutivo para redes ad-hoc que promueva la cooperación y permita a la red adaptarse a anomalías durante el intercambio de mensajes. Para lograr esto es necesario en primer lugar modelar formalmente un mecanismo de confianza evolutivo para redes ad-hoc, tomando como referencia la literatura académica existente. En segundo lugar, se debe implementar dicho modelo en un ambiente controlado de simulación donde se definan 2 indicadores relacionados con el desempeño de

la red. Por último, el comportamiento del modelo se valida con una implementación sobre una red ad-hoc en un ambiente real.

Después de realizar la revisión de la literatura de los protocolos existentes para modelar este tipo de interacciones en redes ad-hoc, se exploran los diferentes enfoques encontrados y se presentan los trabajos con mejores resultados que además tienen un enfoque social-inspirado, alineando el modelo con los objetivos del grupo de investigación TLÖN de la Universidad Nacional de Colombia, como se explicará más adelante. De esta manera, se escoge el modelo propuesto por Mejía en 2011 [32], el cual propone un algoritmo genético con evolución plasmática que logra adaptarse a los agentes egoístas de la red. No obstante, se identifica que el modelo aún necesita ser mejorado para poder enfrentar los niveles de errores no controlados que dificultan la adaptación. Por esta razón, se propone la implementación de juegos estocásticos en el modelo para acelerar el proceso de adaptación. Finalmente, se proponen 2 métricas que permitirán observar el desempeño del modelo. Estas métricas son la confianza global del sistema y la entropía del sistema, con estos datos podremos ver el comportamiento de la comunidad de agentes a través del tiempo.

Las pruebas realizadas se dividen en dos partes. La primera parte consta de los ambientes simulados, en donde se representan las condiciones de operación, incluyendo la probabilidad de errores no controlados y la movilidad de los agentes. Resultado de las simulaciones realizadas con el modelo propuesto, se obtiene un nivel de adaptación mejorado con respecto al modelo tomado inicialmente [32]. La segunda parte consta de la implementación del modelo en una red ad-hoc real. Para esto, se hace el levantamiento de la red sobre la infraestructura disponible gracias al grupo de investigación TLÖN. En estas pruebas se logra validar el comportamiento obtenido en las simulaciones y con esto se confirma el aporte del modelo en términos de velocidad de adaptación en ambientes adversos sobre las redes ad-hoc.

La tesis esta organizada de la siguiente manera. El marco teórico del problema se expone en el capítulo 2, donde se hace un revisión de los conceptos de redes de comunicación auto-organizantes, relevantes para abordar el problema de investigación descrito. Seguido a esto, se presenta en el capítulo 3, la revisión de la literatura en donde se exploran los desarrollos existentes en la comunidad académica, relacionados con la obtención de confianza, como comportamiento emergente en redes auto-organizantes. Posteriormente, en el capítulo 4 se describe en detalle el modelo propuesto en esta tesis. Además, se expone la descripción del ambiente de simulación sobre el cual va a ser probado el modelo para mostrar los resultados simulados. Finalmente, en el capítulo 5 se presenta la implementación del modelo sobre la red ad-hoc junto con los resultados obtenidos, comparados con aquellos obtenidos en las simulaciones.

2 Redes de comunicación auto-organizantes

2.1. Introducción

Los avances tecnológicos son cada vez más frecuentes y variados. Actualmente existe en tecnología la tendencia de conectar a las personas a través de los múltiples dispositivos que ya hacen parte de nuestra cotidianidad (Internet de las cosas, tecnología 5G, entre otras), ya sean dispositivos portátiles (celular, reloj inteligente, computadores, etc) o estacionarios (televisor, nevera, videojuego, etc). La idea es aprovechar la variedad y cantidad de elementos tecnológicos para interconectarlos y obtener un beneficio de la información generada. Las redes ad-hoc tienen este enfoque de interconectar y comunicar dispositivos entre sí. Este tipo de red ha sido investigado desde hace 2 décadas [50] debido al potencial que tiene en el aprovechamiento de la información y de los recursos entre varios dispositivos, utilizando computación distribuida.

El objetivo de este capítulo es realizar una descripción de las interacciones que se dan dentro de un sistema auto-organizante como lo es una red ad-hoc y los diferentes modelos que se utilizan para modelar estas interacciones, particularmente los modelos basados en reputación que tienen diversos enfoques. Se trata de entender cuáles son los desafíos de este tipo de red auto-organizante y los aspectos que se pueden aprovechar de los estudios existentes en comportamientos sociales aplicados a modelos computacionales.

2.2. Sistemas auto-organizantes

En un sistema en el que pueden habitar múltiples dispositivos, la construcción de una red mínima consta de 2 dispositivos. Desde el momento en que la conexión comienza, se vuelve relevante conocer quién toma las decisiones sobre la conexión. En otras palabras, en caso de que se necesite tomar una decisión que afecte a la red, hay que saber si se entrega el control a alguno de los participantes, o se cuenta con una estructura aparte que se encargar de moderar las interacciones. Estas preguntas se han respondido de varias formas dependiendo de la estructura de conexión que se utilice. Por ejemplo, las redes wifi y las conexiones TCP/IP, utilizadas cotidianamente para acceder a internet y para llamadas, respectivamente, manejan

sus conexiones de manera jerárquica, es decir, a través de una relación cliente - servidor, en donde el servidor es el que modera todas las interacciones y es el encargado de llevar a cabo la comunicación entre dispositivos "cliente" de la red. Esta jerarquía da un control total sobre la red al proveedor del servicio. Por otra parte, existe una estructura de mediación entre dispositivos propia de los sistemas auto-organizantes que se caracteriza por su ausencia de jerarquías. Esto quiere decir que cada dispositivo conectado tiene la autonomía de decidir sobre sus acciones y su participación en la red. La responsabilidad de organizar y coordinar esta comunidad de dispositivos no recae sobre un ente superior u orquestador. Los dispositivos deben poder organizarse a sí mismos y por esto se le denomina un sistema auto-organizante.

2.3. Red ad-hoc

Una red ad-hoc o MANET (*Mobile Ad-hoc Network*) es una plataforma computacional flexible, dinámica y estocástica que gestiona recursos distribuidos enlazados inalámbricamente. Estos recursos a su vez pueden ser cambiados, movidos, aumentados y, en general, combinados de formas novedosas [25]. Estas redes son un ejemplo de una red auto-organizante debido a que no existe una infraestructura encargada de gobernar o administrar la red, todos sus integrantes están encargados de coordinar sus tareas. Este tipo de estructura facilita su despliegue en contextos de operación adversos donde no es posible utilizar una estructura preestablecida [17, 43]. Las aplicaciones más mencionadas en la literatura son las VANETs, las redes de sensores y la agrónica:

- VANET: Abreviación de *Vehicular Ad-hoc Network*. Su objetivo es conectar vehículos y sensores de tráfico para compartir información del tráfico. Con esta información, cada integrante puede tomar decisiones sobre la ruta a seguir. Adicionalmente, la información recolectada es útil para las entidades gubernamentales encargadas de la movilidad en la ciudad, ya que puede entender el comportamiento del tráfico en un sector específico. Este tipo de redes se forman de manera espontánea y tienen tiempos de vida muy cortos, debido a que se tiene un alto índice de movilidad y variabilidad en la cantidad de nodos [42, 18]

- Las redes de sensores se caracterizan por contar con diversos tipos de dispositivos conectados y compartir información con un objetivo global. Estas redes se caracterizan por contar con recursos limitados por parte de la mayoría de sus dispositivos, ya que se usan con sensores. Por ejemplo, no se cuenta con una capacidad alta de memoria [42, 13]. Este tipo de redes se concentran en optimizar el uso de energía, procesamiento de información distribuida y la coordinación de tareas al interior de la red [27].

- La agrónica o agricultura de precisión se utiliza para apoyar el proceso de cultivo a través de sensores y otros dispositivos que se encargan de recolectar información distribuida para mejorar la toma de decisiones. La ventaja que ofrece la red ad-hoc en

este contexto es su flexibilidad para desplegarse en diferentes ambientes o escenarios, como en el caso de un cultivo en una zona de páramo, donde las temperaturas varían constantemente.

2.4. Interacción entre agentes

Una red auto-organizante es un sistema complejo que se caracteriza por tener una gran cantidad de individuos o de entes que se comportan de manera autónoma y que pueden interactuar entre sí. Esto se puede comparar con el funcionamiento de una sociedad, la cual necesita algunos elementos básicos para construirse. El elemento primordial de estos sistemas es el lenguaje, ya que para poder interactuar los individuos necesitan un medio de comunicación, ya sea verbal, a través de feromonas, por ondas, por calor, o cualquier otro método. El lenguaje constituye la base de la interacción y a partir de esto se puede construir un sistema complejo como el de una sociedad humana.

Una de las herramientas para el estudio de sistemas complejos computacionales son los sistemas multi-agente, que abstraen el concepto de un sistema como la sociedad humana a través de una comunidad de entes o individuos denominados **agentes**, los cuales tienen como mínimo 2 cualidades: la toma de decisiones (hasta cierta medida) autónomas orientadas a satisfacer sus objetivos propios y además la interacción con otros agentes [53]. En una red ad-hoc, debido a su estructura no jerarquizada, la comunicación se da entre sus integrantes de manera directa. Cada nodo de la red tiene la posibilidad de comunicarse con todos los nodos que pertenezcan a la red y que estén dentro de su rango de alcance sin necesidad de intermediarios. En el caso de los nodos que están fuera de alcance pero que pertenecen a la red, tienen la posibilidad de comunicarse a través de intermediarios mediante procesos de difusión de información. Existen varios protocolos propuestos para la difusión de información en la red y se pueden clasificar según las estrategias, por ejemplo: heurísticas, geométricas, estocásticas, basadas en vecinos, basadas en ubicación y basadas en acuerdos [19]. Este proceso de comunicación constante se puede modelar a través de un sistema multi-agente

2.5. Teoría de juegos

La teoría de juegos es el estudio de modelos matemáticos de las interacciones entre entes racionales capaces de tomar decisiones. Dichas interacciones pueden resultar en conflictos o cooperaciones dependiendo de las estrategias que manejan los individuos [35]. La teoría de juegos brinda un fundamento matemático a la solución de problemas sociales, por esta razón no solamente es usada en las ramas de las Ciencias Sociales, sino también en las Ciencias de la Computación con la teoría de juegos algorítmica (AGT por sus siglas en ingles) [45].

2.5.1. Dilema social

Existen problemas sociales muy estudiados en las ciencias de la computación que tienen en común la complejidad que se requiere para solucionarlos, además de ser fácilmente encontrados en las sociedades humanas. Estos problemas se conocen como dilemas sociales. Existen dos dilemas sociales principalmente estudiados: el dilema del prisionero y la tragedia de los comunes, los cuales se describen a continuación.

2.5.2. El dilema del prisionero

Este dilema describe la situación de dos ladrones que son capturados por la policía e interrogados de manera aislada. Los policías dan a cada uno de los ladrones dos opciones: confesar el crimen o guardar silencio [41]. Esto significa que hay 4 posibles resultados de esta interacción que dependerán de qué tanta confianza se tiene entre los dos individuos. Podemos imaginar que dos ladrones que se tienen toda la confianza nunca van a delatar o traicionar al otro, por lo tanto, este problema pone a prueba la confianza de los individuos. Las consecuencias de cada caso se muestran en la Tabla **2-1**, donde A y B representan la cantidad de años de prisión que debe pagar cada ladrón. Los resultados de la interacción se clasifican de la siguiente manera:

- El caso (1) en que ambos ladrones confiesan el crimen y por ser culpables ambos deben pagar 5 años de prisión (en total se pagarían 10 años de prisión).

- Los casos (2) y (3) en donde uno de los ladrones traiciona al otro y por esto el que confiesa queda libre, mientras que el traicionado debe pagar la máxima pena posible (20 años). Desde el punto de vista del sistema, este es el peor de los casos.

- El caso (4) en donde ninguno de los ladrones acepta el crimen y por esta razón solo les pueden imponer 1 año a cada uno. Este es el caso en que menos años deben ser pagados en total (dos) y es el escenario ideal en un sistema cooperativo.

		Decisión ladrón B	
		Confiesa	Guarda silencio
Decisión ladrón A	Confiesa	(1) A=5 años, B=5 años	(2) A=0 años, B=20 años
	Guarda silencio	(3) A=20 años, B=0 años	(4) A=1 año, B=1 año

Tabla 2-1: Condenas en el dilema del prisionero. Elaboración propia.

2.5.3. El dilema del prisionero iterado

Este dilema describe una variación del dilema del prisionero, donde se presenta la oportunidad de aprender de la experiencia. Esto quiere decir que los agentes participando en el dilema tendrán la oportunidad de repetir el dilema varias veces, con la posibilidad de recordar los resultados de las interacciones anteriores. Esto dependerá de la estrategia: como no es necesario recordar todas las interacciones, el tamaño de esta memoria se debe optimizar, ya que la memoria de un dispositivo no es ilimitada. El objetivo de repetir las interacciones es llegar a una convergencia de los resultados de la interacción. Para esto, se han propuesto diferentes estrategias de agentes que pueden lograr resultados favorables, algunas de las más estudiadas son:

- **Altruista**: El agente siempre coopera en la interacción, ignorando el resultado de las interacciones anteriores.
- **Egoísta**: El agente siempre rechaza la interacción, ignorando el resultado de las interacciones anteriores.
- **Tit-for-tat**: En la primera interacción coopera en la interacción y, a partir de ese momento, la interacción será igual a la decisión que tomó el otro agente en la interacción inmediatamente anterior. Esta estrategia utiliza un espacio de memoria para recordar la decisión del otro agente en la interacción previa.
- **Tit-for-tat suavizado**: Tiene la misma función del tit-for-tat, pero adicionalmente existe una probabilidad definida de cooperar con el otro agente ignorando la interacción previa.

De estas estrategias, el tit-for-tat es la más exitosa para lograr cooperación mutua dentro de las características descritas del dilema del prisionero iterado [5]. Si adicionalmente en el dilema se tiene una probabilidad de que sucedan errores, el tit-for-tat va a perder la cooperación mutua. En este escenario, el tit-for-tat suavizado permite reiniciar la confianza periódicamente para contrarrestar el error en las interacciones.

2.5.4. La tragedia de los comunes

Se refiere a la situación de muchos individuos que conviven en un mismo entorno y poseen un recurso limitado a su disposición (por el ejemplo, el agua para los humanos). Desgraciadamente, si la población es muy numerosa y cada individuo sigue sus intereses individuales, se acaba el recurso rápidamente y todo el sistema se ve perjudicado [20]. Una diferencia entre este problema y el dilema del prisionero es que este se centra en interacciones entre varios (2 o más) individuos. En cambio, en el dilema del prisionero el foco es la interacción entre solamente dos individuos. Sin embargo, los dos problemas se asemejan en que la falta de cooperación entre los involucrados resulta en el peor resultado para el sistema en general.

2.6. Confianza y cooperación

La confianza se define como un estado psicológico que describe la expectativa (probabilidad) que se tiene de que un individuo **A**, al interactuar con otro individuo **B**, se comportará de una manera **X** en un contexto **Y** [8]. Esto significa que el individuo **A** va a preferir actuar de manera **X** sobre cualquier otro comportamiento y esto es lo que diferencia la confianza de una mera expectativa [9]. Por otro lado, la cooperación sucede cuando el individuo **A** actúa voluntariamente con el fin de beneficiar al individuo **B** o a ambos [9]. Esto quiere decir que las decisiones no se limitan a una función objetivo propia, sino que se tiene una visión global de las acciones. Esta definición muestra una estructura bien definida que es lo suficientemente clara para ser aplicada a un modelo computacional como el usado en los sistemas auto-organizantes y particularmente en una red ad-hoc.

El mecanismo de una red ad-hoc para realizar la comunicación entre sus nodos se denomina protocolo de comunicación. Existen muchos protocolos diseñados con diferentes objetivos dentro de la red. Se pueden encontrar enfoques como en [2, 16, 24, 12], donde se busca dar seguridad de la información. Por otro lado en [32, 6] se da prioridad a la dinámica de la red, es decir, a manejar la movilidad constante de sus integrantes. Otro enfoque interesante es el de [26], que se preocupa por la seguridad a través de los conceptos de confianza y colaboración. Recientemente, se han propuesto modelos con algoritmos complejos que cada vez son más robustos, como en [32] donde se usan algoritmos genéticos y evolución plasmática para una adaptación constante de los agentes a los cambios del sistema. Este último modelo, propone una aplicación de un modelo basado en confianza para administrar las interacciones de los agentes. El objetivo es lograr la cooperación de la red y los resultados son positivos en cuanto al crecimiento de la cooperación en la red a medida que pasa el tiempo.

2.7. Conclusiones

En este capítulo se habló de los sistemas auto-organizantes como un conjunto de individuos que toman decisiones y que interactúan entre sí. Estas interacciones generan problemas complejos cuando se trata de cuidar el bienestar global del sistema y para abordarlos la teoría de juegos se presenta como una solución adecuada y pertinente, la cual se encarga de dar una perspectiva matemática a problemas de las ciencias sociales que surgen en este tipo de sistemas. La forma de estudiar los sistemas complejos es partiendo de los elementos individuales hacia una visión global. Los comportamientos que son resultado de muchas combinaciones de interacciones sencillas se denominan comportamientos emergentes. El objetivo de esta tesis es modelar comportamientos emergentes, como el caso de la confianza, en una comunidad de agentes que habitan un sistema auto-organizante. Para esto, se necesita profundizar en las técnicas empleadas en computación de teoría de juegos y particularmente en modelos aplicados a redes ad-hoc.

3 Confianza emergente en redes auto-organizantes: revisión de literatura

3.1. Introducción

En este capítulo se realiza una revisión de la literatura correspondiente a las metodologías propuestas para lograr confianza como un comportamiento emergente en redes auto-organizantes y particularmente en redes ad-hoc. Estas redes emplean autonomía en las decisiones de cada dispositivo en la red, lo cual abre las puertas a nuevos mecanismos de colaboración y de organización dentro de la red. Este tipo de organización no jerarquizada en el caso particular de las interacciones entre dispositivos de la red trae algunos desafíos para el mecanismo que se utilice para incentivar la colaboración entre integrantes.

Con el objetivo de encontrar un corpus de artículos que permitan tener una noción de la literatura académica de los modelos de confianza aplicados a MANETs, se realizó una búsqueda estructurada utilizando como palabras clave MANET, ruteo, confianza y comportamiento. Adicionalmente, se limitaron los artículos a partir del año 2009 hasta el 2019 (debido a que esta investigación se realiza en el transcurso del año 2020) y aquellos enmarcados en las áreas del conocimiento de Computación e Ingeniería. El resultado de la búsqueda consiste en un corpus de 159 artículos encontrados con la siguiente Ecuación de búsqueda en SCOPUS el día 17 de Mayo de 2020.:

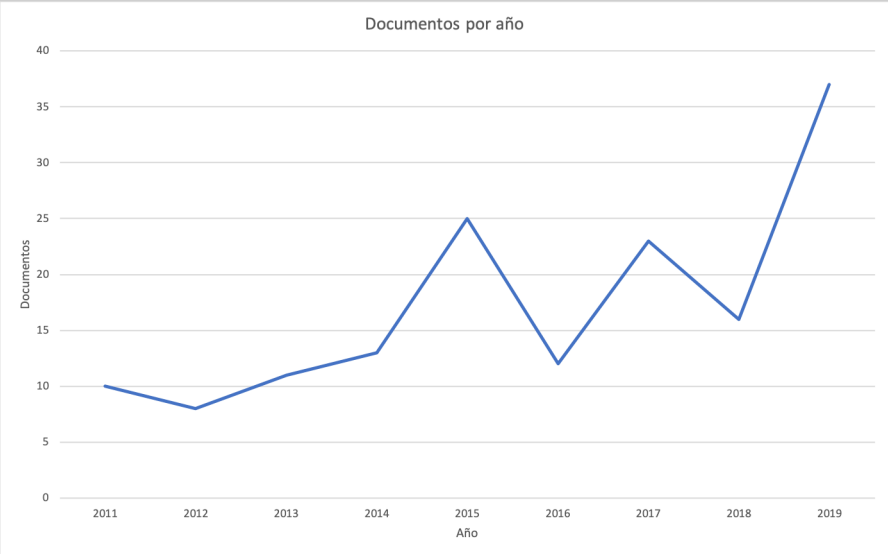

Figura 3-1: Publicaciones por año según ecuación de búsqueda utilizada en SCOPUS el día 17 de Mayo de 2020. Adaptado de la información de SCOPUS.

((TITLE-ABS-KEY (“MANET” .and. “behavior”) AND PUBYEAR >2009) AND ((routing)) AND (trust)) AND (LIMIT-TO (SRCTYPE , “j”) OR LIMIT-TO (SRCTYPE , “k”) OR LIMIT-TO (SRCTYPE , “b”)) AND (LIMIT-TO (SUBJAREA , “COMP”) OR LIMIT-TO (SUBJAREA , “ENGI”)) AND (LIMIT-TO (DOCTYPE , “ar”)) AND (LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014) OR LIMIT-TO (PUBYEAR , 2013) OR LIMIT-TO (PUBYEAR , 2012) OR LIMIT-TO (PUBYEAR , 2011)) AND (LIMIT-TO (LANGUAGE , “English”))

En la figura **3-1** se observa la cantidad de artículos publicados por año y se aprecia el incremento de la relevancia de este tema en la literatura, como se puede ver el mayor número de publicaciones se hizo el último año (2019). El 2020 no se consideró ya que era el año en curso en el momento de la búsqueda y no se puede tener en cuenta aún para los análisis cuantitativos. En la Figura **3-2** se ve la distribución por áreas del conocimiento del corpus de artículos seleccionados, donde se muestra que la mayoría se encuentran ubicados en Ciencias de la Computación e Ingeniería. Cabe resaltar que hay un porcentaje de 1,8 % que involucra a las ciencias sociales (4 artículos), cuyos artículos representan investigaciones académicas orientadas a métodos social-inspirados aplicados a redes auto-organizantes.

Es importante mencionar las características de las redes ad-hoc que el modelo de confianza tendrá para funcionar de manera consistente y confiable. Estas consideraciones son: descono-

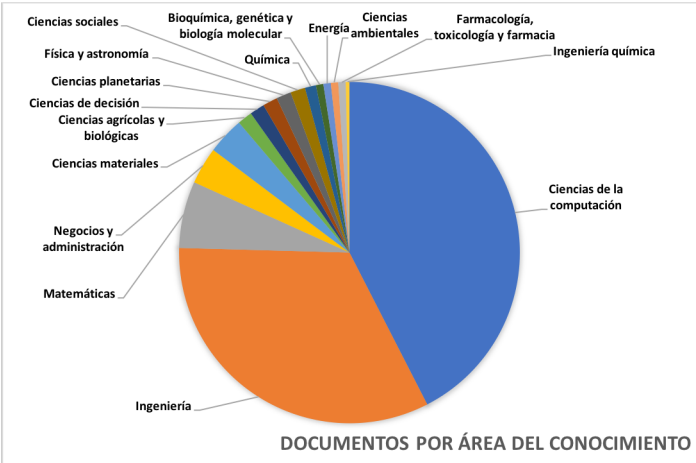

Figura 3-2: Publicaciones por área del conocimiento según ecuación de búsqueda utilizada en SCOPUS el día 17 de Mayo de 2020. Adaptado de la información de SCOPUS.

cimiento de la red, la posibilidad de presencia de nodos egoístas, seguridad de la información, conectividad y estabilidad de la red que implica un error no controlable en las interacciones. Cada una de estas se describe a continuación.

- **Desconocimiento de la red:** Es un campo de la programación basada en agentes, denominado ”problema de visión parcial”, donde los agentes solo tienen acceso a una parte de la información del sistema y esto dificulta la toma de decisiones de cada agente [56].

- **La posibilidad de presencia de nodos egoístas:** En este tipo de redes, en las cuales cada uno de sus integrantes tiene la misma jerarquía que todos los demás, es importante evitar a los participantes que buscan aprovecharse de la red. A estos participantes se les denomina nodos egoístas, y existen trabajos enfocados en el manejo de este tipo de nodos [29].

- **Seguridad de la información:** La integridad de la información que se comparte en la red siempre debe ser garantizada y por la naturaleza distribuida de la red ad-hoc este es un tema que se estudia en la literatura [38, 39, 40, 16].

- **Conectividad y estabilidad de la red:** Esta es una consideración muy importante que puede afectar el funcionamiento de un algoritmo ideal implementado, ya que la posibilidad de que la conexión entre dos dispositivos falle es considerable y puede afectar los sistemas de confianza, por lo tanto este ruido o probabilidad de error se debe sobrellevar en las interacciones de los dispositivos. Este error dependerá de la calidad de la infraestructura de la red y del dispositivo mismo. En la literatura, se encuentran pocos artículos que muestren la cuantificación y consideración de este ruido dentro

Basados en reputación	Basados en créditos
CONFIDANT [11]	SPRITE [57]
CORE [34]	TOKEN [54]
SORI [21]	VCG [3]
OCEAN [7]	

Tabla 3-1: Clasificación de mecanismos para redes auto-organizantes. Adaptado de [30].

de las pruebas realizadas de los modelos. Generalmente, se asume que la conexión es ideal, con una conectividad constante y estable (lo cual no sucede en ambientes reales). Se desprecia esta probabilidad de error, pero es necesario proponer mecanismos que tengan en cuenta estos errores para poder garantizar un mejor desempeño en entornos cambiantes. La consecuencia es que las redes ad-hoc presentan estocacidad en las comunicaciones entre individuos.

A continuación, se realiza un análisis de los resultados encontrados resaltando aquellos mecanismos que pueden incentivar la cooperación dentro de la red con el fin de implementarlo posteriormente al modelo que se quiere proponer en esta tesis. Para esto, es necesario escoger un mecanismo de colaboración, estudiarlo a profundidad y validar los resultados encontrados en la literatura.

3.2. Cooperación en redes ad-hoc

La cooperación en sistemas auto-organizantes es un comportamiento emergente que necesita mecanismos complejos para comprender y estudiar los comportamientos individuales de la red. En otras palabras, la cooperación es la confianza en la red. En la literatura, se encuentra una gran diversidad de propuestas en cuanto a modelos no jerarquizados que buscan controlar el comportamiento de las redes auto-organizantes y promover la colaboración. Estos mecanismos se pueden clasificar en dos grupos: basados en reputación y basados en créditos [30]. Algunos ejemplos de protocolos se pueden observar en la Tabla **3-2**. Otro tipo de clasificación es: basadas en confianza [38, 16], las cuales usan una medida de confianza para determinar la viabilidad de participar en interacciones con un agente específico. Por otro lado, existen mecanismos enfocados en la seguridad de la información para explorar servicios de la red [38] y mecanismos de multi-ruteo [16] que ofrecen una alta tolerancia a errores.

Un proceso común en las redes ad-hoc y ampliamente usado para evaluar el desempeño de algoritmos de interacción que buscan cooperación en la red es el envío de información a través de la red, el cual consiste en transportar información (ya sean archivos, mensajes,

notificaciones o información de cualquier tipo) a lo largo de la red de un punto origen a un destino. Este proceso ofrece muchas interacciones entre los integrantes de la red, siendo un escenario ideal para monitorear la efectividad y pertinencia de los modelos propuestos en los diferentes artículos de la literatura. Este proceso de envío presenta desafíos debido a su recurrencia, movilidad constante de los integrantes de la red y la probabilidad de errores no controlados en el momento del envío. El proceso de encontrar la ruta a través de la cual se va a enviar la información en la red se denomina **ruteo** y existen diferentes protocolos en la literatura que presentan diferentes enfoques, por ejemplo, con modelos basado en demanda [2], basados en confianza y en autenticación [24]. Incluso hay una propuesta que usa algoritmos iterativos para detectar tolerancia a demoras en el ruteo [6]. También se encuentran enfoques de aprovechamiento de agentes egoístas (dispositivos que buscan aprovecharse de la red) usando ruteo oportunista [49, 22]. En la literatura, se encuentran ampliamente utilizados los mecanismos basados en confianza para modelar las interacciones entre los dispositivos tomando diferentes indicadores de referencia como: información autenticada [24], información entregada de forma segura [2], demoras reducidas [6], entre otras.

3.3. Modelos de confianza

Teniendo en cuenta que el objetivo de esta tesis es obtener confianza en la red y que dicho comportamiento es emergente, es necesario entender cómo se puede lograr la emergencia de un comportamiento específico en una red, particularmente de la confianza. En este caso es pertinente utilizar los sistemas multi-agente (definidos en la sección 2.4) como abstracción de la red para poder estudiar los comportamientos resultantes. En estos sistemas existen estrategias básicas enfocadas a la confianza, estudiadas en teoría de juegos (sección 2.5), que utilizan poca memoria y mecanismos sencillos para mantener un buen rendimiento con resultados aceptables. Las estrategias más relevantes se definen y comparan en términos de eficacia en [14], donde la estrategia “Tit-for-tat” (descrita en la Sección 2.5.3) es la que mejores resultados obtiene [14]. Es evidente que esta es una estrategia sencilla que emplea reciprocidad en sus interacciones y que no requiere una cantidad de memoria grande. Existen modelos más complejos que buscan identificar nodos egoístas que intentan aprovecharse de la red en términos de recursos, información u otros aspectos de la red, por ejemplo el enfoque de detectar intrusos en la red a través de data-mining [36]. Por otro lado, un trabajo de 2018 propone un modelo basado en agentes que mejora la seguridad en la red [10], un modelo para la detección y manejo de nodos egoístas [29], un enfoque de adaptación a nodos egoístas para obtener mejores resultados en el ruteo a través de una estrategia de computación evolutiva [32], un modelo similar enfocado en la movilidad de la red [44] y finalmente un modelo que utiliza ”clustering” [4]. Todos estos modelos propuestos están enfocados a obtener resultados a largo plazo en la red ad-hoc.

Algunas alternativas a los modelos de confianza presentados en la literatura son:

- Un modelo basado en fidelidad como el propuesto por Sarah [46], el cual parte de las escalas de confianza entre vecinos, pero se diferencia de los modelos explicados en que la actualización de la confianza se realiza a través de un sistema de denuncias y recomendaciones. Al ser una derivación del modelo de confianza principal, este mecanismo es menos encontrado en la literatura.

- Existe otro enfoque para la solución del envío de paquetes a través de la red, que es el problema que se intenta solucionar a través de la confianza. Las meta-heurísticas sirven para explorar varias soluciones y encontrar así la mejor opción entre las exploradas. Ejemplos de este método se encuentran en [28], que utiliza un algoritmo de múltiples restricciones en calidad de servicio, y en [48] que utiliza como meta-heurística el algoritmo de colonias de hormigas.

3.4. Clasificación y comparación cualitativa de modelos de confianza

Dentro del contexto de las redes ad-hoc hay una consideración importante en cuanto a su infraestructura de software y hardware. Debido a que esta red es distribuida y auto-organizada, se deben tener en cuenta los cambios constantes de ubicación de los integrantes de la red, ya que la proximidad entre dos integrantes es proporcional a la posibilidad de compartir información de forma rápida y confiable, pues los envíos se hacen directamente de dispositivo a dispositivo.
Existe una amplia gama de modelos propuestos con diferentes metodologías y enfoques. En esta sección se propone una clasificación y comparación de algunos modelos de confianza utilizados en redes ad-hoc.

3.4.1. Clasificación según la dimensión estudiada

Dentro del los modelos de confianza encontrados en la literatura, se tienen variaciones que permiten realizar clasificaciones como se propone en [55]. Esta clasificación consiste en dividir en 4 criterios, como se muestra a continuación.

Confianza subjetiva y confianza objetiva

Cada participante tiene una confianza sobre los otros, que se puede entender como una opinión. Esta opinión se considera objetiva o subjetiva dependiendo del criterio sobre el cual se construye dicha opinión. Principalmente, se habla de la rigurosidad de la información proporcionada por el nivel de confianza: si la información es verificable (por ejemplo, el resultado de una ecuación matemática), entonces podemos calificar la confianza como objetiva; pero cuando su información no es verificable, se considera subjetiva (por ejemplo, cuando

se tienen escalas y un nodo considera "confiable" a otro, sin proporcionar estadísticas que sustenten dicha opinión).

Basado en transacciones y basado en opiniones

Los dispositivos tienen un nivel de confianza específico con los otros dispositivos. Esta confianza puede determinarse de dos maneras: como una estadística que determina el desempeño general de interacciones, o se puede asignar una variable que determina el nivel de confianza entre dispositivos. La diferencia entre estos dos radica en que el método basado en transacciones da un valor que viene de un porcentaje de participación equivalente a la cantidad de veces que se ha interactuado. Este método hace mas fácil comparar varios niveles de confianza entre sí de manera ponderada, por ejemplo, si un nodo solicita la opinión sobre un nodo particular, y dos nodos vecinos proporcionan su opinión. En caso de que se tenga el contraste de la opinión de un nodo que ha interactuado una vez con el nodo en cuestión, contra la opinión de un nodo que ha interactuado repetidamente con el mismo, si se utiliza el método basado en transacciones será posible darle mayor prioridad a la opinión con más experiencia pertinente para la consulta.

Información completa e información local

Esta clasificación es ampliamente usada en algoritmos de búsqueda. Se refiere a la cantidad de información a la que tiene acceso un dispositivo en el momento de realizar una búsqueda. Cuando la información esta completa, el dispositivo tiene la capacidad de explorar todas las posibilidades de búsqueda posibles. Por otro lado, existen casos (más frecuentes en la vida real) en que el dispositivo tiene acceso a la información de manera parcial. En este caso, la información se encuentra dentro de un radio de cobertura reducido y el proceso debe considerar que existe información desconocida. En el caso de los agentes de una red ad-hoc, se trabaja con información local [56].

Basado en rangos y basado en umbrales

El proceso usual de un modelo basado en confianza consiste en consultar a los vecinos sobre la confianza en un dispositivo en especial y, dependiendo del tipo de dato que se recibe, se debe tomar una decisión sobre la interacción. En cuanto a esa variable de confianza, se pueden tener dos tipos de variables. El primer tipo consta de una estadística de confiabilidad (por ejemplo 80 %). Con este tipo de datos se maneja un umbral mínimo de confianza para llevar a cabo una interacción, mientras que el segundo tipo de dato es una clasificación o rango de confianza (por ejemplo, confianza alta, media y baja).

3.4.2. Clasificación según el esquema

En [31], se describe una clasificación de modelos según las áreas de estudio en las que se basan. Dichas escuelas son la teoría de la información, confianza en redes sociales, teoría de grafos y teoría de juegos cooperativos y no cooperativos. Cada uno de estos modelos tiene mecanismos que difieren entre sí, tales como la fuente de información de confianza, la validez o peso que se le da a cada una de las opiniones recibidas y la forma en que se manejan los extraños o los dispositivos nuevos en la red. Cada uno de los mecanismo utilizados se pueden ver en la Tabla **3-2**.

3.4.3. Comparación según el esquema

Mediante la información que se tiene en la Tabla **3-2** se pueden encontrar características consistentes entre los modelos.

1. Se observa que para la recolección de información se utilizan dos fuentes principales, la experiencia individual y la recolección de opiniones de los vecinos, para finalmente tomar una decisión.

2. Con respecto al manejo de los nodos nuevos en la red, se puede ver que las estrategias tienen en común la práctica de otorgar el nivel mínimo de confianza al nodo nuevo (este valor depende de la escala que se use en el modelo) para que pueda empezar a participar en la red.

3. Se pueden ver algunas diferencias entre los modelos en la validez de opinión de los nodos. Esto se define en la función de decisión que tiene en cuenta las opiniones, pero el peso de estas opiniones puede variar.

4. La gran diferenciación entre cada uno de los modelos se ve en la calificación y ordenamiento de la información que se tiene del nodo con el que se va a interactuar.

3.5. Validación experimental de un modelo de confianza [51]

3.5.1. Modelo base: Modelo de confianza adaptativo

En las secciones anteriores se realizó una búsqueda de modelos existentes para intentar solucionar el problema propuesto en la tesis, con ese fin se selecciona un artículo particular, con el fin de validar los resultados que se muestran en este y posteriormente hacer la implementación del nuevo modelo a proponer como resultado del trabajo de tesis.

Esquema del modelo de confianza	Recolección de información		
	Fuente de información	**Validez de la opinión**	**Manejo de extraños**
Teoría de la información	Experiencia individual sobre observaciones directas. Recomendaciones solicitadas a nodos de mayor confianza a múltiples saltos que hayan tenido interacción directa con el nodo agente.	Las recomendaciones sólo se solicitan a los nodos de mayor confianza y utiliza este grado para ponderar el peso de su recomendación en la calificación.	La confianza es 0 para un nodo nuevo (en el rango [-1 ,1]) y varía de acuerdo con su comportamiento.
Redes sociales	Experiencia individual dentro del cluster. Referencias solicitadas a los presentadores entre clusters.	Utiliza certificados que son validados por los presentadores utilizando votaciones.	Entra al cluster con el mínimo nivel de confianza, el cual varía con el comportamiento.
Teoría de Grafos	Experiencia individual. Recomendaciones solicitadas a nodos confiables que hayan interactuado con el nodo agente.	En transacciones directas se recibe una credencial que contiene el nivel de confianza, en otro caso la confianza se infiere de los valores de los bordes dentro del grafo.	Los nodos nuevos tienen un nivel de confianza por defecto de acuerdo con la aplicación. Se presentan credenciales de referencia.
Teoría de juegos No Cooperativos	Experiencia individual sobre observaciones directas.	No se solicitan opiniones, la confianza se infiere de las observaciones directas.	Los nodos desconocidos tienen un valor de confianza de 1 (0-3) que varía con de su comportamiento.
Teoría de juegos Cooperativos	Experiencia individual (coopera o no en la coalición). Referencias de K nodos confiables vecinos.	Las opiniones se recogen de k nodos y se adopta el estado de confianza o no confianza por mayoría de votos	Todos los nodos se presumen confiables y dependiendo del comportamiento su estado puede variar.

Tabla 3-2: Recolección de información en modelos de confianza. Tomado de [31].

El artículo escogido apareció en 2011 [32] y consta de un modelo de confianza basado en teoría de juegos cooperativos. En este artículo se concluye que este modelo tiene cualidades adaptativas en una red cambiante. Sin embargo, es importante tener en cuenta cómo fue el proceso de pruebas para llegar a esta conclusión. En este caso, se realizó mediante la simulación de una red ad-hoc pequeña (no más de 9 nodos) realizando "torneos", que consistían en la interacción de todos vs. todos los nodos.

3.5.2. Validación de los resultados publicados

Como parte del trabajo de tesis es necesario validar los resultado presentados en el trabajo de Mejía en 2011 [32]. Con este fin, se desarrollo un ambiente de pruebas que fuera comparable con el usado en el artículo, pero con el fin de poner a prueba el algoritmo, se van a agregar algunos factores que complejizarían el proceso de adaptación para observar su comportamiento en escenarios adversos (pero posibles dentro del funcionamiento en el mundo real). También es importante remarcar cuál es la variable de control del experimento, es decir, el indicador que ayudaría a entender si el algoritmo está funcionando como se espera. Este indicador es la **confianza en la red**, la cual consiste en un porcentaje que representa la cantidad de interacciones que han sido exitosas en contraste con el total de interacciones.

Con este objetivo, se definió una simulación con 100 agentes (muchos más que los usados en el artículo) que interactúan entre sí de manera aleatoria y que después de que cada agente haya interactuado en promedio 1.000 veces podremos ver la evolución de la confianza de la red a lo largo del tiempo de ejecución. Adicionalmente, se decidió incluir un factor importante en la simulación. La probabilidad de error en cada una de las interacciones es un ruido que se introduce al sistema que debe ser considerado, pero el valor de esta probabilidad es difícil de determinar debido a que depende completamente de los dispositivos que se están usando en la red. Por esta razón, se realizarán varias simulaciones con diferentes valores de probabilidad con el fin de ver el comportamiento del algoritmo bajo diferentes condiciones.

3.5.3. Resultados obtenidos

Los resultados obtenidos en la Figura **3-3** muestran el comportamiento de la confianza de la red a lo largo del tiempo. En esta gráfica, se observa que inicialmente la confianza es baja (alrededor del 20 %), pero a medida que transcurren más interacciones se logra mejorar la confianza hasta llegar a casi el 100 % en el caso del escenario marcado con la línea azul (escenario con probabilidad de error 0 %, que es el caso ideal sin ruido del sistema). Estos resultados muestran la capacidad adaptativa esperada del modelo. Con esta información, se validan los resultados de manera exitosa [51] debido a que se logra obtener el comportamiento prometido. Adicionalmente, se logró demostrar que la adaptabilidad del modelo es capaz de sobrellevar una parte de la probabilidad de error de la red. Esto quiere decir que, a través

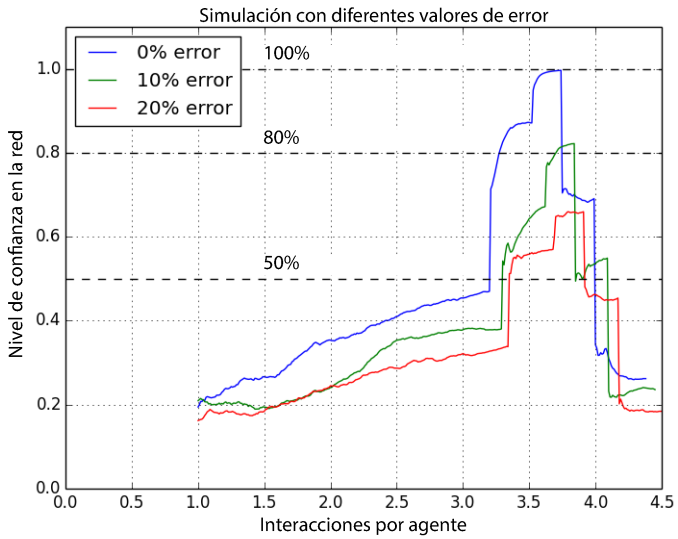

Figura 3-3: Resultados obtenidos sobre la validación del modelo de confianza. Elaboración propia.

de la adaptación del algoritmo, se puede compensar parcialmente la incertidumbre de la implementación en el mundo real. En esta tesis, se propone una mejora a este modelo validado con el fin de tener resultados más consistentes, estables y favorables en las simulaciones. Esto se puede ver en la sección 4.2.1.

3.6. Proyecto TLÖN

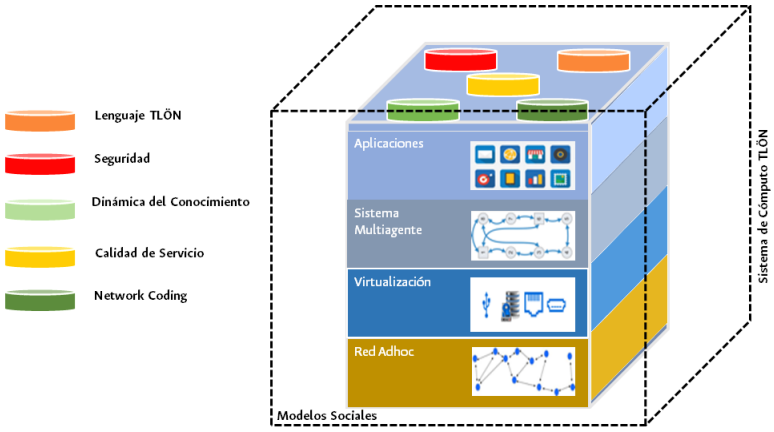

Figura 3-4: TLÖN: un modelo computacional social inspirado. Tomado de [1].

El grupo de investigación TLÖN de la Universidad Nacional de Colombia tiene como obje-

tivo el desarrollo de un proyecto que consiste en un sistema computacional social inspirado utilizando redes ad-hoc. El enfoque del grupo de investigación es crear un sistema utilizando comportamientos sociales y biológicos que permitan controlar el comportamiento descentralizado de la red. En la Figura **3-4** se observa la estructura principal del proyecto TLÖN, la cual está dividida en 4 capas y 5 ejes transversales. Esta implementación se ubicará en la capa del sistema multi-agente ya que es allí donde los diferentes integrantes de la red van a interactuar y a tomar las decisiones constantemente.

El modelo propuesto en esta tesis está enmarcado en el grupo de investigación TLÖN, particularmente en la capa de sistemas multi-agente, donde se implementará el modelo obtenido de esta investigación. Aunque las aplicaciones del modelo propuesto van más allá, ya que esta propuesta es compatible con las múltiples aplicaciones de redes ad-hoc, como por ejemplo redes de control vehiculares (VANETs), sistemas de riego, redes intra-empresariales, redes de servicios, entre muchas otras.

3.7. Conclusiones

En este capítulo se realizó una revisión de la literatura existente relacionada con el tema de modelos de confianza para redes ad-hoc. Después de encontrar numerosos documentos sobre este tema, se realizó una clasificación y comparación entre ellos con el fin de identificar las diferentes técnicas utilizadas y observar cuáles de ellas son más efectivas para este problema particular. Mediante esta comparación, se observó la metodología más prometedora, que permite reducir el enfoque de búsqueda a un algoritmo del tipo "juegos estocásticos cooperativos".

Posteriormente, se escogió un modelo que cumple con esta categoría para realizar un estudio profundo de su funcionamiento. Debido a que este artículo será tan importante para el desarrollo de esta tesis, es necesario validar que los resultados sean verídicos y además extender las pruebas ya realizadas en simulación para poner a prueba la capacidad adaptativa del algoritmo en escenarios más completos. Los resultados obtenidos son satisfactorios, ya que son consistentes con los presentados en la literatura y se procede a realizar los escenarios extendidos, relacionados con la probabilidad de error, que finalmente demostrarán que la ventaja de un algoritmo adaptativo es que puede soportar los cambios constantes de la configuración de la red ad-hoc.

4 Modelo de confianza evolutivo para lograr cooperación emergente en redes ad-hoc a través de algoritmos genéticos

4.1. Introducción

Como se describe en el capítulo 3, una red de agentes que habita un sistema distribuido como el de una red ad-hoc, necesita un modelo que tenga la capacidad de adaptarse a los cambios constantes de la población en términos de localización y de su forma de tomar decisiones. Adicionalmente, el concepto de confianza es una cualidad ideal emergente de una comunidad de agentes autónomos y lograr esta confianza emergente en la red no es un proceso simple, sino que se necesita un mecanismo complejo que mantenga la autonomía de los agentes y obtenga resultados favorables para la red como un conjunto.

Este modelo se propone para combinar los algoritmos genéticos y los juegos estocásticos aplicados a un sistema distribuido para lograr la emergencia de confianza en la red. El cual empieza con la implementación del trabajo propuesto por Mejía en 2011 [32] donde se presenta un algoritmo genético aplicado a las interacciones entre agentes en una red ad-hoc, con lo que se realiza esta implementación y a través de una simulación en un ambiente controlado se valida el funcionamiento del modelo [51]. Posteriormente se complementa el modelo con el concepto de los juegos estocásticos aplicados a la confianza de redes distribuidas de Hilbe (2018) [23]. Por último el resultado es probado en el ambiente de simulación con el fin de compararlo con el modelo inicial y que los resultados de estos experimentos muestren el comportamiento de la confianza en la red a través del tiempo.

4.2. Un modelo basado en confianza

El modelo basado en confianza consta de dos dimensiones. La primera es la confianza como un indicador del desempeño global de la red y la segunda es el nivel de confianza que cada agente tiene con los otros agentes. Esto quiere decir que cada agente tiene una calificación

para cada uno de los otros agentes. Estos dos tipos de confianza se explican a detalle a continuación.

4.2.1. Confianza en la red

En la sección 3 se presentó la pertinencia de la confianza como indicador del desempeño global de las interacciones entre los integrantes de una comunidad de entes autónomos, la cual bajo el contexto de este trabajo, se ve reflejada en las comunidades de agentes dentro del sistema de la red ad-hoc conocido como Multi-Agent System (MAS). El reto de este modelo es que a través de programación individual de agentes se logre la emergencia de confianza como un comportamiento global de la red, que sería el resultado de la complejidad de las múltiples interacciones entre los agentes. Para esto se necesita una definición formal computacional de confianza y esta se evaluará a través del proceso de envío de paquetes de información a través de la red. Cada vez que un envío se realiza, se lleva el registro de su éxito o fracaso y así se calcula la ecuación 4-1, donde se denota con C la confianza total del sistema. Donde n es la cantidad total de envíos de información que se intentaron hacer en la duración del experimento y p_i representa si el envío número i fue exitoso ($p_i = 1$) o fallido ($p_i = 0$). Con este indicador de la confianza podemos evaluar el desempeño de los diferentes modelos propuestos en esta tesis.

$$C = \frac{1}{n}\sum_{i=1}^{n} p_i \text{ con } n \in Z, n > 0, p_i \in \{0, 1\} \tag{4-1}$$

4.2.2. Nivel de confianza entre agentes

Cada uno de los agentes que habitan la red tiene un historial de actividad registrada con los otros agentes. Esta actividad puede ser una interacción previa directa entre los dos agentes, o el producto de la observación de una interacción de un agente vecino. Esto quiere decir que cuando se lleva a cabo una interacción entre dos agentes, los agentes vecinos son testigos de esta interacción y utilizan el resultado para actualizar el historial de actividad de ese agente. Esto se hace con el fin de saber en cuáles agentes puede confiar y en cuáles no, es decir, identificar la **red de confianza**, en la cual se tiene un nivel de confianza asignado a cada uno de los otros agentes. El modelo propuesto representa el nivel de confianza (NC) que tiene el agente a con el agente b en la interacción t, según la ecuación 4-2, la cual define el nivel de confianza que será utilizado por cada agente como criterio de decisión al momento de realizar una cooperación o un rechazo con otro agente.

$$NC_{a,b}(t) = \sum_{i=1}^{3} \beta_{a,b}(t - i) \text{ con } NC_{a,b}(t) \in \{0, 1, 2, 3\} \tag{4-2}$$

$$\text{Teniendo } \beta_{a,b}(t) = \begin{cases} 1 & \text{Interacción u observación } t \text{ fue exitosa} \\ 0 & \text{Interacción u observación } t \text{ fue rechazada} \end{cases} \tag{4-3}$$

4.3. Algoritmos genéticos

Los algoritmos genéticos son ejemplo de una implementación de mecanismos encontrados en sistemas biológicos para solucionar problemas computacionales, donde el objetivo es realizar una representación computacional del proceso en el cual la información de un individuo está guardada en su código genético y esta información es transmitida a las siguientes generaciones por parte de los individuos más aptos de la comunidad.

Partiendo del modelo propuesto en [32], en el cual se presenta un algoritmo genético basado en confianza que codifica la estrategia de cada agente en 16 bits (1 o 0), como se muestra en la Tabla **4-1**, donde $R = Rechazar$ y $C = Colaborar$. La decisión de utilizar 16 bits es producto de las pruebas realizadas [31] con el fin de definir dos parámetros que combinados generan los 16 bits presentados.

- **Tamaño de la memoria:** Para la definición de este parámetro, se considera importante no gastar memoria de manera innecesaria, pero así mismo, la memoria debe ser suficiente para obtener un adecuado grado de adaptabilidad [31]. El valor encontrado es de $m = 2$.
- **Valores del nivel de confianza:** El segundo parámetro se refiere a la cantidad de posibles valores que puede tener el nivel de confianza, que como se puede observar en la Tabla **4-1** son los valores enteros desde 0 hasta 3. Esta decisión se toma teniendo en cuenta 3 elementos relevantes en el modelo, como se listan a continuación.
  - Una mayor cantidad de valores, genera mayor validez y precisión de la estimación de la confianza.
  - Una menor cantidad de valores, necesitará un menor número de bits para codificar la estrategia y esto es deseable debido a que reduce la complejidad computacional en la implementación.
  - Si la cantidad es muy grande, un agente que se ha comportado de manera egoísta, tendrá dificultades para reivindicarse, debido a que cuando cambia su comportamiento, necesita una mayor cantidad de iteraciones para corregir su nivel de confianza.

El ejemplo que se muestra tiene al agente a que va a interactuar con el agente b. Si el agente b tiene por ejemplo, un nivel de confianza de tres ($NC = 3$) y en las últimas dos posiciones del

Nivel de confianza (NC)	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
Interacción t-2 ($\beta_{a,b}(t-2)$)	R	R	C	C	R	R	C	C	R	R	C	C	R	R	C	C
Interacción t-1 ($\beta_{a,b}(t-1)$)	R	C	R	C	R	C	R	C	R	C	R	C	R	C	R	C
Estrategia	**R**	**R**	**R**	**C**	**R**	**R**	**C**	**C**	**R**	**C**	**C**	**C**	**R**	**C**	**C**	**C**

Tabla 4-1: Estrategia ejemplo 0001 0011 0111 0111. Elaboración propia.

historial ha colaborado ($\beta_{a,b}(t-1) = C$, $\beta_{a,b}(t-2) = C$ siguiendo la notación de la ecuación 4-2), entonces la decisión a tomar según la estrategia será de colaborar (C). La estrategia inicial de un individuo será determinada de forma aleatoria, con el fin de que la comunidad tenga variedad de códigos genéticos y pueda empezar el proceso de adaptación que consta de dos subprocesos, el cruce y la mutación, los cuales se explican en detalle a continuación.

4.3.1. Proceso de cruce

Cada agente puede tener comunicación directa con los agentes que están en su "vecindario", esto es, un agente que este dentro de su radio de alcance como se muestra en la Figura **4-1**. Lo primero que se hace es seleccionar a los dos agentes encargados de transmitir su código genético (padres). El proceso de selección de los padres es aleatorio entre los agentes vecinos y la probabilidad de escoger cada individuo se distribuye con una función de probabilidad tal que, $\phi(a) \in [0, 1]$. Esta distribución se muestra en la ecuación 4-4, donde N representa la cantidad total de agentes en el vecindario y $fitness_j$ el puntaje del agente j que se explica en la Sección 4.4. A través de esta función, se pueden escoger los padres de forma aleatoria, donde las estrategias con mayor puntaje tendrán mayor probabilidad de ser escogidas. Una vez los dos padres son escogidos, se obtiene el código genético del hijo, mezclando los genes de los padre escogidos de forma aleatoria a través del proceso conocido en la literatura como cruce uniforme [52].

$$\phi(a) = \frac{fitness_a}{\sum_{j=1}^{N} fitness_j} \text{ con } a \in \{1, 2, \ldots, N\} \tag{4-4}$$

Cruce uniforme

Este tipo de cruce es el proceso de combinación de la información genética computacional utilizada en los algoritmos genéticos En esta se utiliza un 50 % de probabilidad de que cada gen (bit) sea escogido para heredar al hijo. Este proceso se muestra en la **Figura 4-2** con un ejemplo. Como se observa en la figura, cada una de las 16 posiciones del hijo es escogida

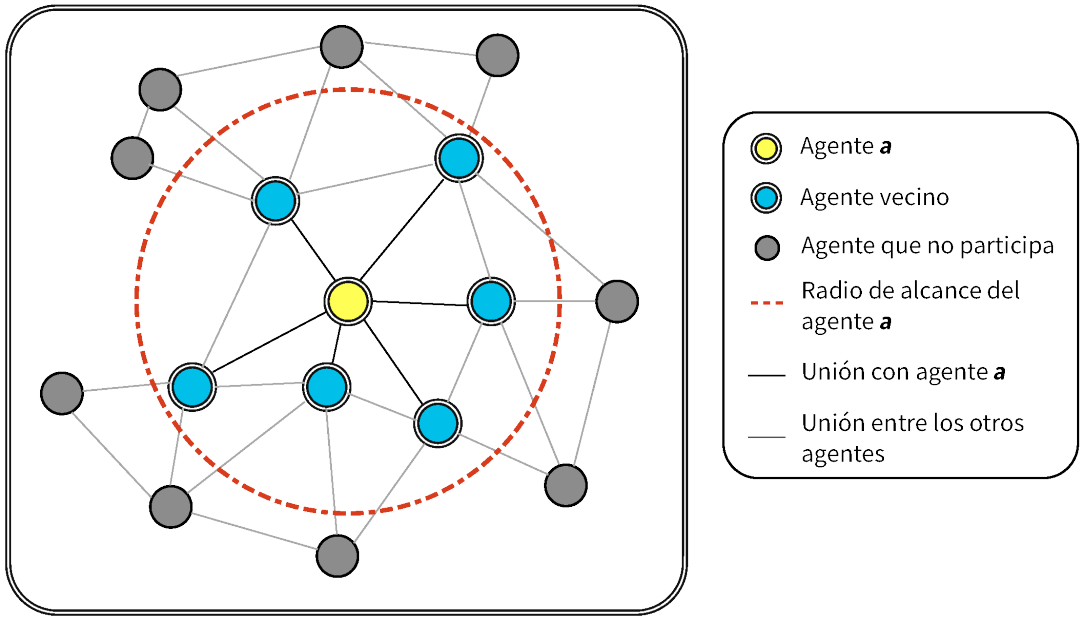

Figura 4-1: Vecindario del agente **a**. Elaboración propia.

de alguno de los dos padres con una probabilidad uniforme. Este proceso aleatorio implica que es posible que el hijo tenga más información del padre 1 que del padre 2 o viceversa.

4.3.2. Proceso de mutación

Posterior al cruce de los padres, se realiza el proceso de mutación, en el cual existe una probabilidad λ_m de que cada bit de los 16 que conforman la estrategia sea alterado (es decir que un bit pase de 1 a 0 o viceversa). Con esto se garantiza una amplia exploración de las posibles estrategias en la red. Para determinar el valor de esta probabilidad, se observa que en el modelo tomado como punto de partida [32] se utiliza un $\lambda_m 0 = 0{,}1\,\%$ asignado de manera arbitraria. No obstante, para este trabajo se utilizará la heurística $\lambda_m = 1/L$, con el fin de tener un valor efectivo y generalmente utilizado en la literatura académica [37], donde L es el tamaño de la estrategia, es decir, $L = 16$ para finalmente obtener $\lambda_m = 6{,}25\,\%$.

4.4. Adaptación

La adaptación como proceso evolutivo es un comportamiento emergente en sistemas complejos, producto de la apropiada definición de las características de los individuos que habitan la red, el cual, en el contexto computacional, depende de la forma en que se le otorgan puntos a los agentes. Estos puntos son los mencionados en la ecuación 4-4 y se representan con la función $fitness_a$. Los puntajes de cada agente son los que determinarán qué tan exitosa es

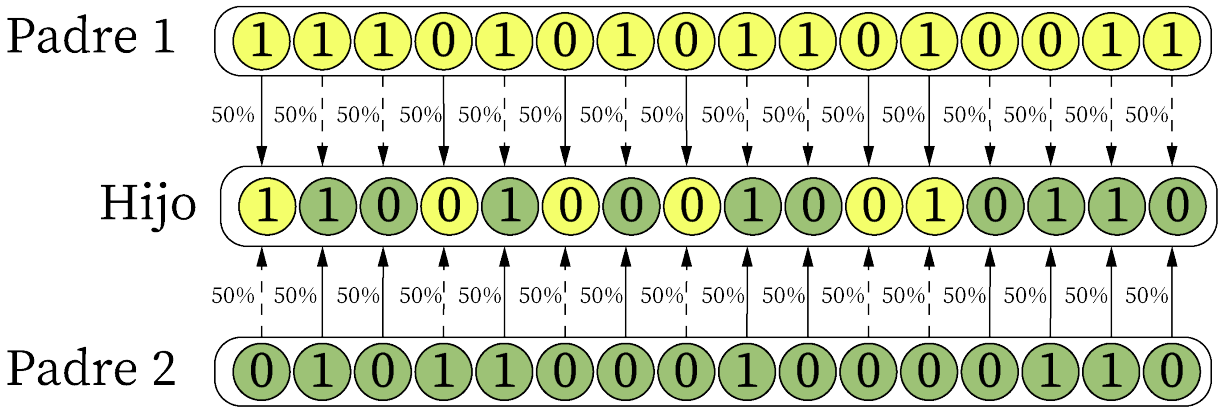

Figura 4-2: Ejemplo cruce uniforme. Elaboración propia.

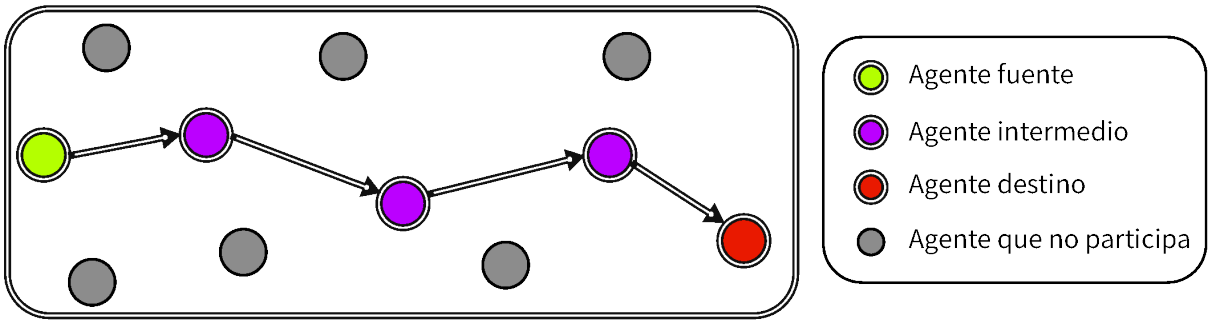

Figura 4-3: Clasificación de agentes en el proceso de envío. Elaboración propia.

una estrategia dentro de la red. La clasificación de cada agente en cada proceso de envío se observa en la Figura **4-3** y la definición de sus puntajes consta de dos partes: los pagos a los agentes fuente y los pagos a los agentes intermedios. En el caso del agente destino y los agentes que no participan, no verán afectados sus puntajes.

4.4.1. Puntaje para agentes fuente

El envío de un paquete de información a través de la red, es el proceso que se simula en el ambiente controlado para probar el desempeño de cada modelo, que inicia con un agente que necesita enviar cierta información a otro agente en la red. El agente que empieza el proceso se conoce como **agente fuente** y está representado en la Figura **4-3**. Este agente recibe puntos dependiendo del resultado final del envío de la información, donde puede o no llegar exitosamente al agente destino y, según el caso, se otorga la puntuación de acuerdo con la Tabla **4-2**.

Resultado del envío	
Éxito	5
Fracaso	0

Tabla 4-2: Tabla de pagos para el agente fuente. Elaboración propia.

Decisión	Cooperar	Rechazar
Cooperar	(A,A)	(B,C)
Rechazar	(C,B)	(D,D)

Tabla 4-3: Tabla de pagos dilema del prisionero. Elaboración propia.

4.4.2. Puntajes para agentes intermedios

Los agentes intermedios interactúan con el agente fuente para decidir si van a cooperar o a rechazar el envío de la información y por cada interacción reciben un pago correspondiente a la Tabla **4-4**. Cada interacción enfrenta a dos agentes que tienen estrategias propias. Este proceso puede representarse con el **dilema del prisionero**, el cual es ampliamente usado en la literatura académica para representar el problema de cómo los intereses individuales afectan los resultados globales de una comunidad. El dilema del prisionero tiene una tabla de pagos que muestra las implicaciones de cada decisión que toman los participantes y su estructura se muestra en la Tabla **4-3**.

Es necesario aclarar que, a diferencia del dilema del prisionero expuesto en el capítulo 2, la tabla del dilema presenta pagos a modo de incentivo, lo que quiere decir que se busca maximizar la cantidad de pagos recibidos. En cambio, en la tabla clásica del dilema se tienen años de prisión a pagar, por lo tanto, se busca minimizar estos puntos. Por otro lado, se tiene la desigualdad 4-5 que mantiene el equilibrio entre las recompensas dadas en cada resultado. Existen muchas variaciones en los pagos de las tablas del dilema del prisionero, pero es importante mantener una coherencia en los valores, esto es, que la mayor recompensa individual se obtiene al traicionar al otro agente (C) y la menor al ser traicionado (B). Igualmente la desigualdad 4-6 garantiza que el mayor beneficio global se obtiene cuando los dos agentes interactuantes cooperan y no cuando uno traiciona a otro.

$$C > A > D > B \tag{4-5}$$

$$2A > B + C \tag{4-6}$$

Las ecuaciones 4-5 y 4-6 garantizan que la cooperación sea premiada y que la traición a pesar

	Nivel de confianza con agente fuente			
	NC=3	NC=2	NC=1	NC=0
Cooperar	3	5	1	0
Rechazar	0	1	5	3

Tabla 4-4: Tabla de pagos para interacciones intermedias. Elaboración propia.

de tener un beneficio individual, será menos beneficioso en términos globales. La aplicación de este concepto se ve reflejado en la tabla de pagos del escenario de simulación que usará en los modelos. Como se ve en la Tabla **4-4**, en este caso se tiene que $A = 3, B = 0, C = 5, D = 1$, cumpliendo con las desigualdades dadas en las ecuaciones 4-5 y 4-6.

4.5. Errores no controlados

En el contexto de las redes ad-hoc se deben considerar las condiciones de operación que pueden afectar los procesos de envío: la movilidad, la entrada y salida de agentes constantes a la red (considerados en el ambiente de simulación) y finalmente la probabilidad de errores externos a la red. Estos errores corresponden a condiciones que afectan las decisiones de los agentes de colaborar o rechazar una interacción. Por ejemplo, si un agente ha decidido colaborar con otro, pero la interacción se ve interrumpida por una falla en la conectividad o porque el equipo no tiene los recursos necesarios para continuar en la red (como sería el caso si se queda sin batería), en la simulación se incluye esta probabilidad de error mediante un parámetro denominado e que va a tomar los valores de 0 %, 10 % y 20 %.

4.6. Entropía

La entropía es la medida del desorden de un sistema y la forma de medirla difiere entre las diferentes áreas del conocimiento, ya sea la termodinámica o la teoría de la información. Comúnmente se representa con la letra H y puede tomar valores entre cero y uno. Para Claude Shannon, la entropía en el contexto de la teoría de la información es la tasa de generación de información por parte de un sistema [47]. Esto responde a la pregunta de: ¿Qué tanta incertidumbre hay sobre el resultado de un proceso específico?. Por ejemplo, en el lanzamiento de una moneda justa se tiene un 50 % de probabilidad en cada resultado y esto supone el valor máximo de entropía posible ($H = 1$). Sin embargo, en el caso de un proceso en el que estamos completamente seguros del resultado, es decir, que tenemos un 100 % de probabilidad sobre un resultado, tendríamos ausencia de incertidumbre, por lo tanto, la entropía es nula ($H = 0$).

La ecuación general de la entropía (4-7) permite calcular la incertidumbre de un evento

específico. Para la simulación definida en este capítulo, dicho evento es la interacción entre dos agentes.

$$H_k = \sum_{j=1}^{N} \theta_j \log_2 \left(\frac{1}{\theta_j} \right) \text{ con } H, \theta_j \in [0, 1] \tag{4-7}$$

donde N es la cantidad de resultados posibles de la interacción que sabemos que son cooperar y rechazar, es decir, que $N = 2$. Por otro lado, θ_j es la probabilidad de que suceda el evento j que se explica en la ecuación 4-10 y H_k representa la entropía de la interacción número k en el proceso de envío. A su vez, para hallar la entropía de un proceso de envío (H_{env}) se utilizará la ecuación 4-8.

$$H_{env} = \frac{1}{N} \sum_{k=1}^{N} H_k \tag{4-8}$$

donde N es la cantidad de interacciones que hay en un proceso de envío, es decir, la cantidad de agentes intermedios que hay en la ruta (Figura **4-3**). Finalmente, la entropía total del sistema (H) es igual al promedio de las entropías de los envíos realizados durante la simulación (ecuación 4-9) con N como la cantidad de envíos realizados durante la simulación.

$$H = \frac{1}{N} \sum_{env=1}^{N} H_{env} \tag{4-9}$$

Esta medida de incertidumbre es un indicador que se utilizará para entender el comportamiento de los algoritmos probados en la red. Para aplicarlos se necesitan las probabilidades de que suceda cada interacción, para así poder reemplazar los valores de la ecuación 4-7. Estas probabilidades se asignarán dependiendo del nivel de confianza del agente intermedio con el agente fuente siguiendo la ecuación 4-10.

$$\theta_j = \frac{NC}{3} \text{ con } NC \in \{0, 1, 2, 3\}, \theta_j \in \{0, \frac{1}{3}, \frac{2}{3}, 1\} \tag{4-10}$$

4.7. Ambiente controlado de simulación

En esta sección se define un entorno de simulación en el cual se pueden poner a prueba los modelos que se proponen en este trabajo de tesis para así poder compararlos. Para esto, se necesita un software especializado en la simulación basada en agentes, que permita realizar los experimentos y que pueda soportar la complejidad de la red que está conformada por los agentes con el modelo basado en confianza. Por estas razones, se decidió utilizar Netlogo, que cumple con todas las condiciones mencionadas previamente y además ha sido ampliamente usado en estudios de simulación basada en agentes, incluyendo el trabajo que se revisa en la

sección 4.3 [32].

En el modelo de simulación se incluyen 100 agentes que conforman la red y se definen 3 tipos de agentes que se denominarán: agentes egoístas, agentes genéticos y agentes estocásticos (los cuales serán explicados más adelante en la sección 4.8). Los agentes egoístas son aquellos que nunca van a cooperar en una interacción y solamente participan cuando ellos son el agente fuente (para beneficio propio). Los agentes genéticos son aquellos que utilizan el modelo de algoritmos genéticos según la descripción dada en la sección 4.3.

Debido al alto costo computacional que conlleva estas simulaciones y los recursos disponibles para la realización de esta tesis, se realizará un total de 50 corridas por cada uno de los escenarios de simulación propuestos. Con el fin de garantizar la rigurosidad estadística de los resultados, se utilizará el método denominado ***bootstraping***, el cual se explica a continuación.

Bootstraping

Es un método estadístico no paramétrico de remuestreo que se basa en el teorema del límite central [15]. Consiste en tomar una muestra inicial de n elementos que siguen una distribución desconocida. Posteriormente, se escoge una nueva muestra con n elementos de manera aleatoria a partir de los datos de la muestra inicial (muestreo aleatorio con reemplazo). De esta nueva muestra se mide la media. Este proceso se repite una gran cantidad de veces para finalmente tener un conjunto de medias. A partir de este conjunto, se pueden sacar los estadísticos necesarios. Debido al teorema del límite central, este conjunto de datos sigue una distribución normal y gracias a esto se puede utilizar un intervalo de confianza del 95 % utilizando la media y la desviación estándar multiplicada por la constante 1,96.

Este es un método valioso para el análisis de información de salida de simulaciones [15] y por esa razón es apropiado para esta tesis. Como se mencionó previamente, la muestra inicial de cada escenario es de 50 corridas. El *bootstraping* se aplicará a esta muestra 1.000 veces y a partir de los 1.000 datos obtenidos se generan la media y los intervalos de confianza del 95 %.

4.7.1. Formato de resultados de las simulaciones

Los resultados de las simulaciones realizadas como parte de este trabajo de tesis ofrecen los valores de confianza y entropía a lo largo del tiempo de simulación. Debido a estas características, no se puede dar un valor de desviación estándar definitivo para una simulación, en cambio debe tenerse el valor de desviación estándar de cada uno de los puntos de la gráfica. Por esa razón, se decidió incluir en las gráficas tanto la media de los datos obtenido como el umbral que contiene los resultados obtenidos con un 95 % de confianza. Esto se puede observar en la Figura **4-5** donde las líneas continuas son la media y las franjas semitransparentes

son los intervalos de confianza.

4.7.2. Escenario de simulación

Para la simulación se deben tener en cuenta principalmente dos factores para que el modelo pueda ser evaluado en las condiciones adecuadas. Estos factores son el constante cambio de la población y los posibles errores inesperados en la red (como se definió en la sección 4.5). Cada vez que suceden en promedio 1000 interacciones por agente, se hace la transición entre etapas, lo que significa que al final de la simulación se tendrá un promedio de 5000 interacciones por agente.

Se aclara que en los escenarios van a convivir los agentes egoístas con los agentes con algoritmo, es decir, los agentes genéticos o estocásticos (no se combinan agentes genéticos con los estocásticos). Se definen 5 etapas en las cuales se va a variar la población de agentes egoístas y genéticos/estocásticos como se muestra en la Tabla **4-5**. En esta tabla se observa que la simulación comienza con la mitad de la población de agentes con algoritmo y la otra mitad de agentes egoístas, posteriormente, se modifica la población aumentando la cantidad de agentes con algoritmo. Con el 30 % de la población que cambia, lo que sucede es que estos agentes "mueren" y se genera un agente nuevo (sin memoria previa) con la estrategia correspondiente. De esta manera, siempre se mantiene una población total de 100 agentes en la simulación, y así sucesivamente en cada cambio de población por etapa.

En la simulación se tiene un elemento adicional de las simulaciones que tiene como objetivo incluir la posibilidad de movimiento de los agentes, teniendo en cuenta que en las redes adhoc se pueden tener dispositivos móviles como celulares o sensores portátiles. Con este fin, al finalizar la interacción los agentes se mueven en una distancia aleatoria hacia una dirección aleatoria, lo cual evidentemente modifica la distancia que tiene a los agentes vecinos. Por otro lado, la probabilidad de errores, como se definió en la sección 4.5, se implementará en cada simulación con diferentes valores, con el fin de ver el desempeño de los algoritmos. La primera implementación del modelo propuesto se hará usando el escenario de simulación definido con 3 niveles de error y los resultados se muestran en las Figuras **4-5** y **4-6**.

En al Figura **4-4** se observa un resumen del modelo con todos los elementos considerados en la simulación realizada. Se tienen en cuenta los tipos de agentes que participan en las interacciones, el error introducido al sistema y los indicadores medidos a lo largo de la simulación.
La Figura **4-5** muestra en el eje Y el comportamiento del nivel de confianza de la red (Sección 4.2.1) y en el eje X la cantidad promedio de interacciones por agente. Cada una de las etapas descritas en la Tabla **4-5** sucede cada 1000 interacciones. Los resultados muestran

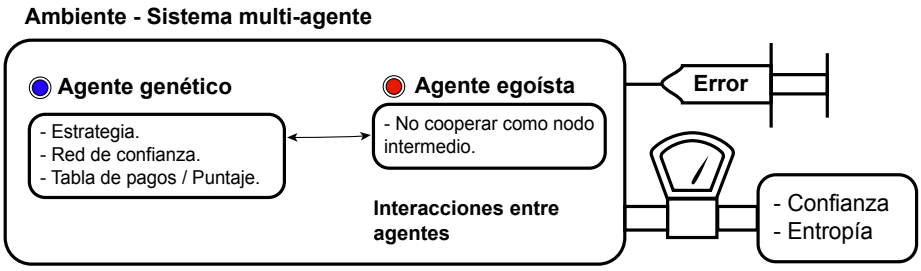

Figura 4-4: Modelo completo de agentes genéticos.

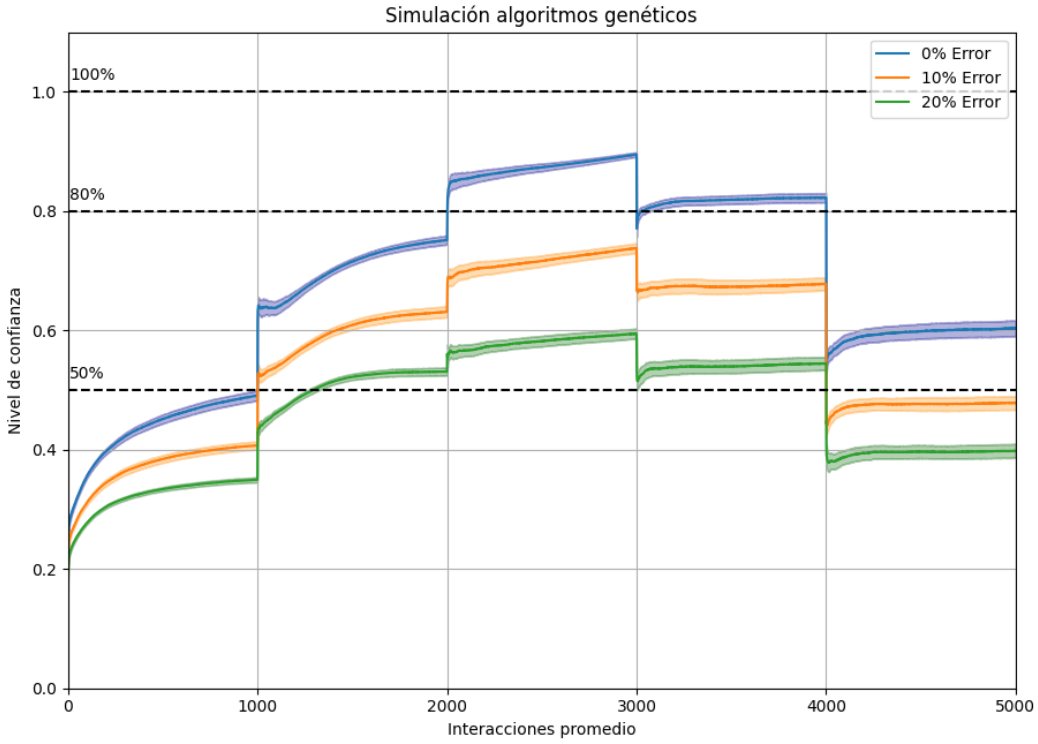

Figura 4-5: Resultados: Confianza modelo algoritmo genético con interacciones promedio. Elaboración propia.

Etapa	Población agentes con algoritmo	Población agentes egoístas
1	50 %	50 %
2	80 %	20 %
3	100 %	0 %
4	80 %	20 %
5	50 %	50 %

Tabla 4-5: Etapas de la simulación. Elaboración propia.

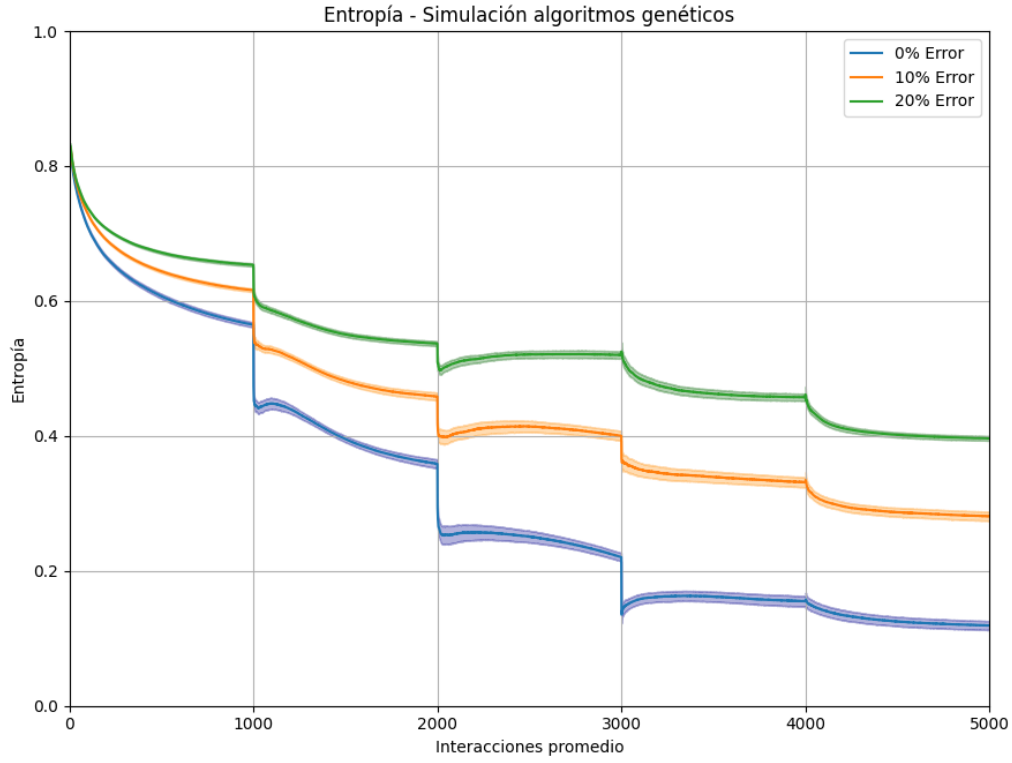

Figura 4-6: Resultados: Entropía modelo algoritmo genético con interacciones promedio. Elaboración propia.

que la cantidad de agentes egoístas y de porcentaje de error condiciona el desempeño de la confianza de la red. Sin embargo, el algoritmo genético logra adaptarse a la red y mejorar la confianza a medida que pasa el tiempo. El algoritmo genético demuestra su capacidad de adaptación sin importar la cantidad de error que haya en la red. Sin embargo, la velocidad de adaptación es notablemente lenta, lo cual es un problema, ya que es posible que antes de que el algoritmo logre adaptarse a la red, esta cambie de nuevo y el proceso deba volver a empezar. Por esta razón, es necesario mejorar la velocidad de adaptación del modelo y como respuesta a esta necesidad se presenta el modelo final de esta tesis, que implementa el concepto de los juegos estocásticos para complementar los algoritmos genéticos.

En cuanto a la entropía, como se observa en la Figura **4-6** el sistema empieza con una entropía elevada, debido a que al principio los agentes no saben si deben confiar o no en los otros y a medida que pasa el tiempo, los agentes aprenden de la red y reducen la incertidumbre en los procesos de envío. Esto no significa que siempre van a tener éxito, sino que saben cuales agentes generalmente cooperan y cuales no. Además, se ve el efecto del error en la entropía, lo cual es acorde con lo esperado, debido a que este error es una entropía adicional inyectada al sistema.

4.8. Juegos estocásticos

En [23], se hace una exploración sobre la aplicación de juegos estocásticos en dilemas sociales tales como el dilema del prisionero iterado y el juego de los bienes públicos, con el fin de que la cooperación emerja del sistema rápidamente. Los juegos estocásticos son un modelo del estudio de Teoría de Juegos, que se encarga de abordar aquellos problemas que involucran la interacción de más de un individuo y la decisión de cada individuo, lo cual afecta el bienestar de los otros [35]. Los juegos estocásticos constan de etapas o estados que cambian constantemente dependiendo de las decisiones que se toman durante el "juego" [33], que en este contexto el juego se refiere al momento en que dos agentes interactúan (dilema del prisionero). La aplicación del concepto de juegos estocásticos en el dilema del prisionero consta de 2 estados [23] que se muestran en la Figura **4-7**, en la cual se muestran los 2 estados posibles del sistema, que se denominan **juego 1** y **juego 2**. Las transiciones entre estados o juegos dependerá de los resultados de las interacciones, como se muestra en la Figura **4-7**. En esta figura se evidencia que si los 2 agentes involucrados en el juego cooperan, pasarán a jugar el **juego 1** (el más favorable) y en el otro caso (es decir, si solo uno coopera o ninguno coopera) jugarán el **juego 2**.

4.8.1. Interacciones entre agentes intermedios

La definición de estos dos juegos se basa en el hecho de que el **juego 1** es más beneficioso que el **juego 2**, es decir, siguiendo la notación de la Figura **4-7** se tendrá que $b_1 > b_2$, utilizando

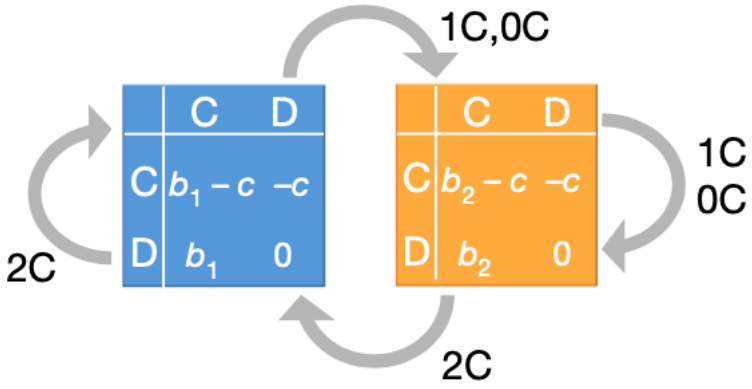

Figura 4-7: Tablas de pagos con juegos estocásticos. Tomado de [23].

	Nivel de confianza con agente fuente			
	NC=3	NC=2	NC=1	NC=0
Cooperar	4	6	0	-2
Rechazar	-2	0	6	4

Tabla 4-6: Tabla de pagos para interacciones intermedias en el juego 1. Elaboración propia.

el modelo de tablas de pagos definido anteriormente en la Tabla **4-3**, y además se deberá cumplir con las condiciones definidas en las desigualdades 4-5 y 4-6. Se define que los valores a utilizar serán de $b_1 = 6$, $b_2 = 4$ y $c = 2$ para los valores en la Figura **4-7**, lo cual significa que según la Tabla **4-3** se tienen valores de $A = b_{1\vee2} - c$, $B = -c$, $C = b_{1\vee2}$ y $D = 0$. Las tablas de pagos que se definieron anteriormente deben modificarse para cumplir con estas nuevas definiciones. Los nuevos sistemas de pagos se describen en la Tabla **4-6** para el **juego 1** y en la Tabla **4-7** para el **juego 2**.

	Nivel de confianza con agente fuente			
	NC=3	NC=2	NC=1	NC=0
Cooperar	2	4	0	-2
Rechazar	-2	0	4	2

Tabla 4-7: Tabla de pagos para interacciones intermedias en el juego 2. Elaboración propia.

Resultado del envío	
Éxito	6
Fracaso	0

Tabla 4-8: Tabla de pagos para el agente fuente en el juego 1. Elaboración propia.

Resultado del envío	
Éxito	4
Fracaso	0

Tabla 4-9: Tabla de pagos para el agente fuente en el juego 2. Elaboración propia.

4.8.2. Interacciones con el agente fuente

En el caso del agente fuente se hace una modificación en la tabla de pago que también dependerá del juego que se encuentre activo, como se puede observar en las Tablas **4-8** (para el juego 1) y **4-9** (para el juego 2). Estos puntajes muestran que las consecuencias de cambiar de un juego a otro afectan directamente el puntaje del agente fuente.

4.8.3. Transiciones de juego

Durante el proceso de definición de este modelo surgió una pregunta relevante: ¿El resultado de la interacción de dos agentes que pertenecen a una comunidad debería afectar los juegos activos de los dos agentes o de toda la comunidad? Esta pregunta es relevante porque la decisión que se tome puede afectar los resultados de una manera no predecible. Por lo tanto, se decide que se generarán ambos casos del modelo y el funcionamiento de cada uno se explica detalladamente a continuación.

Juegos estocásticos globales

En este caso particular del modelo, se considera que el resultado de cada interacción modificará el juego activo de todos los integrantes de la comunidad de agentes, lo que quiere decir que hay una relación directa entre las decisiones tomadas por los individuos y las consecuencias sobre toda la red.

Juegos estocásticos individuales

El otro caso a tener en cuenta es una versión en la cual el resultado de la interacción de dos agentes modifica el juego activo solamente de los dos agentes que participaron en la interacción. De esta manera, las consecuencias son locales, es decir, las puntuaciones dependerán

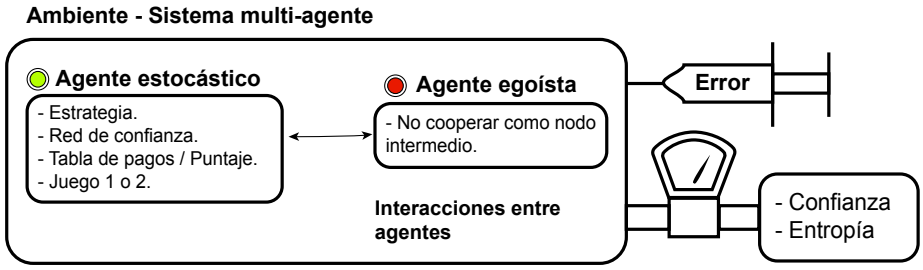

Figura 4-8: Modelo completo de agentes estocásticos.

del agente y de los agentes con los que interactúa.

En al Figura **4-8** se observa un resumen del modelo similar al presentado con agentes genéticos (Figura **4-4**). Se tienen en cuenta los tipos de agentes estocásticos como se presentaron en esta sección junto con el error introducido al sistema y los indicadores medidos a lo largo de la simulación.

4.9. Simulación final

Como etapa final de la definición y validación del modelo se realizan las simulaciones que mostrarán el comportamiento de los 3 modelos descritos (algoritmos genéticos, juegos estocásticos globales e individuales). Adicionalmente, se tienen los 3 posibles valores de error (0 %, 10 % y 20 %) para un total de 9 simulaciones y sus resultados se organizan como se muestra en la Tabla **4-10**. De esta manera, se puede comparar el desempeño de los modelos bajo condiciones similares de funcionamiento.

En la Figura **4-9** se observa el escenario ideal, en el cual no existe el error no controlado. En la figura se evidencia el buen resultado obtenido previamente por los algoritmos genéticos (verde) junto con los últimos modelos propuestos, donde los dos modelos de juegos estocásticos tienen un comportamiento estadísticamente indistinguible entre sí. Sin embargo, se muestra una evidente mejora en la velocidad de adaptación con respecto a los genéticos. Principalmente, en la primera etapa de la simulación se logra casi un 10 % de confianza adicional.

En cuanto a la entropía (Figura **4-10**) también se evidencia una diferencia notable entre el modelo genético y los de juegos estocásticos (indistinguibles entre sí). Para este indicador, el valor es menor en los modelos estocásticos, lo que significa que la incertidumbre sobre el resultado de las interacciones se reduce más rápido con estos modelos. En otras palabras, los agentes están aprendiendo más rápido en quién confiar y en quién no. Sin embargo, la entropía converge en resultados similares al final de la simulación, es decir, que la ventaja

Parámetros de las simulaciones			Indicador	
Simulación	Error	Modelos	Confianza	Entropía
1	0 %	Algoritmos genéticos Juegos estocásticos global Juegos estocásticos individual	Figura **4-9**	Figura **4-10**
2	10 %	Algoritmos genéticos Juegos estocásticos global Juegos estocásticos individual	Figura **4-11**	Figura **4-12**
3	20 %	Algoritmos genéticos Juegos estocásticos global Juegos estocásticos individual	Figura **4-13**	Figura **4-14**

Tabla 4-10: Etapas de la simulación. Elaboración propia.

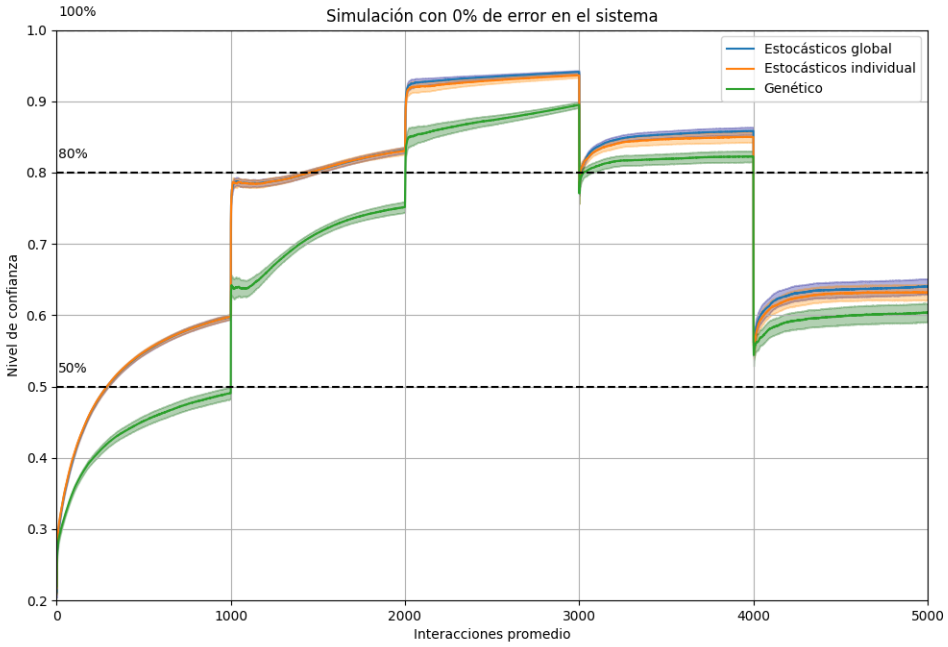

Figura 4-9: Resultados en confianza de los modelos con 0 % de error. Elaboración propia.

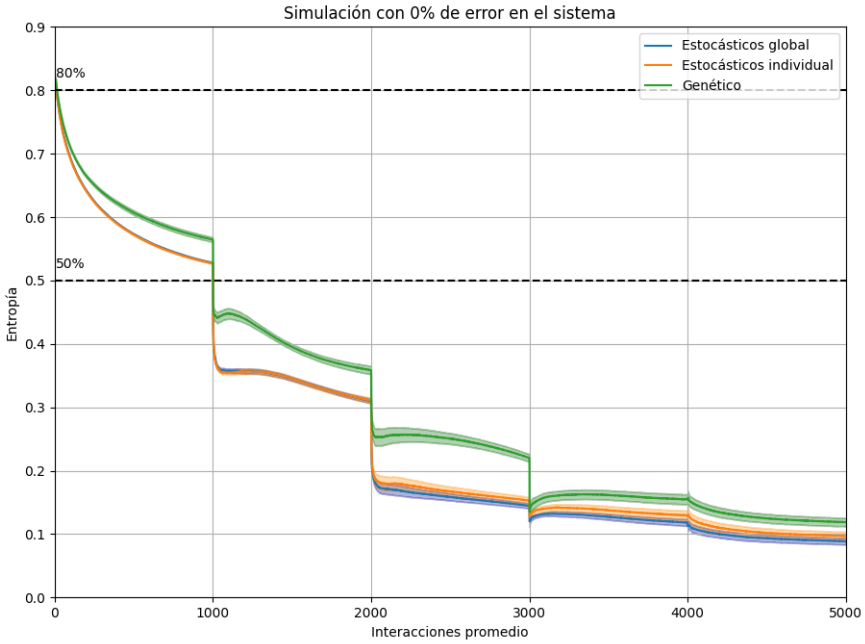

Figura 4-10: Resultados en entropía de los modelos con 0 % de error. Elaboración propia.

obtenida es en la velocidad de adaptación para posteriormente converger al mismo punto.

La segunda simulación introduce un porcentaje de error no controlado del 10 % y como se observa en la Figura **4-11** el modelo genético alcanza una confianza máxima del 75 % aproximadamente, que es menor en comparación con el escenario sin error. A pesar del error inyectado, los juegos estocásticos todavía logran mejores resultados que los algoritmos genéticos, ya que alcanzan hasta un 80 % de confianza en la tercera etapa de la simulación, lo que indica que la mejora en la velocidad de adaptación se mantiene. Con estas condiciones se empieza a evidenciar una separación entre el modelo estocástico global y el individual a partir de la etapa 4, donde los juegos estocásticos globales mantienen mejores resultados que los individuales. Esto sugiere que la interpretación global del modelo maneja mejor los errores externos al sistema.

La entropía (Figura **4-12**) en el escenario con 10 % de error aún muestra una ventaja para los juego estocásticos sobre el modelo genético, sin embargo, esta ventaja tiende a disminuir a medida que avanza la simulación. De manera general, los valores de la entropía disminuyeron con respecto al escenario sin error externo, esto se debe a que este error inyectado es en esencia entropía inyectada al sistema.

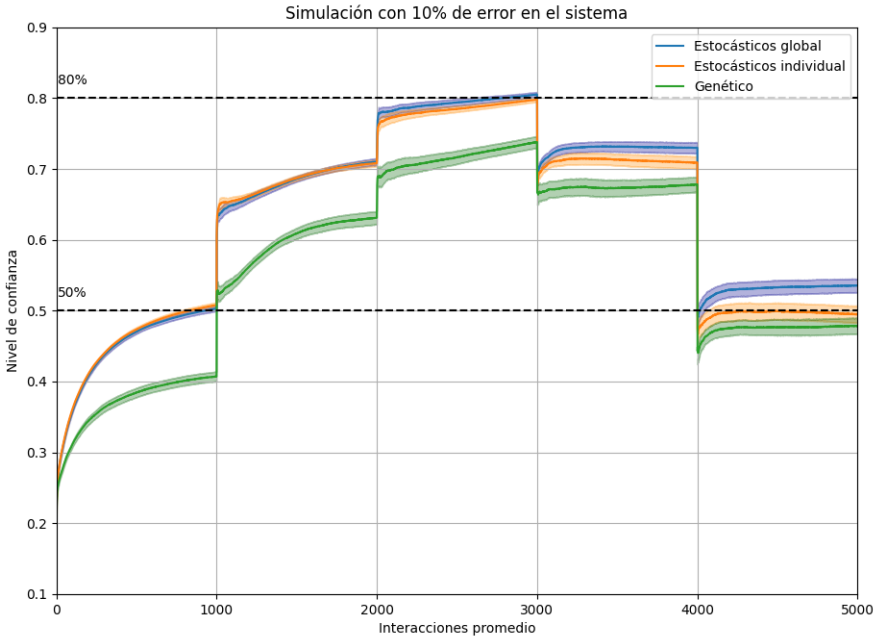

Figura 4-11: Resultados en confianza de los modelos con 10 % de error. Elaboración propia.

Finalmente, los resultados de la confianza en el escenario con mayor error externo (20 %) se muestra en la Figura **4-13**. Allí se observa que la ventaja en la velocidad de adaptación de los modelos estocásticos persiste. Sin embargo, durante la etapa 5, los 3 modelos tienen sus intervalos de confianza traslapados entre sí. También se tiene la ligera ventaja del modelo estocástico global sobre el individual, como se manifiesta en las etapas 3 y 4. Es evidente que un 20 % de error afecta a todos los modelos considerablemente.

La entropía en este escenario con 20 % de error (**4-14**) tiene resultados muy similares para todos los modelos durante toda la simulación. Es interesante observar cómo los modelos estocásticos logran mejores resultados de confianza en las primeras etapas, a pesar de manejar los mismos valores de entropía durante toda la simulación. Esto demuestra la capacidad de los juegos estocásticos para manejar el comportamiento de la red en entornos constantemente cambiantes e impredecibles.

4.10. Conclusiones

En este capítulo se demostró que la emergencia de cooperación en una red de agentes es posible a través de la adaptación. Tres modelos fueron propuestos, empezando con los algoritmos genéticos que obtienen confianza en la red, pero los cambios constantes y la posibilidad de

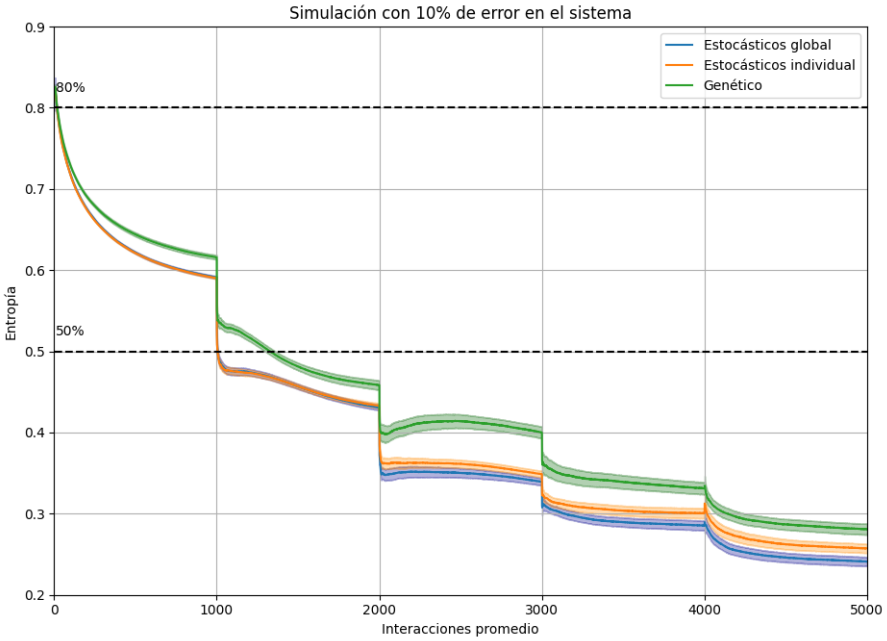

Figura 4-12: Resultados en entropía de los modelos con 10 % de error. Elaboración propia.

errores externos son una amenaza al desempeño de la confianza. La debilidad observada de los algoritmos genéticos es la velocidad de adaptación. Por esta razón, se exploró la posibilidad de usar juegos estocásticos. Con la definición de este nuevo modelo surgieron dos ramificaciones a considerar en las validaciones: los juegos estocásticos globales y los juegos estocásticos individuales. Finalmente, se realizaron las simulaciones en un entorno controlado y se evidenció que los juegos estocásticos mejoran notablemente la velocidad de adaptación y pueden garantizar una emergencia de cooperación en una red dinámica y distribuida. Además, ambas variaciones del modelo presentaron buenos resultados, lo cual significa que cualquiera de los dos es una alternativa viable a implementar. No obstante, un criterio que puede ser decisivo en una red ad-hoc particular para decidir entre el modelo estocástico global y el individual, puede ser la facilidad de difusión de información a todos los integrantes de la red (ya que esto será necesario en el escenario global para modificar el juego activo de todos los agentes) y en el caso de que esto sea un problema se puede optar por la variación individual del modelo.

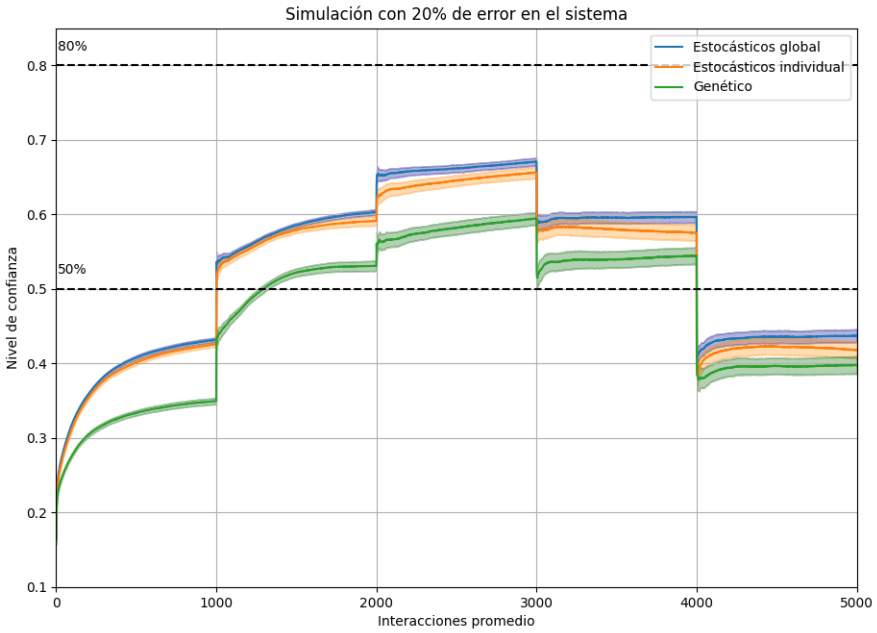

Figura 4-13: Resultados en confianza de los modelos con 20 % de error. Elaboración propia.

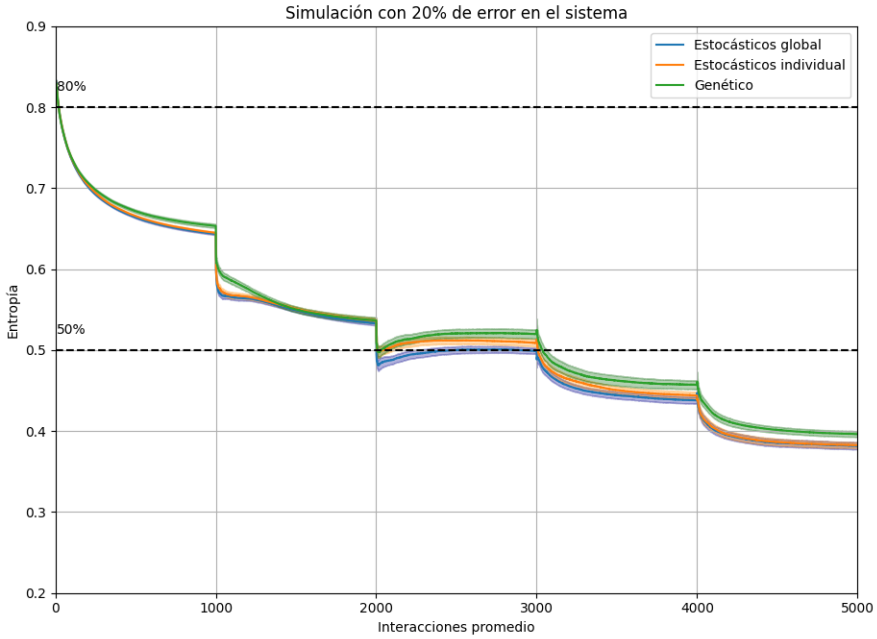

Figura 4-14: Resultados en entropía de los modelos con 20 % de error. Elaboración propia.

5 Implementación sobre la red ad-hoc

La última etapa de esta investigación es realizar una implementación del modelo propuesto en una red ad-hoc con el apoyo del grupo de investigación TLÖN, que proporciona la infraestructura para realizar dicho proceso. Adicionalmente, se hace un reporte sobre la complejidad de la implementación. Es importante remarcar que el objeto principal de esta tesis es el modelo, el cual es probado a través de simulaciones (proceso expuesto en el capítulo 4) y posteriormente implementado en una prueba piloto sobre una red ad-hoc. En este capítulo se describe la implementación que permitirá entender cómo el modelo encaja en la arquitectura de las redes ad-hoc en general y cuáles son los requerimientos del sistema para sostener el modelo.

5.1. Arquitectura utilizada sistema multi-agente

Los elementos mínimos para la creación de una red ad-hoc son dos dispositivos y una conexión de tipo distribuida entre ellos. En el caso de esta implementación, se utilizan 5 dispositivos (Raspberry Pi 4) proporcionados por el grupo de investigación TLÖN. Después de realizar la conexión ad-hoc entre los dispositivos, se despliega la infraestructura de la red, según se describió en la sección 3.6. El diseño de esta red tiene la capa del sistema multi-agente, sobre la cual se realiza esta implementación. En este nivel se agrega el código que permite crear uno o más agentes en un mismo dispositivo, así cada dispositivo cuenta con 20 agentes creados conviviendo en el sistema multi-agente de la red para un total de 100 agentes. Además, se tiene el proceso de envío de mensajes a través de la red. Este proceso equivale al usado en las simulaciones (Sección 4.4) para realizar las pruebas en la implementación.

5.2. Implementación del modelo

La implementación consta de 2 etapas. Primero, la inicialización de la red, en donde se hace el levantamiento de la infraestructura y de la población inicial de agentes sobre el sistema multi-agente. Segundo, el proceso de envío de información a través de la red, el cual es ejecutado numerosas veces (hasta lograr 1000 interacciones por agente) con el fin de que el algoritmo tenga la oportunidad de adaptarse a la red.

Requerimientos de memoria mínimos para cada agente de la red		
Variable	**Tipo variable**	**Definición**
Red de confianza	Diccionario{ String: Arreglo <Entero x 3>}	El diccionario contiene n elementos, siendo n la cantidad de agentes en la red. La llave del diccionario es el identificador del agente y el valor es un arreglo con los resultados de las ultimas 3 interacciones para calcular así la confianza.
Estrategia	Arreglo <Bit x 16>	La estrategia consta siempre de 16 bits (1 o 0 para cada bit).
Iteraciones	Entero positivo	Se lleva la cuenta de las iteraciones que se han tenido, ya que después de una cantidad K (pruebas realizadas con K=10,25 y 50) de iteraciones se realiza la reproducción genética (explicada en la sección 4.3).
Puntaje	Entero positivo	El puntaje es la acumulación de los pagos que se obtienen después de cada interacción. El sistema de pagos está definido en las secciones 4.8.1 y 4.8.2.
Juego	Binario	Es el juego en el que se encuentra el agente. Como en el modelo se propone un sistema con 2 juegos, el número es binario. El sistema de cambio entre juegos se explica en la sección 4.8.3.

Tabla 5-1: Requerimientos de memoria para la implementación del modelo propuesto. Elaboración propia.

5.2.1. Primera etapa: inicialización de la red

El levantamiento de la red empieza con un dispositivo que inicializa la instancia de la red ad-hoc, sobre la cual pueden unirse otros dispositivos adicionales. Luego de que la parte física de la red (2 o más dispositivos) está conectada, se puede proceder a la creación de los agentes que van a interactuar en la capa del sistema multi-agente. En el momento de la creación de los agentes es importante denotar que existen 2 tipos de agentes: los "agentes estocásticos" y los "agentes egoístas". Los agentes estocásticos se refieren a aquellos que tienen implementado en su lógica el modelo propuesto en el capítulo 4, particularmente se utiliza el modelo estocástico individual, debido a que utiliza menos el proceso de difusión de información, ahorrando así recursos computacionales. Los agentes egoístas son aquellos que no cuentan con una estrategia, por lo que su comportamiento consiste solo en participar en interacciones participando como destino o fuente (beneficio propio). Esto quiere decir que cuando los otros agentes soliciten su cooperación como agente intermedio de la transferencia, el agente egoísta nunca va a cooperar. En la Tabla **5-1** se presentan las variables requeridas con definición y tipo de valor, que serán los atributos de los agentes para asegurar el funcionamiento del modelo propuesto en esta tesis.

Cabe resaltar que no es necesario que los dispositivos mismos sean los encargados de almacenar la información descrita en la Tabla **5-1**, ya que en las redes ad-hoc es común contar con dispositivos de poca memoria, por ejemplo, sensores utilizados generalmente para crear redes de monitoreo como en sistemas avanzados de riego de cultivos. En estos casos, se puede almacenar la información en la memoria distribuida de la red con el fin de que el sensor no necesite una memoria adicional para funcionar, lo cual puede complicar su funcionamiento.

5.2.2. Segunda etapa: envío de información

El proceso de envío de información se realiza de manera aleatoria, esto quiere decir la selección de un agente **destino** se hacen uniformemente aleatorio entre los agentes que conviven en la red, esto con el fin de fomentar la interacción constante y diversa entre los integrantes de la red. De esta manera, se emplean los denominados "torneos" usados en teoría de juegos, que constan de una ronda en la cual cada uno de los integrantes debe participar una vez como agente **fuente** del envío y los agentes **destino** son escogidos de manera aleatoria. De la misma manera los agentes intermedios son escogidos dependiendo del nivel de confianza y la proximidad, teniendo en cuenta que en una red real con múltiples dispositivos el camino a seguir va a depender del proceso de **ruteo**. El ruteo puede depender de muchas variables y existen una creciente cantidad de propuestas en la literatura de protocolos de ruteo que tienen diferentes enfoques. Por esta razón, la implementación realizada durante esta tesis deja parcialmente excluido el componente de ruteo en la red, usando el nivel de confianza y la proximidad como factores de decisión de la ruta a seguir. Adicionalmente, el error no controlado de la red es incierto, debido a que durante la implementación no se agrega error de

manera forzada, sino que siendo un escenario real el error esta presente de manera inherente en el sistema.

Los requerimientos de procesamiento del modelo son aquellos procesos requeridos por cada agente para que el modelo funcione correctamente. Dichos procesos se encuentran listados en la Tabla **5-2**, donde se muestra el uso de las variables expuestas en la Tabla **5-1** durante el proceso de interacción. Los procesos de creación e interacción de agentes son procesos naturales que deben existir en la red independientemente del modelo de interacción que se use, pero en este caso necesita algunos elementos adicionales, los cuales se aclaran en la descripción de cada proceso. Por otro lado, los procesos de actualización de contadores y de reproducción genética son procesos nuevos en comparación con las redes ad-hoc tradicionales y necesarios en los algoritmos genéticos. Estos dos procesos son ejecutados al final de cada interacción, pero no siempre son llevados a cabo, ya que por ejemplo la reproducción genética se realiza después de un determinado número de interacciones (cada 50 interacciones en el caso de estas pruebas).

5.3. Resultados obtenidos

El proceso de implementación descrito a lo largo del capítulo se realizó sobre un sistema cuyo lenguaje de programación es Python. En este proceso, cada agente realizó 1000 envíos con rutas aleatorias, con los 100 agentes que conviven en la red. Esto es comparable con una etapa de las simulaciones realizadas en el capítulo 4. Es necesario realizar varias interacciones para que los agentes efectuaran al menos 10 reproducciones genéticas, con el fin de iniciar el proceso de adaptación y probar que la herencia esta funcionando dentro del sistema. Después de la programación de las pruebas se ejecutó todo dentro del sistema sin errores, y se obtuvieron más de 10 procesos de reproducción genética y un indicador de confianza en la red del 80 % para las pruebas, en las cuales se tenían 80 agentes genéticos y 20 egoístas. Estos resultados se presentan en la Figura **5-1** donde el eje vertical muestra la confianza de la red (C, que se explicó en la sección 4.2.1) y el eje horizontal, la cantidad promedio de interacciones.

Como se observa en la Figura **5-1**, la adaptación de la red es veloz, ya que la confianza oscila en el valor del 80 % y se estabiliza después de las primeras 100 interacciones aproximadamente. Este es un comportamiento similar al obtenido en las simulaciones, el cual se observa también en la gráfica con el color naranja. Estos datos de la simulación son un extracto de los resultados obtenidos en el capítulo 4 en la Figura **4-9**. Con esto se observa que los algoritmos genéticos combinados con los juegos estocásticos tienen una adaptación satisfactoria en ambientes reales. Con esta prueba piloto, es posible validar el comportamiento del modelo propuesto en esta tesis.

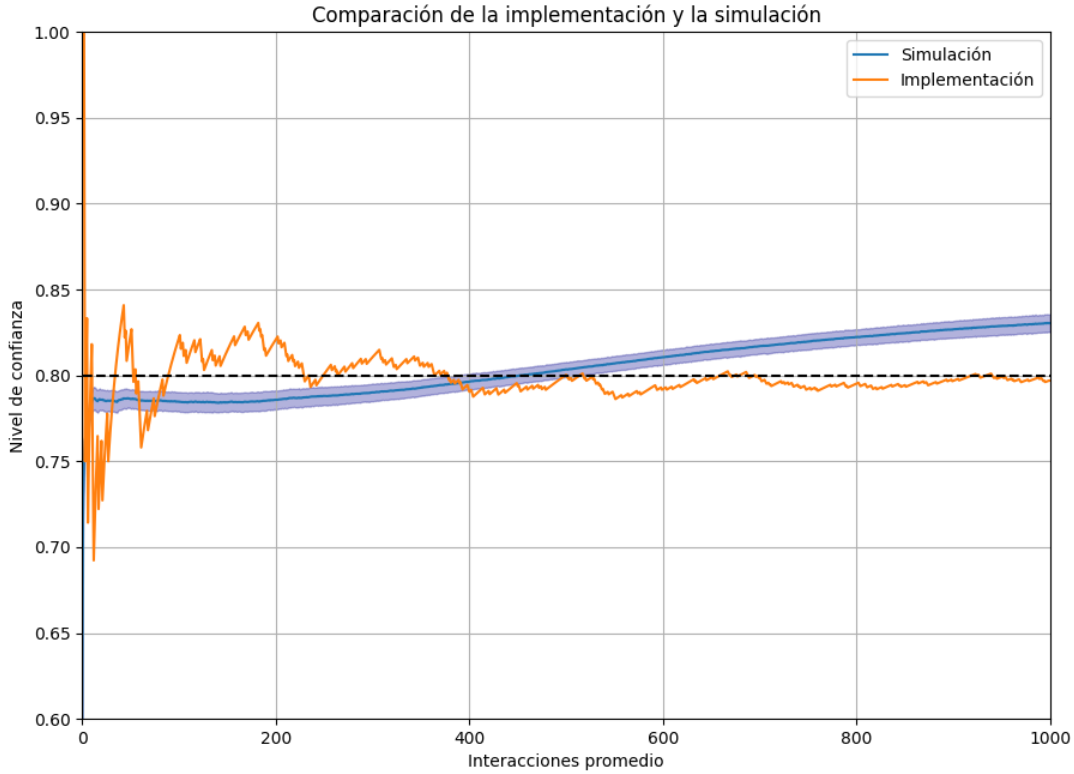

Figura 5-1: Resultados de la implementación sobre la red ad-hoc con una población de 80 % de agentes genéticos y 20 % de agentes egoístas, en comparación con las simulaciones. Elaboración propia.

5.4. Conclusiones

En este capítulo se propuso una estructura de implementación del modelo sobre una red ad-hoc programada en Python, a través de la cual se obtuvo información relevante para el modelo, como lo son las variables mínimas requeridas (memoria), los procesos principales (procesamiento) y los resultados de la cooperación en la red. Esta información es útil para que las personas que desean utilizar este método tengan una dimensión de la memoria y del procesamiento necesario por parte de la red para soportar el modelo propuesto, además de que pueden evidenciar la efectividad de la adaptación del modelo propuesto.

Se puede resaltar que los elementos principales de las redes ad-hoc que deben ser aprovechados en la implementación del modelo son los recursos distribuidos del sistema, es decir, tanto la memoria como el procesamiento requeridos en cada interacción pueden ser ejecutados con los recursos que la red puede proporcionar. Estos elementos se vuelven relevantes debido a que en las redes ad-hoc se suelen tener dispositivos simples, con poca memoria o velocidad de procesamiento. Ejemplo de esto son los sensores, que son una parte importante en las aplicaciones de las redes ad-hoc, como las VANETs (redes de vehículos) y los sistemas de riego inteligente.

Procesos principales para cada agente de la red		
Proceso	**Variables usadas**	**Descripción**
Creación de un agente	Todas las variables de la Tabla **5-1**	Se crea una nueva instancia de agente que tiene todas las variables con sus valores iniciales.
Interacción entre dos agentes	Estrategia y red de confianza	Para determinar si un agente decide cooperar con otro, se sigue la tabla de pagos descrita en la sección 4.8.1 y para esto se necesita consultar su estrategia y su historial de interacciones.
Actualizar contadores	Historial, interacciones, puntaje y juego	Después de una interacción es importante actualizar el historial, aumentar el contador de iteraciones y agregar los pagos correspondientes a la variable *Puntaje*. Por último, se debe revisar si es necesario hacer un cambio de juego (existen el juego 1 y el juego 2).
Proceso de reproducción genética	Puntaje y estrategia	El proceso de reproducción se realiza cada K interacciones (con K = 50 para el caso de esta implementación, pero dicho dato puede ser cambiado). En este proceso, se realizan el cruce y la mutación descritos en la sección 4.3. El resultado de esta reproducción dejará una nueva estrategia y las variables de *Iteraciones* y *Puntaje* reiniciados en ceros.

Tabla 5-2: Procesos necesarios para la implementación del modelo propuesto. Elaboración propia.

6 Conclusiones

6.1. Conclusiones

- En el capítulo 2 se describió la necesidad de un modelo de confianza que se ajuste a las condiciones de las redes ad-hoc. Posteriormente, se realizó la revisión de la literatura (capítulo 3) para clasificar las propuestas existentes y determinar un punto de partida adecuado para el trabajo de esta tesis. Con esto se encuentra que los modelos basados en confianza son ampliamente usados. En particular, el modelo que utiliza algoritmos genéticos propuesto por Mejía [32] ofrece una adaptabilidad constante al entorno. Esto se ajusta a los requisitos del problema de investigación y además presenta unos indicadores favorables en términos de confianza de la red. Adicionalmente, se mostró que el campo de estudio de los juegos estocásticos utiliza conceptos pertinentes para el manejo de sistemas constantemente cambiantes, lo cual beneficiará el desempeño del modelo desde el punto de vista de la adaptación. Finalmente, se propone la implementación del modelo con algoritmos genéticos complementados con juegos estocásticos, con el fin de obtener la adaptación como mecanismo de evolución de los algoritmos genéticos y mejorar la velocidad de adaptación a los cambios constantes de la red.

- Se propuso un ambiente de simulación que implementa todas las características relevantes de las redes ad-hoc con el fin de poner a prueba el modelo genético con juegos estocásticos en escenarios de simulación. Las dos métricas a utilizar son la confianza y la entropía de la red. La confianza es el indicador principal sobre el cual se determina el éxito del modelo, que se define como el porcentaje de interacciones exitosas sobre el total de interacciones intentadas. Por otro lado, la entropía es un indicador que permite entender parte del funcionamiento de los modelos a lo largo del tiempo, ya que muestra la incertidumbre que maneja el sistema. Las simulaciones realizadas arrojan resultados del indicador de confianza favorable (80 % para la prueba con 80 agentes genéticos y 20 agentes egoístas) para la red. Adicionalmente, con la inclusión de los juegos estocásticos, se logra mejorar la velocidad de adaptación en casi 10 % en comparación con los resultados obtenidos por Mejía [32] durante la primera etapa de la simulación (descrita en la sección 4.9). Así mismo, la entropía permite entender cómo los agentes califican en términos de confianza a los otros integrantes de la red. Estos resultados demuestran que se consiguió un modelo que cumple con los objetivos

propuestos.

- Finalmente, se realizó la validación de los resultados obtenidos en el ambiente de simulación con una implementación en una prueba piloto sobre una red ad-hoc real. Esta red fue proporcionada por el grupo de investigación TLÖN, donde se programa el funcionamiento del modelo propuesto (según se describe en el capítulo 4). Posteriormente, se realizan pruebas que arrojan resultados que validan el comportamiento observado en simulaciones. Con esto, se observa la adaptación del modelo mediante el indicador de confianza de la red, en el que se obtuvo un 80 % de confianza con una población de 80 agentes estocásticos individuales y 20 agentes egoístas (similar a los resultados obtenidos en las simulaciones). Adicionalmente, se presenta un esquema con los requisitos mínimos en términos de memoria y procesamiento que el sistema necesita para garantizar que la red tiene la capacidad de utilizar el modelo propuesto.

6.2. Trabajo futuro

6.2.1. Algoritmos genéticos

Los algoritmos genéticos tienen muchas variaciones que vale la pena explorar en este modelo. Las variables que se deben definir en un modelo de algoritmos genéticos como la probabilidad de mutación, la probabilidad de cruce, el tamaño del código genético y la escala de clasificación de confianza. Estos son parámetros que fueron definidos para esta tesis a través de referencias relevantes en la literatura, pero aún así es posible que una combinación diferente de estos parámetros proporcione mejores resultados para este escenario particular de las redes ad-hoc.

6.2.2. Redes distribuidas

El enfoque de la cooperación emergente puede ser extendido a otro tipo de redes distribuidas, como los estudios en computación distribuida en la nube, redes tolerantes a demoras u otras arquitecturas, como las redes centradas en la información (ICN), que hacen parte de la infraestructura pensada para redes modernas como la 5G y las futuras VANETs.

6.2.3. Redes numerosas

Durante la implementación realizada, se utilizaron solo 5 dispositivos debido a la disponibilidad que se tiene a este tipo de dispositivos y redes, gracias a la colaboración del grupo de investigación TLÖN. Sin embargo, este modelo está diseñado para funcionar en redes ad-hoc grandes, por esto es apropiado realizar pruebas de la implementación sobre una infraestructura grande (con más de 90 dispositivos) para observar el desempeño.

6.2.4. Aplicaciones

El modelo validado en esta tesis tiene el potencial de ser usado en todo tipo de redes ad-hoc. Sin embargo, es necesario observar el comportamiento de este modelo sobre implementaciones específicas y observar posibles ventajas sobre escenario particulares. Por ejemplo, VANETs, sistemas de riego y agrónica.

Bibliografía

[1] *Proyecto TLÖN - acerca del proyecto.* http://www.tlon.unal.edu.co/proyecto-tlon/acerca. – Accessed: 2020-11-29

[2] Abdel-Halim, I T. ; Fahmy, H M A. ; Bahaa-Eldin, A M.: Agent-based trusted on-demand routing protocol for mobile ad-hoc networks. En: *Wireless Networks* 21 (2014), Nr. 2, p. 467–483

[3] Anderegg, Luzi ; Eidenbenz, Stephan: Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. En: *Proceedings of the 9th annual international conference on Mobile computing and networking*, 2003, p. 245–259

[4] Ashwin, M ; Kamalraj, S ; Azath, M: Weighted Clustering Trust Model for Mobile Ad Hoc Networks. En: *Wireless Personal Communications* 94 (2017), Nr. 4, p. 2203–2212

[5] Axelrod, Robert ; Hamilton, William D.: The evolution of cooperation. En: *science* 211 (1981), Nr. 4489, p. 1390–1396

[6] Ayday, E ; Fekri, F: An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks. En: *IEEE Transactions on Mobile Computing* 11 (2012), Nr. 9, p. 1514–1531

[7] Bansal, Sorav ; Baker, Mary: Observation-based cooperation enforcement in ad hoc networks. En: *arXiv preprint cs/0307012* (2003)

[8] Bauer, Paul C.: Conceptualizing trust and trustworthiness. (2017)

[9] Bauer, Paul C. ; Keusch, Florian ; Kreuter, Frauke: Trust and cooperative behavior: Evidence from the realm of data-sharing. En: *PloS one* 14 (2019), Nr. 8, p. e0220115

[10] Bisen, D ; Sharma, S: An enhanced performance through agent-based secure approach for mobile ad hoc networks. En: *International Journal of Electronics* 105 (2018), Nr. 1, p. 116–136

[11] Buchegger, Sonja ; Le Boudec, Jean-Yves: Performance analysis of the CONFIDANT protocol. En: *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002, p. 226–236

[12] Chatterjee, P ; Sengupta, I ; Ghosh, S K.: STACRP: A secure trusted auction oriented clustering based routing protocol for MANET. En: *Cluster Computing* 15 (2012), Nr. 3, p. 303–320

[13] Fadel, Etimad ; Gungor, Vehbi C. ; Nassef, Laila ; Akkari, Nadine ; Malik, MG A. ; Almasri, Suleiman ; Akyildiz, Ian F.: A survey on wireless sensor networks for smart grid. En: *Computer Communications* 71 (2015), p. 22–33

[14] Fitzek, F.H.P. ; Katz, M.D.: *Cooperation in wireless networks: Principles and applications: Real egoistic behavior is to cooperate!* Springer, 2006. – 1–641 p.. – cited By 186

[15] Friedman, Linda W. ; Friedman, Hershey H.: Analyzing simulation output using the bootstrap method. En: *Simulation* 64 (1995), Nr. 2, p. 95–100

[16] Gera, P ; Garg, K ; Misra, M: Trust-based multi-path routing for enhancing data security in MANETs. En: *International Journal of Network Security* 16 (2014), Nr. 2, p. 102–111

[17] Gershenson, Carlos ; Heylighen, Francis: When can we call a system self-organizing? En: *European Conference on Artificial Life* Springer, 2003, p. 606–614

[18] Ghosekar, Pravin ; Katkar, Girish ; Ghorpade, Pradip: Mobile ad hoc networking: imperatives and challenges. En: *IJCA Special issue on MANETs* 3 (2010), p. 153–158

[19] Hanbali, Ahmad ; Ibrahim, Mouhamad ; Simon, Vilmos ; Varga, Endre ; Carreras, Iacopo: A Survey of Message Diffusion Protocols in Mobile Ad Hoc Networks, 2008

[20] Hardin, Garrett: The tragedy of the commons. En: *science* 162 (1968), Nr. 3859, p. 1243–1248

[21] He, Qi ; Wu, Dapeng ; Khosla, Pradeep: SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. En: *2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733)* Vol. 2 IEEE, 2004, p. 825–830

[22] Hegde, S B. ; Babu, B S. ; Venkataram, P: A Cognitive Theory-based Opportunistic Resource-Pooling Scheme for Ad hoc Networks. En: *Journal of Intelligent Systems* 26 (2017), Nr. 1, p. 47–68

[23] Hilbe, Christian ; Šimsa, Štěpán ; Chatterjee, Krishnendu ; Nowak, Martin A.: Evolution of cooperation in stochastic games. En: *Nature* 559 (2018), Nr. 7713, p. 246–249

[24] Jayanand, A ; Chenthil Kumaran, N: Trusted and authentication based routing security for MANET. En: *International Journal of Applied Engineering Research* 10 (2015), Nr. 1, p. 105–120

[25] Katz, M. ; Fitzek, F.H.P. ; Lucani, D.E. ; Seeling, P.: Mobile clouds as the building blocks of shareconomy: Sharing resources locally and widely. En: *IEEE Vehicular Technology Magazine* 9 (2014), Nr. 3, p. 63–71

[26] Li, W ; Parker, J ; Joshi, A: Security through collaboration and trust in MANETs. En: *Mobile Networks and Applications* 17 (2012), Nr. 3, p. 342–352

[27] Loo, Jonathan ; Mauri, Jaime L. ; Ortiz, Jesus H.: *Mobile ad hoc networks: current status and future trends*. CRC Press, 2016

[28] Mandhare, V V. ; Thool, V R. ; Manthalkar, R R.: QoS Routing enhancement using metaheuristic approach in mobile ad-hoc network. En: *Computer Networks* 110 (2016), p. 180–191. – ISSN 1389–1286

[29] Mani, P ; Kamalakkannan, P: Conviction based packet promotion scheme for efficient detection of selfish nodes in mobile Ad Hoc networks. En: *International Review on Computers and Software* 9 (2014), Nr. 2, p. 212–218

[30] Marias, Giannis F. ; Georgiadis, Panagiotis ; Flitzanis, D ; Mandalas, K: Cooperation enforcement schemes for MANETs: A survey. En: *Wireless Communications and Mobile Computing* 6 (2006), Nr. 3, p. 319–332

[31] Mejia, Angela M.: *Evolución genética de estrategias para modelos de confianza en redes móviles ad-hoc basados en teoría de juegos*. 2010. – unpublished thesis

[32] Mejia, M ; Peña, N ; Muñoz, J L. ; Esparza, O ; Alzate, M A.: A game theoretic trust model for on-line distributed evolution of cooperation inMANETs. En: *Journal of Network and Computer Applications* 34 (2011), Nr. 1, p. 39–51

[33] Mertens, J-F ; Neyman, Abraham: Stochastic games. En: *International Journal of Game Theory* 10 (1981), Nr. 2, p. 53–66

[34] Michiardi, Pietro ; Molva, Refik: Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. En: *Advanced communications and multimedia security*. Springer, 2002, p. 107–121

[35] Myerson, Roger B.: *Game theory*. Harvard university press, 2013

[36] Ninu, S B. ; Behin Sam, S: A collaborative Intrusion Detection System for manet using data mining technique. En: *ARPN Journal of Engineering and Applied Sciences* 13 (2018), Nr. 14, p. 4387–4392

[37] Ochoa, Gabriela: Setting the mutation rate: Scope and limitations of the 1/L heuristic. En: *Proceedings of the 4th Annual Conference on Genetic and Evolutionary Computation*, 2002, p. 495–502

[38] Pariselvam, S ; Parvathi, R M S.: Trust based security mechanism for service discovery in MANET. En: *Journal of Theoretical and Applied Information Technology* 56 (2013), Nr. 2, p. 226–234

[39] Pouyan, A A. ; Yadollahzadeh Tabari, M: FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network. En: *International Journal of Communication Systems* 30 (2017), Nr. 1

[40] Rajeshwar, J ; Narsimha, G: Secure way routing protocol for mobile ad hoc network. En: *Wireless Networks* 23 (2017), Nr. 2, p. 345–354

[41] Rapoport, Anatol ; Chammah, Albert M. ; Orwant, Carol J.: *Prisoner's dilemma: A study in conflict and cooperation*. Vol. 165. University of Michigan press, 1965

[42] Raychaudhuri, Dipankar ; Gerla, Mario: *Emerging wireless technologies and the future mobile internet*. Cambridge University Press, 2011

[43] Raychaudhuri, Dipankar ; Mandayam, Narayan B.: Frontiers of wireless and mobile communications. En: *Proceedings of the IEEE* 100 (2012), Nr. 4, p. 824–840

[44] Reddy, V B. ; Venkataraman, S ; Negi, A: A dynamic trust evolution model for MANETs based on mobility. En: *International Journal of Ad Hoc and Ubiquitous Computing* 28 (2018), Nr. 4, p. 230–246

[45] Roughgarden, Tim: Algorithmic game theory. En: *Communications of the ACM* 53 (2010), Nr. 7, p. 78–86

[46] Saha, H N. ; Singh, R ; Bhattacharyya, D ; Banerjee, P K.: Modified Fidelity Based On-Demand Secure (MFBOD) Routing Protocol in Mobile Ad-Hoc Network. En: *Foundations of Computing and Decision Sciences* 40 (2015), Nr. 4, p. 267–298

[47] Shannon, Claude E.: A mathematical theory of communication. En: *ACM SIGMOBILE mobile computing and communications review* 5 (2001), Nr. 1, p. 3–55

[48] Sridhar, S ; Nagaraju, V ; Bapu, B R T. ; Shankar, R ; Anitha, R: Trusted and optimized routing in mobile ad-hoc networks emphasizing quality of service. En: *Applied Mathematics and Information Sciences* 12 (2018), Nr. 3, p. 655–663

[49] Thorat, S A. ; Kulkarni, P J.: Opportunistic Routing in Presence of Selfish Nodes for MANET. En: *Wireless Personal Communications* 82 (2015), Nr. 2, p. 689–708

[50] Tonguz, Ozan K. ; Ferrari, Gianluigi: A communication-theoretic approach to ad hoc wireless networking. En: *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks* Vol. 2 IEEE, 2006, p. 715–722

[51] Vega, Diego A. ; Ospina, Juan P. ; Latorre, Julian F. ; Ortiz, Jorge E.: An adaptive trust model for achieving emergent cooperation in ad hoc networks. En: *Current Trends in Semantic Web Technologies: Theory and Practice*. Springer, 2019, p. 85–100

[52] Vekaria, Kanta ; Clack, Chris: Selective crossover in genetic algorithms: An empirical study. En: *International Conference on Parallel Problem Solving from Nature* Springer, 1998, p. 438–447

[53] Wooldridge, Michael: *An introduction to multiagent systems*. John Wiley & Sons, 2009

[54] Yang, Hao ; Shu, James ; Meng, Xiaoqiao ; Lu, Songwu: SCAN: self-organized network-layer security in mobile ad hoc networks. En: *IEEE Journal on Selected Areas in Communications* 24 (2006), Nr. 2, p. 261–273

[55] Zhang, Qing ; Yu, Ting ; Irwin, Keith: A Classification Scheme for Trust Functions in Reputation-Based Trust Management. En: *ISWC Workshop on Trust, Security, and Reputation on the Semantic Web* Vol. 127 Citeseer, 2004

[56] Zhang, Yujun ; Yan, Tan ; Tian, Jie ; Hu, Qi ; Wang, Guiling ; Li, Zhongcheng: TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks. En: *Ad Hoc Networks* 21 (2014), p. 109–122. – ISSN 1570–8705

[57] Zhong, Sheng ; Chen, Jiang ; Yang, Yang R.: Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. En: *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)* Vol. 3 IEEE, 2003, p. 1987–1997