Universidad Autónoma de Baja California
Facultad de Ingeniería, Arquitectura y Diseño
Maestría y Doctorado en Ciencias e Ingeniería

"Privacidad en la Ubicación de la Fuente de Datos"

Tesis que para obtener el grado de Doctor en Ciencias

Presenta
María de los Ángeles Cosio León

Director
Dr. Juan Iván Nieto Hipólito

Ensenada, Baja California, México. 7 de Diciembre de 2012

Universidad Autónoma de Baja California

Facultad de Ingeniería, Arquitectura y Diseño

Maestría y Doctorado en Ciencias e Ingeniería

"Privacidad en la Ubicación de la Fuente de Datos"

Tesis

que para obtener el grado de Doctor en Ciencias presenta:

María de los Ángeles Cosio León

Aprobada por:

Dr. Juan Iván Nieto Hipólito

Director de Tesis.

Dra. Larysa Burtseva

Dra. Mabel Vázquez Briseño

Dra. Mireya Saraí García Vázquez

Dr. Juan de Dios Sánchez López

Ensenada, Baja California, México, Diciembre de 2012

RESUMEN de la tesis de María de los Ángeles Cosio León, presentada como requisito parcial para la obtención del grado de DOCTOR EN CIENCIAS, Ensenada, BC., México, Diciembre de 2012

"Privacidad en la Ubicación de la Fuente de Datos"

Resumen aprobado por:

Dr. Juan Iván Nieto Hipólito

Director de Tesis.

Siendo la ubicación un dato a partir del cual es posible deducir información adicional del objeto o sujeto de interés, es necesario contar con herramientas para reducir la posibilidad de que una persona no autorizada acceda a este dato. A la entidad que intenta acceder sin autorización a la información de la fuente de datos, en este trabajo la definimos como *el adversario* y a su actividad como *un ataque*. Para reducir la probabilidad de éxito de un ataque, esta investigación tuvo como objetivo diseñar un protocolo de encaminamiento con consciencia en la privacidad en la ubicación de la fuente de datos llamado NUKU (Nucu keeps untracking). NUKU se diseño para redes inalámbricas de múltisalto donde las transmisiones entre un nodo origen y un nodo destino generalmente se realizan por un conjunto de nodos intermedios que se identifican como una ruta.

NUKU emula el comportamiento de las hormigas en su búsqueda por alimento. En su búsqueda las hormigas trazan varias rutas de la fuente de alimento al nido, sin importar si es el camino más corto entre el nodo fuente y el nodo destino. Las rutas son preferidas unas sobre otras por el nivel de una sustancia llamada feromona que las hormigas sueltan de manera natural en su caminar. Rutas con niveles de feromona altos son las que siguen el resto de las hormigas que buscan comida. Los paquetes seguirán una ruta entre el nodo fuente y el nodo destino hasta que el nivel de feromona disminuya debido a un proceso de evaporación. En NUKU la evaporación es controlable en cada nodo parte de la ruta. NUKU tiene capacidad de proteger hasta tres veces más paquetes transmitidos que las propuestas existentes en la literatura. La tecnología de red utilizada para probar el desempeño del protocolo fue una *Red inalámbrica de dispositivos para adquirir datos del contexto (WSN).*

Palabras Clave: Privacidad, redes inalámbricas múltisalto, WSN, Heurísticas bioinspiradas, Algoritmos basados en hormigas.

ABSTRACT of thesis presented by María de los Ángeles Cosio León as partial requirement to obtain the Doctor of Science degree, Ensenada, Baja California, México, Diciembre de 2012

"Data Source Location Privacy"

Abstract approved by:

Dr. Juan Iván Nieto Hipólito

Thesis director.

Using location datum as an index; it is possible to deduce additional information from the subject or object of interest; hence, it is necessary mechanisms to control location data access by unauthorized people. We call *The Adversary* to the entity gaining access from the data source information without rights; the strategy to achieve her aim, we denominated as an attack. In intention to reduce successful attack's likelihood, this research aimed to develop a routing protocol aware of source location privacy; it is called NUKU (nucu keeps un-tracking). NUKU was designed for multihop wireless networks. A multihop wireless network transmission between a source and destination node uses a set of intermediate nodes. The set of intermediate nodes in the network defines a route.

To define routes, NUKU emulates ant searching by food behaviour. Ants from the food zone to nest build routes by dropping on visited nodes a chemical substance called pheromone. Routes could not be the shortest path between the source and destination nodes. Routes with highest pheromone level are preferred over lower ones. Once routes exist, packet transmissions follow the highest pheromone level routes. In NUKU's scenario as packets traverse over routes, an evaporation process removes pheromone in nodes' route up to pheromone trail disappear on route. NUKU controls the evaporation process node by node. NUKU can protect three times more packets than other proposals in the literature. The network technology used to analyse NUKU's performance was a public *WSN*.

Keywords: Privacy, Multihop Wireless Networks, WSN, Bioinspired Heuristics, Ant based algorithms

Dedicatoria

Al Dr. Jesús Luna García, muchas de sus ideas compartidas están aquí.

Don Javier y Doña Irma, por enseñarme el valor de ser familia.

A mis hermanos, por su cariño y el soporte que recibo.

Bell, gracias por estar siempre.

A dos personas que me regalan el sabor de estar en casa, Doña Gloria y Rafa.

A mis amigos: Luz, Maty, Federico, Alex, Héctor, Arturo, Juan Pablo, Luis, Humberto.

Agradecimientos

Al Dr. Juan Ivan Nieto Hipólito, Director en este trabajo de tesis

A la Dra. Larysa Burtseva, hay personas que tocan un momento nuestra vida y logran hacer una diferencia.

Al Consejo nacional de ciencia y tecnología, (CONACYT).

A la Universidad Autónoma de Baja California, (UABC).

A mis profesores del posgrado MYDCI.

A la Dra. Mabel Vázquez Briseño, Apoyo con beca de Investigación.

A los miembros del comité de tesis.

Al Dr. Abdelmajid Khelil, por sus sugerencias.

Al Dr. Raúl Aquino Santos, por su aporte a mi desarrollo profesional.

Índice General

Índice de figuras

Índice de Tablas

Acrónimos

ACO Optimización por colonia hormigas (Ant Colony Optimization) iv

ADLs Actividades de la vida diaria(Activities of Daily Life) 4

AML Latencia promedio del mensaje(Average Message Latency) 39

DTN Redes tolerantes al retardo (Delay Tolerant Networks) 38

FFD Dispositivo con funciones completas (Full Function Device) 13

GPS Sistema de posicionamiento global (Global Positioning System) 4

IOI Objeto de interés (Item Of Interest) 4

LBS Servicios basados en la ubicación (Location Based Services) 4

Low-Rate WPAN Red inalámbrica de area personal de baja tasa de transmisión (Low Rate Wireless Personal Area Networks) vii

MAC Control de acceso al medioMedium Access Control 11

NUKU Nucu evita el seguimiento (Nucu Keeps Un-tracking) iv

OSI Módelo de interconexión de sistemas abiertosOpen System Interconnection . . . 6

PAN Red de area personal (Personal Area Network) 13

PII Información de identificación personal (Personal Identification Information) . 22

PSN Redes de intercambio de datos en dispositivos de bolsillo (Pocket Switched Network) 38

RFD Dispositivo con funciones reducidas (Reduce Function Device) 13

RFID Identificadores por radio frecuencia (Radio-Frequency Identification) 4

SOI	Sujeto de interés (Subjects Of Interest) 4
TTL	Tiempo de Vida(Time To Live) 51
WSN	Red inalámbrica de dispositivos para adquirir datos del contexto (Wireless Sensor Network) 3

CAPÍTULO I

INTRODUCCIÓN

Un gran porcentaje de las personas cree que su información, inclusive su ubicación no es adecuadamente protegida, por los servicios que se ofrecen a través de los sistemas de comunicación electrónica como por ejemplo la Internet, por lo cual consideran que su *privacidad* esta amenazada. Sin embargo, esta preocupación no afecta en demasía la apertura para la adopción de nuevas tecnologías (Acquisti y Grossklags, 2005) ademas de (Janice Tsai, 2007). Tomando sentido lo expresado por Scott McNealy, CEO de Sun hasta Abril 24 de 2006, respecto al uso de las nuevas tecnologías: “Es un hecho que tenemos un nivel de privacidad de cero. Así que, usemos o no la tecnología, esta condición se mantiene.”

Altman, 1975 define *la privacidad* como “Procesos de regulación de limites, a través de los cuales las personas optimizan el acceso a su información personal, considerando un espectro de restricciones para su apertura asociado a su contexto actual”. Derivado de la definición general de privacidad, se desglosa un tipo específico, *Privacidad en la Ubicación*, que desde una perspectiva legal refiere ”*al derecho de los individuos para determinar por si mismos, cuando, cómo y hasta qué punto la información respecto a su localización puede ser comunicada a otros*”.

En los últimos años, la evolución de los sistemas de comunicación inalámbrica, ha dado pauta a una amplia gama de servicios. Una clase de estos, son los que cuentan con consciencia en la ubicación de la fuente de datos. Estos tienen la capacidad de seguir y reportar la traza de movimiento del *Sujeto de interés (SOI)* u *Objeto de interés (IOI)* (Beresford y Stajano, 2003). Ejemplo de ello, son los servicios de seguimiento de la ubicación para pacientes mayores o con problemas mentales, asignándoles de forma virtual áreas de movilidad con seguridad en su integridad física. Lo que permite al *SOI* realizar sus *Actividades de la vida diaria (ADLs)*, sin una consciencia de la monitorización continua. Otro ejemplo de estas facilidades es la propuesta de Doukas y Maglogiannis, 2008 para personas invidentes. Esta solución, guía al usuario en una dirección especificada basado en un ubicación actual. Todos estos servicios se auxilian de tecnologías de cobertura amplia en exteriores como *Sistema de posicionamiento global (GPS)* (Lakshmanan y Sivakumar, 2009) y tecnologías para interiores, como *WSNs* e *Identificadores por radio frecuencia (RFID)*; permitiéndoles ofrecer, continuidad en la cobertura del servicio.

En los servicios de seguimiento el prestador y quien hace uso de ellos, son entidades que tiene una relación de confianza sustentada en intereses recíprocos, además de reglas sobre el uso de los datos, inclusive su ubicación.

Un grupo diferente de soluciones, son aquellas que ofrecen información sobre servicios para el usuario basadas en su ubicación actual, a tales soluciones se les conoce como *Servicios basados en la ubicación (LBS)*. En estas aplicaciones, existe interés por ambas partes de conocer la ubicación de la fuente de datos, sin que exista una relación de confianza. Ya que, diferente a los servicios de seguimiento, el usuario no tiene certeza del destino o uso que tendrán sus datos, una vez que el prestador tenga acceso a ellos.

Las aplicaciones *LBS*, hacen uso exhaustivo de información del contexto del usuario (Schilit y

otros , 1994). Información que les permite contestar a preguntas tales como: ¿Quién es?, ¿Dónde esta?, ¿Cúando? y ¿Qué es?, con el objetivo de determinar *¿Por qué lo hace?* (Abowd y otros , 1999).

En la práctica los elementos del contexto se dividen en dos grandes jerarquías: contexto primario y Contexto secundario. El contexto primario incluye: *Ubicación, Identidad, Actividad y Hora en que se ejecuta*. Los del contexto secundarios son una subclasificación cada uno de los elementos de los primarios. En la Figura I.1 se muestran los elementos del contexto primario, siendo usados para indagar en fuentes adicionales sobre el contexto secundario.

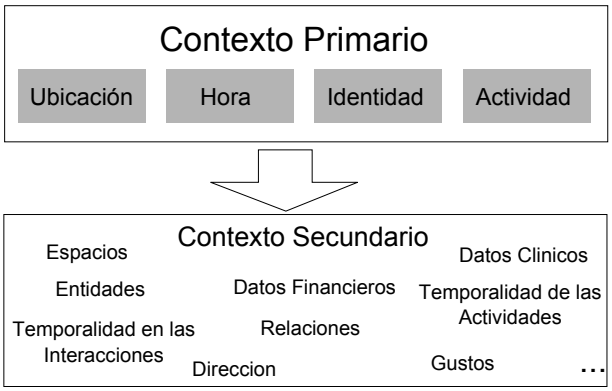

Figura I.1: Contexto Primario como índice.

Siendo la ubicación un elemento del contexto primario, a partir del cual es posible deducir información adicional del contexto secundario (como se muestra en la Figura I.1) es necesario considerar estrategias, para que una persona no autorizada acceda a esta información. A la entidad que intenta acceder sin autorización a la información de la fuente de datos, en este trabajo la definimos como *el adversario* y a su actividad como *un ataque*.

I.1 Descripción del Problema

En las redes inalámbricas múltisalto (Lakshmanan y Sivakumar, 2009), la transmisión de los datos, no se realiza de forma directa entre el dispositivo fuente y el dispositivo destino, sino que se retransmite, a través de una secuencia de nodos hasta llegar a su destino. A estos nodos se les conoce como *nodos de encaminamiento*. La selección de estos nodos, la realiza un protocolo de encaminamiento, el cual

desarrolla sus funciones en la capa de red del *Módelo de interconexión de sistemas abiertos (OSI)*, para la interconexión de sistemas abiertos de comunicaciones. Estos protocolos utilizan diversas técnicas para trazar rutas entre un nodo fuente y un nodo destino. Estas rutas son de longitud variable en el numero de nodos de encaminamiento necesarios para lograr enlazar la fuente con el destino. La elección de los nodos de encaminamiento disponibles en la red inalámbrica de múltisalto se hace optimizando restricciones como: energía en el nodo, cantidad de tráfico, calidad en los enlaces, el camino más corto desde el nodo fuente al nodo destino, entre otras. Además, de la característica múltisalto, estas redes son inalámbricas, lo cual las hace vulnerables a escuchas o recepciones pasivas. Esta condición se ve favorecida, debido a que no es posible agregar restricciones para el acceso al medio de transmisión.

En redes inalámbricas múltisalto, sí *el adversario* conoce o cuenta con suficientes elementos para deducir la ruta entre un nodo fuente y un destino, entonces conoce la ubicación de la fuente de datos y por lo tanto acceder a información del contexto secundario y parte del primario como se muestra en la Figura I.1. En consecuencia, el problema a resolver en este trabajo de investigación es ocultar la ruta que siguen los paquetes entre un nodo fuente y un nodo destino, esto se lograría agregando consciencia de la privacidad de la fuente de datos al protocolo de encaminamiento. La Figura I.2 muestra los actores que intervienen en el problema a resolver:

- Red inalámbrica múltisalto, compuesta de N nodos de encaminamiento.
- Nodo Fuente, el origen de los datos a transmitir.
- Nodo Destino, el lugar a donde se dirigen los flujos de datos.
- Protocolo de Encaminamiento, entidad que proporciona la ruta entre el nodo fuente y el nodo destino, en la Figura I.2, la ruta se muestra como el conjunto de nodos de encaminamiento de color gris.
- El Adversario, persona no autorizada para conocer la ubicación del nodo fuente y quien realiza el ataque.

El problema descrito se resume en la siguiente pregunta de investigación:

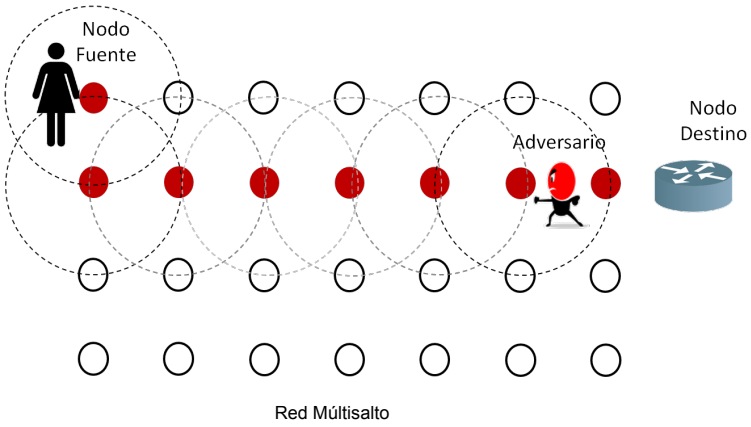

Figura I.2: Elementos en el escenario del problema

¿Cómo diseñar un protocolo de encaminamiento en una red inalámbrica múltisalto que sea capaz de ocultar la ruta que sigue el flujo de datos transmitidos entre un nodo fuente y un nodo destino?

I.2 Objetivos.

Objetivo general:

Diseñar y caracterizar un protocolo de encaminamiento con consciencia de la privacidad en la ubicación de la fuente de datos, empleando como caso de uso una Red inalámbrica de dispositivos para adquirir datos del contexto, WSN.

Objetivos específicos:

1. Valoración del rendimiento del protocolo, frente a diferentes tipos de adversarios propuestos en la literatura.
2. Proponer una arquitectura para la implementación del protocolo en dispositivos embebidos de tipo Low-Rate WPANs, basada en el estándar IEEE 802.15.4a 2006.

No son objetivos de esta investigación:

- Ocultar a un dispositivo cuando este se conecta a la red.
- Proveer de nuevos mecanismos de cifrado.
- Modificar el estándar IEEE 802.15.4a 2006.
- Ocultar la ubicación del dispositivo destino.
- Anonimato en la Comunicación.

I.3 Organización de la tesis

En esta sección se realiza una descripción breve del contenido de cada uno de los capítulos.

CAPITULO II "EL ESTÁNDAR IEEE 802.15.4 2006a" En este capitulo se introduce el estándar que se utilizó como caso de uso del algoritmo propuesto. Se eligió esta tecnología de red porque se preveé que sea la infraestructura de red de los servicios ubicuos y la tecnología habilitadora del paradigma de la Internet de las Cosas. Pero principalmente porque desde su concepción operan de una manera inalámbrica múltisalto.

CAPITULO III "ESTADO DEL ARTE" Se describen soluciones propuestas en la literatura al problema abordado para la tecnología de red (WSN), se hace un análisis de las mismas y se identifican sus ventajas y desventajas. Este análisis permitió elegir una solución base con la cual comparamos nuestra propuesta. Además, se conceptualizó un nuevo tipo de adversario, el cual es mas agresivo que los definidos en las propuestas analizadas.

CAPITULO IV "NUKU ENCAMINAMIENTO Y PRIVACIDAD" En este capitulo se presenta la propuesta para resolver el problema que en la literatura se referencia como *Obtención no autorizada de la ubicación de la fuente de datos en WSN* (Rios y Lopez, 2011; Ozturk y otros , 2004) y (Kamat y otros , 2005).

CAPITULO V "RESULTADOS" En esta sección se describe el escenario propuesto para la evaluación de NUKU así como la implementación de los diferentes elementos que lo integran, con el objetivo de simular el comportamiento del mismo. Adicional a lo anterior se muestran cuadros y gráficas comparativas permiten demostrar las ventajas de NUKU en redes de sensores.

CAPITULO VI "CONCLUSIONES" En este capitulo se concluye esta disertación con una síntesis de la investigación realizada, una discusión respecto a los resultados con una visión global. Concluyendo finalmente con trabajo a futuro derivado del uso de heurísticas bioinspirados aplicados a la privacidad.

I.4 Contribuciones de la tesis

La contribución principal de esta tesis es un algoritmo basado en heurísticas bioinspiradas con consciencia en la privacidad de la ubicación de la fuente de datos. El algoritmo diseñado transmite información entre la fuente de datos y el destino sin ofrecer suficiente información para que el adversario logre ubicar a la fuente por un periodo de tiempo. Los resultados obtenidos muestran un funcionamiento superior en las métricas empleadas para su comparación frente a otras soluciones.

CAPÍTULO II

EL ESTÁNDAR IEEE 802.15.4 2006a.

El estándar IEEE 802.15.4 (LAN/MAN Standards Committee, 2006), define las características de la capa física y el *Control de acceso al medio (MAC)* para una *Red inalámbrica de area personal de baja tasa de transmisión*. Estas redes están constituidas por dispositivos de bajo consumo de energía, este consumo lo logran por sus bajas tasas de transmisión de datos, periodos de inactividad en los transceptores y hardware reducido. Los dispositivos que conforman una *WSN* son de bajo costo y casi nulo mantenimiento en los dispositivos.

El costo de los dispositivos que forman las *WSNs* y sus capacidades para la adquisición continúa de datos en su esfera de cobertura, las convierten en tecnologías atractivas para soluciones de monitorización de aplicación masiva. Ejemplo de ello es en el paradigma de los servicios ubicuos, para el cual las *WSNs* son consideradas como la mejor tecnología de red (Zheng y Lee, 2004), consideración que convierte su estudio en una área de investigación con bastante actividad, para resolver problemas asociadas a la monitorización de personas.

Las *WSNs* se relacionan a soluciones que ofrecen servicio a personas y el objetivo de esta investigación es proveer de un mecanismo para mejorar y mantener la privacidad, por lo que el uso de esta tecnología como caso de uso de la solución se justifica a través de la resolución de un problema practico.

II.1 Redes inalámbricas de dispositivos de adquisición de datos

Los avances en las tecnologías inalámbricas y los microprocesadores de bajo consumo, han permitido la aparición de tecnologías de adquisición de datos de bajo costo, bajo consumo de energía y de aplicación en un amplio espectro de ambientes. Ejemplo de ello son las (*WSNs*). Los dispositivos que las componen, de forma genérica cuentan con un transceiver, una unidad de procesamiento, una unidad de adquisición de datos y un microprocesador; cuyo objetivo es adquirir datos de su contexto y transmitirlos a una unidad central.

Para su funcionamiento, el estándar IEEE 802.15.4 *Low-Rate WPAN* (LAN/MAN Standards Committee, 2006) define las características de la capa física y el control de acceso al medio (MAC) para bajo consumo y ciclos de trabajo reducidos. Los servicios de datos MAC se acceden por medio de la parte común de la subcapa, MAC common part sublayer-Service Access Point (MCPS-SAP) y el acceso a servicios MAC se logra por medio de la capa MAC de manejo de identidades, MAC sublayer management entity-Service Access Point (MLME-SAP). Esos dos servicios proporcionan una interfase entre las subcapas de convergencia de servicios específicos (Service-Specific Convergence Sublayer, SSCS) u otros tipos de Control de Enlace Lógico (Logical Link Control, LLC) propietarios, como se muestra en la Figura II.1.

Para llevar al cabo sus transacciones, el estándar define cuatro diferentes tipos de paquetes a los que llamaremos marcos:

Data Esta clase de marcos permite la transmisión de datos.

Beacon marco de un coordinador, se usa para señalización (Para informar de su presencia o definir los limites de un superframe.[1]

Acknowledgment Usado para la confirmación en la recepción de un marco.

MAC command Este es utilizada para administrar las operaciones de transferencia en el *Control de acceso al medio*.

[1] Una superframe es definida por beacons en su inicio y termino, esta clase de marco puede tener una parte activa y otra pasiva, en esta última el coordinador puede entrar en modo ahorro de energía.

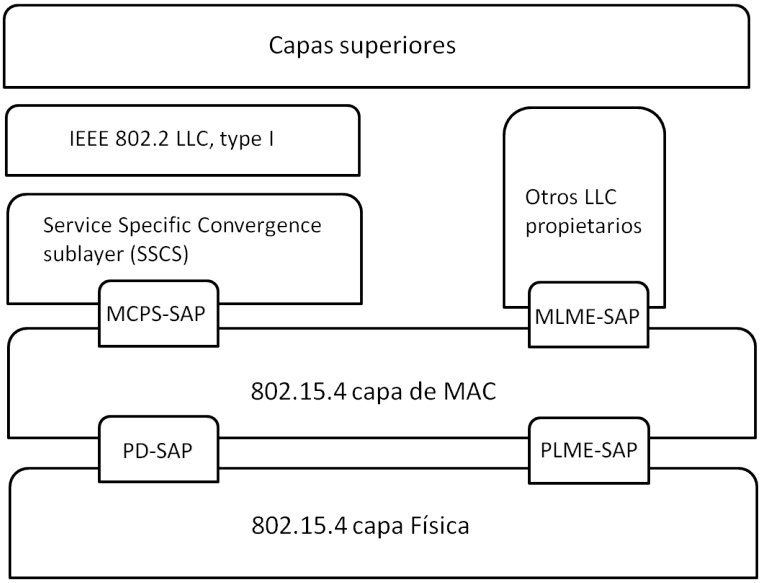

Figura II.1: Arquitectura de un dispositivo Low-Rate WPAN

El primer marco contienen información proveniente de la capa de aplicación, en la Figura II.1 se identifica como capas superiores. El segundo como ya se acoto hace funciones de señalización en el *MAC*. En tanto que el tercer y cuarto marco se originan en el *MAC* y se usan para comunicaciones punto a punto. Para mayor detalle en este tema favor de revisar el estándar IEEE 802.15.4 (LAN/MAN Standards Committee, 2006).

II.1.1 Topologías en el estándar

El *Dispositivo con funciones completas*, FFD y el *Dispositivo con funciones reducidas*, RFD son los dos tipos de dispositivos definidos por el estándar. El primero opera en tres modos en una Red de area personal (PAN): el primer modo opera como coordinador de la PAN, el segundo como coordinador y finalmente el tercero como dispositivo cliente. Otra de sus características es que un Dispositivo con funciones completas (FFD) establece comunicación con Dispositivo con funciones reducidass (RFDs) o con otros FFDs, en tanto que un RFD solo lo hace con dispositivos FFD. Las aplicaciones de los dispositivos RFD son realmente simples, como controlar una luz o en un sensor infrarrojo pasivo. Estas aplicaciones no tienen altos requerimientos en la transmisión de datos y su principal requerimiento es la asociación a la red mediante un FFD. Existe un tipo de nodo FFD llamado Nodo sumidero; por

sus características funcionales es a este dispositivo donde los flujos de datos generados por la red se dirigen. Este dispositivo cuenta con *handoff* vertical, característica que le permite la interacción con otro tipo de estándares de comunicación.

Dependiendo de los requerimientos de la aplicación, estas redes operan en dos topologías: tipo estrella y punto a punto. Ambas topologías se muestran en la Figura II.2. En la topología tipo estrella, la comunicación se establece entre los dispositivos y una unidad central controladora, llamada *PAN coordinator*. Una vez que el PAN es activado, tiene la capacidad para establecer su propia red, administrar conexiones de dispositivos RFD y recibir datos de los nodos asociados. Las redes de tipo estrella, operan de forma independiente, considerando que el identificador de la PAN no debe ser usado por alguna otra red en la esfera de influencia.

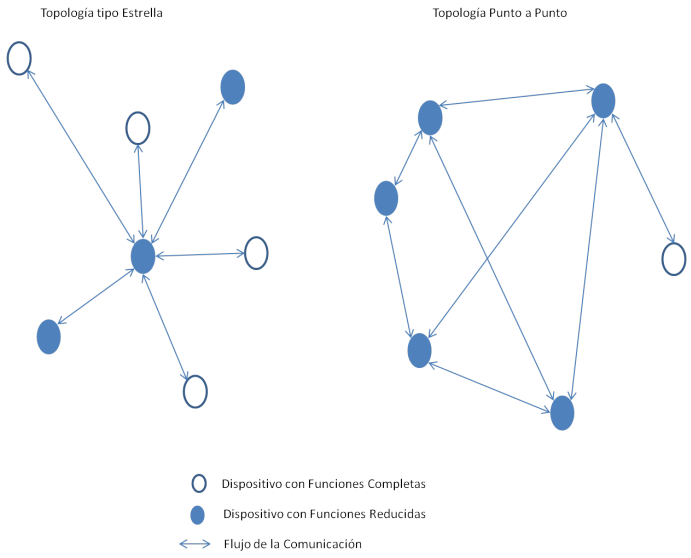

Figura II.2: Topologías propuestas en el estándar.

En la topología de red punto a punto, cada dispositivo es capaz de comunicarse con otros que se encuentren en su cobertura; las estructuras de la red son construidas fuera de la topología punto a punto, por lo que es posible fijar condiciones en la topología para formar la red.

Un ejemplo de la aplicación de la topología punto a punto es la red de árboles agrupados, en esta clase de redes la mayor parte de los nodos son FFDs, existiendo nodos RFDs, en la hojas del árbol, esta estructura obedece a que los nodos RFDs no tienen la capacidad de hacer funciones de nodo coor-

dinador. Cualquiera de los nodos FFDs actúan como nodos coordinadores y proveedores de servicios de coordinación a otros nodos o coordinadores. La forma simple de una red de grupos de árboles es una red formada solo por un grupo de nodos, aun así estas redes crecen hasta formar una red de varios vecindarios de nodos agrupados manteniendo un solo punto de conexión. El hecho de que tengan un solo punto de conexión hace que la latencia en la transmisión de mensajes crezca en proporción al diámetro de la red. Debido a este problema es necesario el uso de técnicas de encaminamiento que favorezcan la transmisión con baja latencia y bajo consumo de energía.

II.1.2 Topología jerárquica basada en niveles de seguridad.

Las topologías que el estándar define (estrella y punto a punto) permiten proponer esquemas adicionales, con consciencia de la seguridad para las interacciones que realizan los nodos. Considerando lo anterior, en la Figura II.3 se muestra la topología de red propuesta para un mejor rendimiento del protocolo propuesto. Esta topología permite tanto interacciones seguras como el ahorro de energía.

Esta estructura relaja la seguridad conforme se desciende en ella. El nivel inferior es conformado por nodos móviles, *mdevice*, que hacen uso de la red para la transmisión de paquetes. En este nivel no existen restricciones a los dispositivos móviles para formar parte de la red; permitiendo que el nodo móvil entregue sus credenciales para su validación, en un proceso exitoso de validación el proceso de encaminamiento ofrece una ruta entre el nodo móvil y el destino. El siguiente nivel comprende nodos, para los cuales la interacción con los niveles superiores tiene restricciones de acceso que son fijadas por los nodos pasarela *gwdevice*.

En la Tabla II.1 se describen cada uno de los elementos de la topología jerárquica mostrada en el Capitulo II.3.

Rol	Subgrafo	Dispositivo	Definición
sdevice	S	*Dispositivo Sumidero*	Provee conectividad entre WSN e Internet. El tráfico de entrada y el de salida, pasa a través de este dispositivo. En esta capa de la estructura, nodos no reconocidos o con bajos privilegios no pueden acceder a el.

Continua en la página siguiente.

Rol	Subgrafo	Dispositivo	Definición
gwdevice	W	*Dispositivo Gateway*	Administra las conexiones entre los *sdevices* y *vdevices*, para pertenecer a este grupo, los dispositivos deben tener una alta reputación, para ello consideramos la existencia de un sistema de immunización, el cual continuamente evalúa el comportamiento de los dispositivos *gdevice* (este es considerado, más no implementado).
vdevice	D	*Dispositivo Sumidero Virtual*	Dispositivo con iguales capacidades de un dispositivo sumidero; sin embargo no provee conectividad a Internet, ya que no tiene derecho para eso. Para desempeñar sus funciones, cuenta con acceso al conjunto de dispositivos gateway; por lo que, este dispositivo puede enviar paquetes y generar *tokens* para la autentificación de los dispositivos *mdevices*.
cdevice	G	*Nodo Coordinator*	Un conjunto de estos dispositivos constituye la dorsal inalámbrica de la red de sensores. Estos dispositivos administran las conexiones de los dispositivos móviles. Adicional a la anterior tarea, los *cdevices* ejecutan tareas de encaminamiento, por lo que contienen en sus procesos las capacidades de encaminamiento de Nucu evita el seguimiento. Este tipo de nodos evolucionan a nodos *vdevice*, una vez que estos han probado ser confiables para la nueva tarea; este cambio no es automático, sino que es motivado cuando es necesario contar con un *vdevice* adicional.
mdevice	M	*Nodo Móvil*	Su principal característica en su comportamiento es la movilidad, ello implica la existencia de mecanismos para administrar una sesión de datos y re-conexión entre nodos una vez que se sale del área de cobertura, para continuar con la transmisión sin perder la sesión iniciada. *Es importante decir que los resultados hasta ahora obtenidos no incluyen movilidad*.

Tabla II.1: Rol, Subgrafos, y sus definiciones en la estructura propuesta

En la estructura propuesta, el subgrafo S esta compuesto por el conjunto de nodos sumidero en G y el subgrafo D es el conjunto de nodos *vdevice*, tal que $D \subset G$ *and* $D \cap S = \emptyset$. En la solución propuesta, el conjunto D es clave, debido a que relacionan nodos seguros, *gwdevice*, con aquellos que no ha sido evaluado su comportamiento, *mdevice*.

II.1.3 Prestaciones de seguridad en el estándar

La naturaleza abierta de estas redes y los objetivos de bajo costo que se le asocian, imponen retos importantes a la implementación de entornos seguros. La Figura II.4 muestra la superficie susceptible

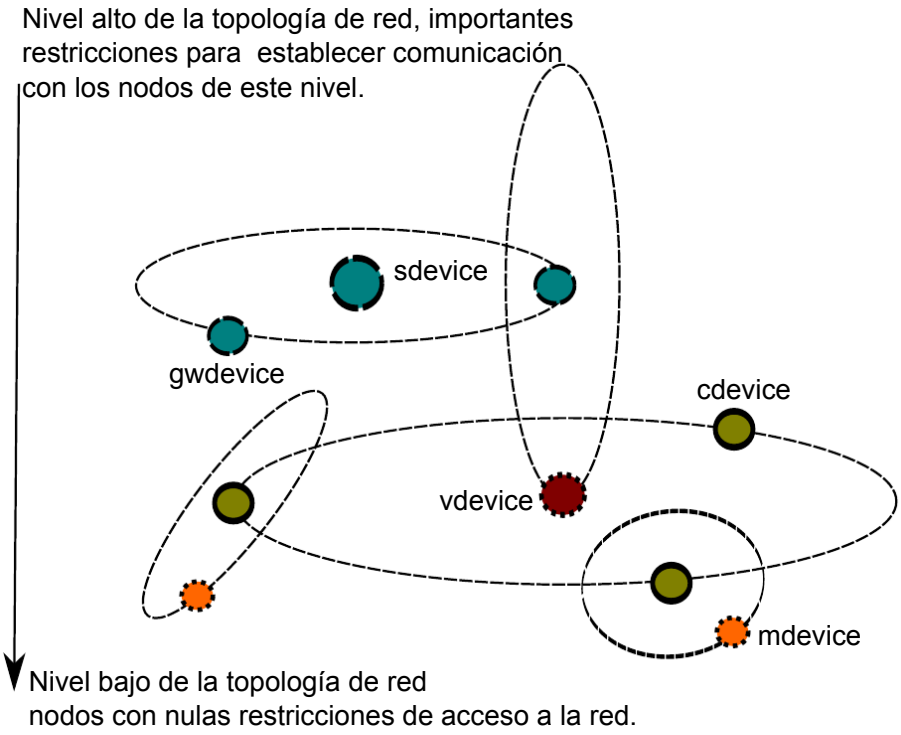

Figura II.3: Topología jerárquica basada en niveles de seguridad

de ataques en un dispositivo de esta clase de redes. Como se ve en la figura antes descrita (Figura II.4, los dispositivos de las WSN son vulnerables a ataques provenientes de la red, la adquisición de datos y los comandos de control. En términos de la espontaneidad en la presencia de estos dispositivos, generan relaciones de corto tiempo, esta característica dificulta la validación a dispositivos que se integran a la red. Las relaciones de confianza entre los dispositivos son presupuestas, fundamentadas en el hecho de que están en el mismo contexto y por ende que pertenecen a la misma red.

Los mecanismos de seguridad en el estándar están definidos para la topología tipo estrella; sin contar con ninguna previsión para redes descentralizadas. La topología que presentan las redes múltisalto es descentralizada, por lo que es necesario implementar mecanismos de control para llaves, cifrado de canal, etc, para extender el alcance de los mecanismos de seguridad ofrecidos por el estándar IEEE 802.15.4.

Para el cifrado de la información se proveen mecanismos criptográficos simétricos de 128 bits como máximo. Estos son definidos en su capa de seguridad y controlados por el *MAC*. El material

de seguridad, particularmente las llaves, se considera que las proveerán los procesos en la capa de aplicación por lo que el estándar no define ninguna consideración para hacerlo. Iguales condiciones existen para la configuración de los requerimientos de seguridad. Estos deben ser especificados en la capa de aplicación, por medio de los parámetros de control que se proponen para ello, permitiendo que puedan o no habilitarse, dando oportunidad a la administración y optimización de los recursos disponibles en el dispositivo.

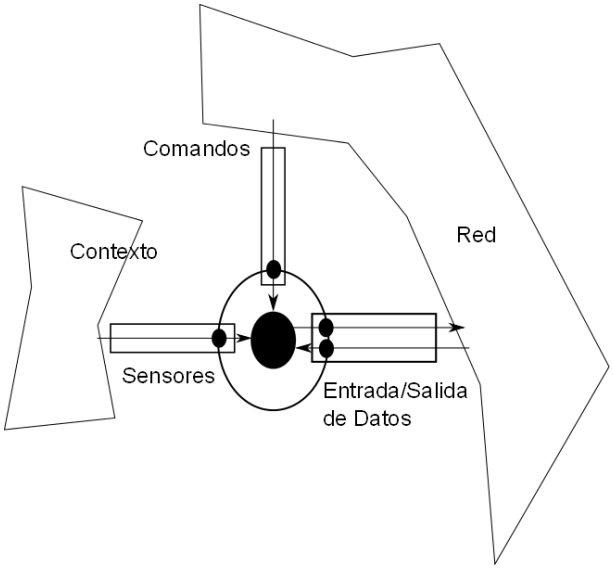

Figura II.4: Superficie de ataque de un dispositivo Low-Rate WPAN

II.1.4 Encaminamiento en una WSN

según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

La capa de red desde la perspectiva del modelo OSI, su misión es proporcionar conectividad y selección de ruta entre un nodo destino y un nodo fuente aún cuando no tengan conexión directa. Ofrece servicios a la capa de transporte y se apoya en las funciones del enlace de datos quién administra la

forma como se darán las interacciones entre nodos para la transmisión de paquetes. En una WSN con una topología diferente del tipo estrella (ver Figura II.2); donde el destino de los datos, desde un nodo fuente a un nodo destino, sigue más allá de sus vecinos a un salto es necesario el uso de mecanismos de encaminamiento. Estos mecanismos construyen caminos sujetos a restricciones o reglas previamente definidas, para buscar las mejores rutas en un escenario. Entre las restricciones más comunes refieren a umbrales de energía en los nodos y la distancia más corta que un conjunto de nodos ofrecen entre el nodo fuente y el destino. De forma genérica un camino se define como el subconjunto de nodos unidos al través de un subconjunto de aristas en una WSN G desde un nodo fuente s a un nodo destino d: $(v_s, v_{s+1}, v_{s+2} \dots v_d) \in V$ (camino simple).

En su funcionamiento los algoritmos de encaminamiento son clasificados como proactivos y reactivos, existiendo soluciones híbridas como lo describen los autores (Sohraby y otros , 2007). Los algoritmos proactivos buscan proveer de forma constante de rutas frescas, este comportamiento las hace sumamente demandantes para los recursos de las WSNs. Los algoritmos reactivos, por su parte, reaccionan a un requerimiento de transmisión de datos, haciéndolos más amables con dispositivos de la WSNs.

El uso de algoritmos exactos como el algoritmo de *Dijkstra*, (Descripción del algoritmo se encuentra en (Cormen y otros , 2001) en las WSNs no es una solución adecuada por las capacidades de los dispositivos y el incremento en los requerimientos de recursos conforme las redes crecen. El anterior comportamiento en el algoritmo obedece a que es necesario el almacenamiento de las tablas de encaminamiento hacia los diferentes nodos de la red.

Sohraby y otros , 2007 proponen una clasificación de los protocolos de encaminamiento asociada a los escenarios donde ejecutan su tarea, en su clasificación incluyen las características que en el escenario encuentran y de las cuales toman ventaja para su funcionamiento:

Red Plana En esta arquitectura de red, todos los nodos se consideran como pares. Estas redes presentan diversas ventajas, tales como mínima sobrecarga para el mantenimiento de la estructura de la red, así como mayor potencial para el descubrimiento de caminos, ya que no se restringe a grupos de nodos, más aun, reduce la posibilidad de fallas en los caminos, ante una mayor posibilidad de conexión.

Red por grupos En esta red los nodos se organizan en grupos, donde en cada grupo, un nodo con mayor cantidad de energía u otra característica que sea de interés, asume las actividades de coordinación, convirtiéndose en la cabeza del grupo. Este nodo no solo coordina las actividades al interior del grupo, además realiza tareas de comunicación entre diferentes grupos. La mayor aportación en esta organización es el ahorro de energía.

Data-centric Este clase de algoritmos utiliza una *nomenclatura basada en atributos*: el nodo sumidero envía una petición o interés de datos a la red; los nodos sensores que tienen los datos solicitados responden a la petición, pero la información es encaminada ejecutando un procedimiento de agregación/consolidación. Estos algoritmos ofrecen un agregado de la información solicitada, el cual se conforma de la información adquirida de múltiples fuentes. Para la transmisión del acumulado de los datos se utilizan métodos: *broadcasting*, basado en atributo, *multicasting*, *geocasting* y *anycasting*.

Geográficos Estos algoritmos consideran la localización de los nodos para direccionar a ellos. De aplicación en escenarios donde la localización del fenómeno es de interés para el usuario de los datos.

En redes con escenarios dinámicos, como las WSNs, las técnicas estáticas de generación de rutas no ofrecen la mejor solución y suelen muy caras computacionalmente hablando, es decir requieren ejecutarse mucho tiempo de forma continua, ya que las condiciones del escenario cambian constantemente, y el número de combinaciones necesarias para encontrar el camino optimo hace el problema complejo o intratable.

Ofreciendo una solución para esta clase de escenarios, surgen los algoritmos basados en heurísticas los cuales se describen en los trabajos de Zanakis y Evans, 1981 y Onwubolu y Babu, 2004. Ejemplo de ellos son los protocolos de encaminamiento bioinspirados (Saleem y otros , 2011; Villalba y otros , 2010). En las conclusiones de su trabajo de investigación, figura el hecho que los algoritmos ACOs son los más favorecidos frente a las diversas *metaheurísticas* propuestas en la literatura, (Para información que le permita introducirse en el tema referirse a (Glover, 1986) y (Osman y Laporte, 1996)) ello debido a las características de exploración y mantenimiento de caminos por parte de los hormigas desde el hormiguero hasta la zona de alimentación.

Por la importancia que los mecanismos de encaminamiento tiene en el comportamiento de la red y la transmisión de datos, diversos autores han asegurado:

- Los datos del proceso de encaminamiento de los flujos de datos,
- Protección de los nodos fuente y sumidero,
- Parámetros para la construcción de la ruta,
- Los datos que se transportan.

Los autores Karlof y Wagner, 2003 del articulo "Encaminamiento seguro en redes inalámbricas de dispositivos para adquirir datos del contexto: ataques y contraataques"[2], describen una serie de protocolos de encaminamiento con capacidad de proteger la red de ataques se consolidan en la capa de red.

Las soluciones de encaminamiento con consciencia de seguridad, justifican su existencia en el hecho de que un mal funcionamiento debido a ataques de intrusos, reduce de forma substancial el rendimiento de la red. En el tema de privacidad los autores Shaikh y otros , 2010 describen una serie de soluciones cuyo objetivo es proveer privacidad, esencialmente *soluciones centradas en el usuario y las relacionadas con computación pervasiva*, aplicaciones que forman parte de las nuevas tendencias en el uso de las WSNs.

II.2 Servicios de monitorización a través de una WSNs

Las redes de sensores han probado su pertinencia en muy diversas áreas. Cada una con requerimientos específicos en la recolección, procesamiento y transmisión de los datos. En su primera etapa de uso, los dispositivos que conformaban una WSN, eran nodos estacionarios, adquiriendo información de eventos que ocurrían en su esfera de cobertura, lo que les permitía describir su contexto, respecto a un parámetro o parámetros de monitorización, tales como temperatura, ruido ambiental, contaminación, movimiento de animales, presencia de incendios en bosques etc. Estas redes por la forma cómo los dispositivos y los usuarios de la información generada por la red interactúan, se clasifican como *centradas en los datos*, característica definida por Stojmenovic, 2005, como el conjunto de soluciones de

[2]Secure routing in wireless sensor networks: attacks and countermeasures

las cuales las personas son usuarios externos de la información que se genera, sin una relación que los asocie con el área de interés.

Sin embargo, el uso de esta tecnología de red se ha filtrado a los escenarios que integran movilidad. Característica que diferencía de las aplicaciones de la primera etapa.

En la Tabla II.2 se muestra una taxonomía sobre la evolución que los dispositivos que conforman las Low-Rate WPANs y cómo esta tecnología ha migrado de su aplicación en sitios agrestes con casi nulo soporte por parte de personal técnico a escenarios, donde es muy valorada su reducida intrusión en las actividades del usuario.

Características	Tradicional WSNs	Centrada en el usuario WSNs
Hardware	Hardware especifico.	Hardware básico con capacidad de expansión.
Funcionalidades	Totalmente automático Sistemas autónomos.	Flujos interactivos de datos entre la fuente y el servicio de monitorización.
Numero y tipo de dispositivos	Miles de dispositivos cubriendo área especificas.	Dispositivos heterogéneos monitorizar variables fisiológicas y actividades variables.
Portabilidad	Dispositivos fijos.	Dispositivos móviles y fijos asociados a humanos.

Tabla II.2: las WSNs y la evolución de sus aplicaciones

Aun cuando las WSNs presentan características físicas apropiadas para ser usadas en aplicaciones centradas en el usuario, existen retos en materia de: energía, procesamiento y cantidad de datos que pueden transportar; que deben ser resueltos para prestar servicios con la calidad requerida. Adicional al manejo de los datos y su transmisión, existen los problemas de privacidad asociados a la arquitectura abierta en las redes de sensores como ya se explico en la sección II.1.3 y los requerimientos legales de protección a los datos que deben ser cubiertos por los sistemas que administren Información de identificación personal (PII) por sus siglas en inglés.

II.3 Discusión

Las características que el estándar ofrece a la seguridad y privacidad de los datos, dejan importantes tareas por realizar en las capas superiores. Aun cuando es posible asegurar los datos que se transmiten, se deben de implementar mecanismos que permitan la protección del material de seguridad que provee el aseguramiento de los datos. Otra de las condiciones es que el estándar define claramente en el aseguramiento en topologías tipo estrella, sin embargo para otro tipo de topologías no hace ninguna consideración.

El estándar también provee de mecanismos de configuración, que permiten obtener diferentes niveles de seguridad. La flexibilidad que las hace atractivas para ser utilizadas en soluciones que provean privacidad y permitan la configuración personalizada en el servicio que prestan a los usuario por las capas de aplicación, como mencionan los autores Dey y otros , 2010. Esta investigación no hace intención para modificar el estándar que sirve como caso de uso. Ante esta premisa, es una ventaja la nula definición de mecanismos más allá de la capa de enlace, aun cuando el estándar provee de una breve descripción de la forma como deberían realizarse las interacciones en las dos topologías que propone, esta condición nos permite incluir nuestra propuesta sin interferir en las definiciones existentes. 45

CAPÍTULO III

ESTADO DEL ARTE.

En esta sección se describen soluciones cuya característica es la integración de mecanismos de privacidad en la capa de red; proponiendo una solución al problema de *Obtención no autorizada de la ubicación de la fuente de datos en WSN*. Estas soluciones agregan a los protocolos de encaminamiento, consciencia para proteger la ubicación de la fuente; modificando su comportamiento básico, mediante consideraciones que aun cuando les restan efectividad en algunos de sus parámetros (por ejemplo incremento de la latencia); el objetivo es lograr un balance entre la privacidad ofrecida y las características de las rutas generadas.

III.1 El adversario.

Un adversario para esta investigación, es un agente cuyo objetivo es poner al descubierto la ubicación del nodo emisor de datos. Agregando efectividad a otras estrategias de ataque, sea en el espacio virtual o en el espacio físico.

III.1.1 Tipos de Adversario

Para ejecutar el ataque un adversario, cuenta con diferentes capacidades para hacerse de información que le permita consolidar su ataque, considerando la forma como interactúa con los actores en el escenario se clasifican como:

Adversario Global; tiene acceso a todos los nodos y enlaces en la red, por lo que es capaz de acceder a toda la información que la red genere. En contra parte, un *adversario local*, solo tiene acceso a los datos, nodos y enlaces de una porción de la red. Estos conceptos también pueden ser asociados a la veracidad de la información que recibe; donde uno global siempre recibe datos verdaderos, en tanto que uno local se refiere a qué la información a la cual tiene acceso su veracidad es parcial.

Adversario pasivo/externo, este adversario no forma parte de la red; solo escucha los mensajes transmitidos por ella; típicamente es invisible, logrando mayores daños conforme su invisibilidad se prolonga. *Este adversario solo compromete los canales de comunicación entre los nodos*.

Ataque	Objetivo	Defensa
Análisis de tráfico	Observar el tráfico	Ocultar los patrones de tráfico.
Temporalidad	Examina las rutas y cuando se usan	Transmisiones por lotes.
Contenido	Extraer e identificar la información	Cifrado.
Conteo	Duración de la transmisión	Ocultar los patrones de tráfico.
Intersección	Descubrir tiempos de actividad	Distribuir mensajes en la escala de tiempo.

Tabla III.1: Ataques y defensas (Adversario Pasivo)

Adversario activo/interno, este adversario es visible al interior de la red, con capacidad para alterar los paquetes que son transmitido a través de la red y para controlar los nodos.

Típicamente un adversario es dinámico, siguiendo diferentes estrategias para fortalecer su ataque; por ejemplo: iniciar con la recolección de información respecto a las restricciones que el algoritmo de encaminamiento, considera para la selección de las rutas e información respecto a la actividad de la

Ataque	Objetivo	Defensa
Análisis de tráfico	Modificar y retrasar el tráfico Dividir los flujos de tráfico	Definir un tiempo de vida en las transmisiones. No se cuenta con defensa para ello.
Denegación de Servicio (DoS)	Degradación del rendimiento y el anonimato	Moneda Digital o acertijos.
Etiquetado	Modificar mensajes	Verificación de integridad.
Colusión	Comprometer segmentos de red o grupos de dispositivos	Tirar mensajes.
Sybil	Controlar caminos	Ninguna.
Reputación	Denegar el acceso, evitar su presencia	Moneda Digital o acertijos.
Replay	reuso de mensajes validos	Uso de nonces[1] o etiquetas de tiempo.

Tabla III.2: Ataques y defensas (Adversario Activo)

red, comprometiendo los nodos y los enlaces. Emplea bastante de sus cursos para inferir quien recibe o envía un mensaje, bien sea dentro de los límites del cómputo o fuera de ellos.

Un adversario puede ser determinista. Esto implica que tiene un plan de ataque programado probabilísticamente, dependiente de la frecuencia relativa de la secuencia de acciones o eventos observados; o no determinista, esto significa que se desconoce el comportamiento que sigue su plan de ataque.

El *modelo de la amenaza* está constituido de la combinación de los tipos de adversarios y la forma cómo interactúan para generar una estrategia exitosa. Un modelo de amenaza fuerte, es aquel con capacidad para comprometer los nodos (adversario interno) y los enlaces (adversario externo), observar todo el tráfico de la red (adversario pasivo con un alcance global), alterar el tráfico (adversario activo) mezclando todas estas capacidades en su operación (Danezis y otros , 2003).

Diseñar una solución con capacidad para sobreponerse a un ataque como el descrito en el párrafo anterior, se corre el riesgo de obtener resultados no deseados. *Por lo tanto en el diseño de sistemas que permitan proteger la privacidad y la seguridad, se realiza con un modelo especifico de amenaza en mente,* intentando resolver puntos críticos asociados al tipo de información que maneja el sistema.

En cualquier modelo de ataque que sigan los adversarios, su objetivo siempre es asociar un emisor con un receptor, identificar al emisor o receptor para un tipo particular de mensaje o seguir el camino que los mensajes entre dos entidades intercambian.

La Tabla III.3 muestra una aproximación general a los tipos de ataque, que son susceptibles de sufrir los actores en el escenario de una transmisión de datos. La perpetración exitosa de un ataque en

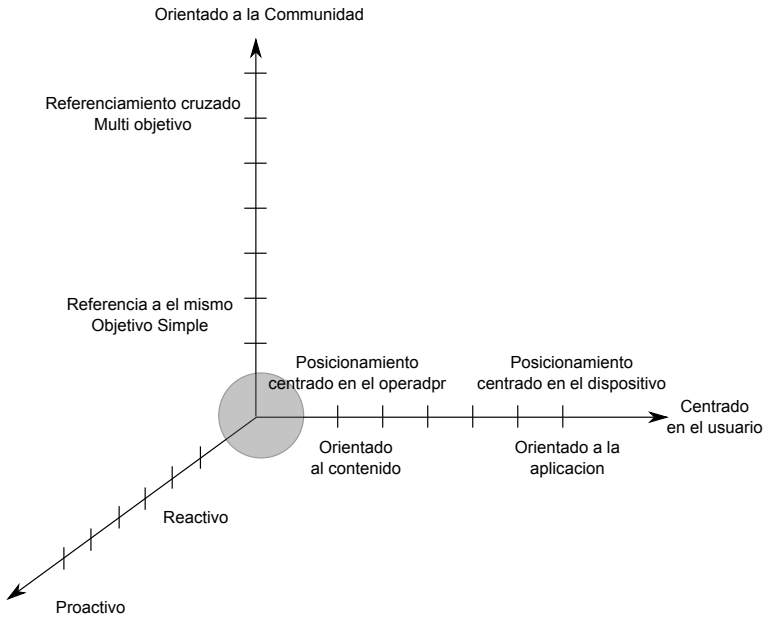

Figura III.1: La evolución de los servicios de localización.

el destino, diferirá la magnitud del daño causado en función de del arreglo de los servicios, distribuida o centralizada, en tanto que en el nodo fuente el daño esta asociado a las expectativas del adversario y las características del SOI u IOI.

III.1.2 Estrategias de ataque en la literatura para el problema estudiado

En trabajos de Kamat y otros , 2005 y Ozturk y otros , 2004 se definen dos tipos de adversario basados en el juego *The Panda Hunter*, que sirvieron para probar la efectividad de sus propuestas al proteger la ubicación del nodo fuente. Los adversarios antes referidos también fueron empleados por las soluciones sintetizadas en la tabla III.4. Sus características se describen a continuación:

Adversario Pasivo, a_p**.** El ataque se inicia en el nodo sumidero; en este lugar el adversario espera por eventos, una vez que detecta uno, sigue el camino hacia la fuente inmediata del evento, este proceso se repite hasta el punto donde encuentra el nodo, fuente de las transmisiones.

Adversario Cauteloso, a_c**.** Este adversario es muy similar al adversario pasivo, la diferencia reside en que *solo espera un tiempo t en un mismo lugar*; una vez que este tiempo transcurre, sin detectar

Objeto	Tipo de Amenaza
Fuente	Adquisición de datos. Ejecución de procesos. Exposición de Información de localización. Exposición de Información del tipo de dispositivo. Acceso de entidades ajenas. Entrada de datos no requeridos.
Red	Escucha del tráfico de datos (Ataque pasivo). Re-direccionamiento del tráfico de datos con la intención de adquisición de los mismos(Ataques activos).
Destino	Los tipos de amenazas son iguales a las que esta expuesta fuente de datos. Con excepción del punto 3 para plataformas centralizadas. (ver Figura III.1).

Tabla III.3: El objetivo del adversario en un sistema de comunicación y los tipos de daño.

un evento más, el adversario regresa un salto a la vez, siguiendo el camino antes recorrido. El algoritmo se detiene cuando el adversario encuentra un nodo fuente de datos o se ha finalizado el tiempo de transmisión.

III.2 Privacidad en la ubicación en WSN

Un trabajo que aborda el tema de forma exhaustiva es el propuesto por los autores Rios y Lopez (2011), que aborda los trabajos más representativas; así como los retos que aun deben ser resueltos en materia privacidad en WSNs.

Existen tres perspectivas en la literatura desde las cuales se investigan soluciones a este tema:

Privacidad en la ubicación del destinatario es necesario deducir la información que permita a una persona no autorizada conocer la ubicación del dispositivo destino. La importancia de proteger este nodo en redes múltisalto, se debe a que el dispositivo destino o nodo sumidero se encarga de interconectar dos clases de tecnologías de red (Figura III.2), una desactivación de este nodo implica el aislamiento de la red. Algunos trabajos realizados con este objetivo son propuestos por: (Jian y otros , 2008), ellos presentan un algoritmo de encaminamiento, con consciencia de la privacidad en la ubicación del destino. En los nodos pasarela, habilitan un protocolo al cual llaman LPR (Location-Privacy Routing Protocol). El objetivo de este algoritmo es evitar los ataques de tipo *packet-tracing*. LPR genera caminos con longitudes mayores al *camino más corto*, lo que deriva en un mayor consumo

de energía, por lo que proponen un mecanismo que permite negociar el factor de privacidad ofrecido al realizar transmisiones. Nezhad y otros , 2008 proponen un algoritmo llamado *Destination-Controlled Anonymous Routing Protocol for Sensornets* (DCARPS), con el mismo objetivo del algoritmo antes descrito.

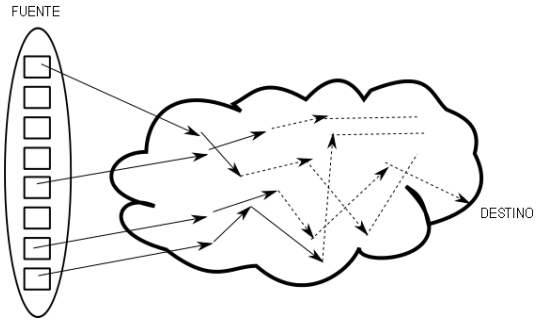

Figura III.2: Privacidad en la ubicación del nodo destino.

Privacidad en la ubicación del origen, Figura III.3. Estas soluciones buscan proteger la ubicación del nodo fuente de la transmisión. Existen dos lineas para evitar este daño, la primera solución es ofrecida a través de la reducción de información que un paquete puede proporcionar respecto al nodo fuente; otra clase de protección es implementada durante el encaminamiento. La protección asociada a mecanismos de encaminamiento intenta evitar los ataques pasivos a la escucha de las transmisiones en la red.

Para ofrecer protección en las debilidades antes citadas se han propuesto soluciones como la de los autores (Ozturk y otros , 2004) y (Kamat y otros , 2005) embebiendo mecanismos de privacidad en la capa de red, otros autores que exploran el mismo problema y ofrecen una solución son (Rios y Lopez, 2011) proponen una solución con consciencia del contexto.

Un tercer tipo se refiere al *anonimato en la Comunicación*; esto significa que no es posible relacionar un mensaje en particular con un par de nodos emisor-receptor, así como un mensaje no puede ser asociado a un par de nodos en particular. El diagrama de esta clase de protección a la privacidad se puede ver en la Figura III.4. Para ofrecer este tipo de privacidad se usa un mecanismo llamado Mix-Networks. Una selección de trabajos representativos asociados a este problema es propuesta por (Sampigethaya y Poovendran, 2006).

Es del interés de esta investigación, explorar la problemática asociada con la protección de la

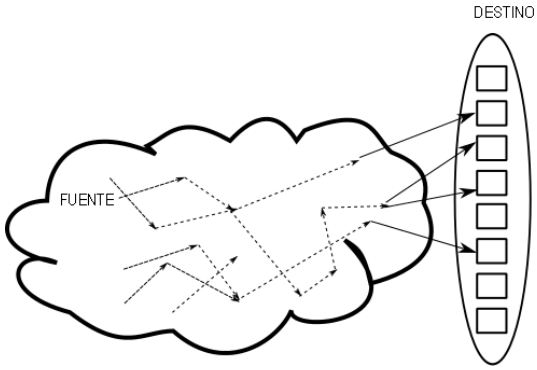

Figura III.3: Privacidad en la ubicación del nodo fuente.

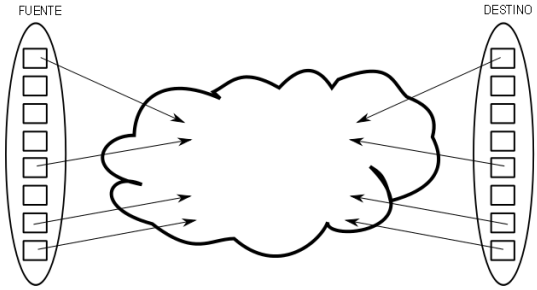

Figura III.4: Anonimato en la comunicación.

privacidad en la capa de red y la ubicación del dispositivo fuente.

III.3 Consciencia de la privacidad en la capa de red

Introducir consciencia de privacidad a las transacciones que se realizan en la capa de red requiere el desarrollo de mecanismos, con capacidad para proteger de usuarios no autorizados en los siguientes tres aspectos:

- Ubicación del emisor.
- Ubicación del receptor; en algunas ocasiones del par emisor-receptor como se mostró en la sección III.2.
- Privacidad en los datos, esto incluye la identidad del emisor; existen propuestas muy maduras en ese punto, atendidas mediante mecanismos de cifrado, (Chaum, 1981), (. Dierks CerticomT.

DIERKS CERTICOM and C. Allen).

Agregar consciencia de la privacidad en la capa de red no es una tarea trivial. Esto se debe a las restricciones que existen en las WSNs, descritas ya en el Capitulo II. La consciencia integral de privacidad en la ubicación considerando la fuente, el destino y en los datos es una tarea compleja. Este trabajo se centra en ofrecer privacidad en la ubicación del dispositivo emisor. En las siguientes secciones describiremos las técnicas de encaminamiento que se han propuesto para la protección de la privacidad en la ubicación del dispositivo emisor.

III.3.1 Señuelos para mejorar la privacidad

Para proveer protección a la privacidad en los aspectos descritos en la sección anterior, para las redes de sensores se han propuesto diversos mecanismos satélite a los mecanismos de encaminamiento y transmisión de paquetes en la red. Ejemplos de estos son:

las fuentes falsas, nodos que inician la generación de flujos como si se tratara de paquetes reales. Para incrementar su efectividad, deben de considerarse aspectos como, su ubicación respecto a las fuente, frecuencia de los mensajes, cantidad de mensajes, dirección de los mensajes, entre otros aspectos que permitan ofrecer fortaleza ante análisis estadísticos del tráfico generado.

Generación de paquetes falsos a través de la red se transmiten paquetes con datos no reales. Una variante de este tipo de tráfico es usado por los autores (Luo y otros , 2010), ellos proponen la generación de paquetes bajo dos consideraciones: la primera es que este mecanismo se activa, si existe una transmisión de un paquete real, la segunda condición esta sujeta al nivel de energía existente en los nodos. Si el umbral mínimo de energía no ha sido alcanzado se aplica la probabilidad de transmisión.

III.3.2 Encaminamiento por *Caminar Aleatorio* (Random Walk)

Los mecanismos basados en la técnica de *Caminar Aleatorio* (Random Walk), introduce aleatoriedad en el proceso de selección del nodo destino en el vecindario, que es una característica empleada para proteger la privacidad en la ubicación de la fuente de datos. De este mecanismo se consideran dos vertientes; uno de ellos es llamado *Caminar Aleatorio Puro*, no es estadísticamente seguro, ya que el nodo seleccionado como destino inmediato de la transmisión, después de un número h de saltos se

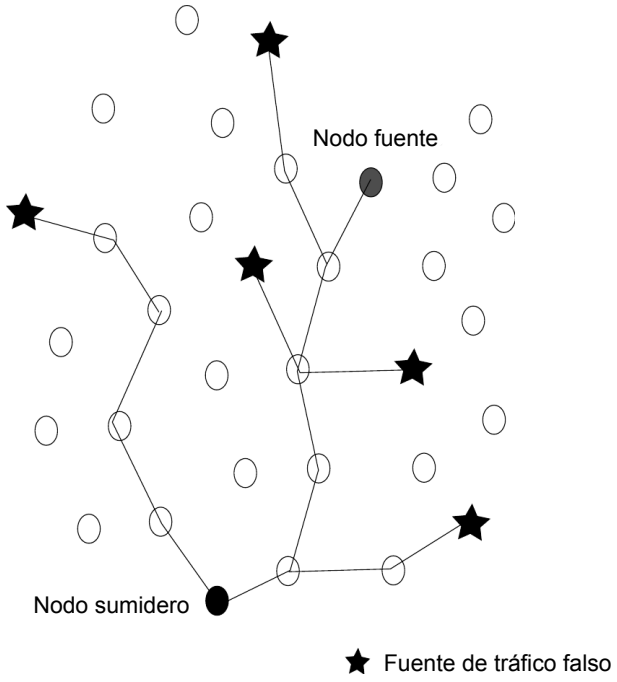

Figura III.5: Fuentes de tráfico falso.

localiza en el área del nodo fuente como lo demuestran los autores (Kamat y otros , 2005). La segunda variante, se refiere a modificaciones que se han realizado al algoritmo de *Caminar Aleatorio* con la intención de proveer privacidad (A sector-based directed random walk y A hop-based directed random walk).

El primero requiere que cada sensor sea capaz de dividir un plano bidimensional, en dos planos, usando nodos de referencia que permitan realizar la tarea antes mencionada. El segundo tipo de Caminar Aleatorio requiere que cada nodo conozca el número de nodos que existe entre el y el nodo sumidero. Ambas soluciones proveen privacidad, pero ello no significa que el nivel sea aceptable.

III.3.3 Encaminamiento por Inundación

El uso de técnicas de inundación para hacer llegar los paquetes de un nodo fuente a un nodo destino es una de las técnicas más simples de implementación, además de ser factible para muchos de los escenarios clásicos propuestos para las WSN. Una de las principales ventajas de este método es el

incremento de la confiabilidad en la entrega de los paquetes ya que cada paquetes será reenviado al menos una vez, por cada uno de los nodos en la red. Sin embargo, el reenvío no controlado de paquetes ocasiona el problema conocido como *broadcast storm*; dando lugar a tres grandes deficiencias en el algoritmo:Implosión, Traslape, No consideraciones de los recursos existentes en los nodos, problemas que se describen a continuación.

Implosión Debido a que los nodos entregan paquetes empleando broadcasting, el mismo paquete alcanza el mismo nodo via diferentes rutas. Cuando un nodo recibe un paquete, este no verifica si el mismo lo ha recibido más de una vez, característica que provoca que un mismo paquete sea enviado a un mismo destino más de una vez.

Traslapar Cuando dos nodos detectan el mismo evento, ambos pueden enviar los datos generados al nodo sumidero. Lo cual puede causar que el nodo sumidero reciba información duplicada.

No consideraciones de los recursos No existe una sola consideración respecto a los recursos en el mote sea de energía o capacidad de procesamiento.

Para proteger la privacidad de la ubicación de la fuente en una red inalámbrica múltisalto la técnica por inundación no es una solución adecuada Xi y otros , 2006a. Para explicar el problema que presenta la técnica de inundación al ser usada para proveer privacidad en la ubicación de la fuente, se propone el siguiente escenario:en una *WSN* existe un nodo que es una fuente de datos, este nodo envía un número fijo de paquetes en un tiempo t hasta un nodo sumidero; cada uno de los paquetes es etiquetado con un valor consecutivo al ser enviados por el nodo fuente. Un adversario se ubica en un nodo i de la red y se queda ahí en espera de recibir dos paquetes etiquetados con números consecutivos, para calcular cual es el tiempo que le toma al segundo paquete en arribar. El resultado de esta evaluación se considerará un valor constante para el arribo por paquete. Reproduciendo esta evaluación en cada uno de los nodos de la red, un adversario cuenta con suficiente información, para deducir la ubicación del nodo fuente.

III.3.4 Técnicas de encaminamiento Phantom.

Estas técnicas fueron introducidas por Ozturk y otros (2004) y Kamat y otros (2005), representando un hito en algoritmos enfocados a la protección de la privacidad. Phantom divide su comportamiento

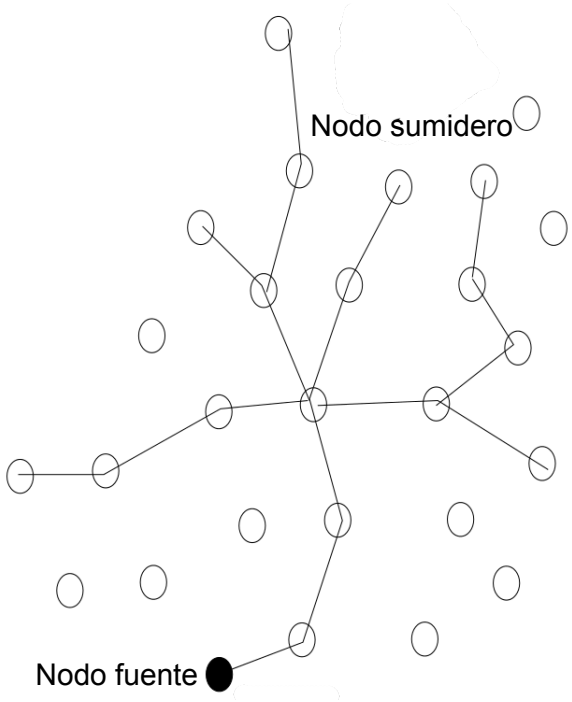

Figura III.6: Encaminamiento Phantom.

en dos fases, como se muestra en la Figura III.6; la primera hace uso de la técnica llamada *Caminar Aleatorio* (Random Walk), en la segunda fase, su estrategia es usar *Caminar Dirigido* para la transmisión de paquetes. Una vez que los paquetes han sido retransmitidos un número predefinido de saltos, h_{walk}; el nodo al cual arriban los paquetes después de haber finalizado su primera jornada, se le llama *phantom node*. En este punto, el algoritmo de encaminamiento cambia su estrategia e inicia a emplear la técnica de transmisión de paquetes llamada *inundación probabilística* para alcanzar el nodo sumidero.

De la anterior técnica los autores concluyen que: *Cuando las distancias entre el nodo sumidero y el nodo fuente son grandes, existen mayores posibilidades de proteger la privacidad del nodo fuente*. La energía consumida es un problema importante en este algoritmo debido al uso de la técnica de inundación. Existe un problema adicional relacionado con las transmisiones reales, ya que la relación entre paquetes reales y los debidos a la inundación no son uniformes y esta ultima técnica normalmente se apodera del canal de comunicaciones, lo cual incrementa los parámetros de paquetes perdidos y

paquetes tirados por la pila del mote.

Los autores Li y Ren (2010) para proteger la ubicación de la fuente de datos proponen tres diferentes técnicas de encaminamiento: a)(source-location privacy through routing to a random intermediate node (RRIN), b) source-location privacy through angle-based multi-intermediate nodes, c) source-and location privacy through quadrant-based multi-intermediate node). Las propuestas usan encaminamiento dinámico; las soluciones generan rutas usando dos fases para alcanzar al nodo sumidero. Sin embargo, una de sus soluciones requieren calcular funciones trigonométricas, números aleatorios, operaciones de punto flotante, la mayor parte de estos cálculos con altos requerimientos de computo. No se propone un mecanismo de encaminamiento para la segunda fase en las soluciones, los autores solo comentan que es necesaria.

En el mismo articulo, los autores explican que el primer algoritmo tiene un problema de seguridad en la selección del nodo RRIN; el problema de seguridad emerge porque se considera la distancia entre el nodo fuente y el RRIN como parámetro de selección de este último. Para reducir el daño a la seguridad ocasionado por la forma de selección del RRIN, Li y Ren (2010) exploraron la selección totalmente aleatoria del nodo intermedio; sin embargo conforme el periodo de seguridad crece, también se incrementan los parámetros de latencia y mensajes tirados por las pilas.

Grow routing (GROW) es un algoritmo propuesto por Xi y otros (2006a). Ellos usan *caminos aleatorios usando la heurística voraz* y técnicas phantom. En la primera fase, el algoritmo construye una ruta desde el nodo sumidero hasta un nodo alejado de el definido con anterioridad. Esta ruta es un señuelo para los dispositivos que pertenecen a la WSN; cada uno de los nodos que pertenecen a esta ruta, se convierten en el punto donde el procedimiento de encaminamiento de paquetes cambia, siguiendo la filosofía de los algoritmos Phantom; los paquetes que arriban a la ruta señuelo solo la siguen hasta el nodo sumidero.

Adicional a la técnica del camino señuelo, los autores proponen el uso de *paquetes falsos con consciencia del nivel de energía;* esto significa que los nodos solo envían esta clase de paquetes, si un umbral de energía mínimo no ha sido alcanzando. Según los resultados obtenidos por los autores de GROW, este algoritmo ofrece condiciones para la privacidad; pero la entrega exitosa de los paquetes al nodo sumidero, no es garantizada porque depende de que el paquete alcance un nodo de la ruta señuelo, más aun la existencia de la ruta esta sujeta a la cantidad de energía contenida en los nodos, ya

que no se menciona, respecto a procesos que se encarguen del mantenimiento de la ruta. Los autores comentan dos faltas en el algoritmo: La primera asociada al uso de *caminos aleatorios*, lo cual hace posible que los paquetes retornen a la fuente; el segundo caso se refiere a las rutas de longitud mínima, ya que los nodos cerca del nodo sumidero producen transmisiones no seguras.

Los autores Shaikh y otros , 2010 en su propuesta consideran la protección de la privacidad de la identidad y de la ubicación. Su algoritmo considera restricciones en la memoria y en la energía almacenada en los dispositivos de las WSNs. En este algoritmo solo nodos confiables forman parte de las rutas; la condición de confianza se evalúa por medio de los paquetes enviados de forma exitosa por el nodo. Para medir el nivel de privacidad ofrecido, introducen un nuevo parámetro llamado diversidad en los caminos, un valor alto en este parámetro, implica un mayor nivel de privacidad cuando el adversario realiza ataques del tipo *backtracking*. En las conclusiones los autores establecen que, altos niveles de privacidad están fuertemente asociados a alta latencia en las transmisiones.

Existen otras soluciones en la literatura que proporcionan protección a la fuente de datos y anonimato en las transmisiones, esta última característica no es de interés para esta investigación, ya que existen soluciones que requieren conocer la identidad y la ubicación de la fuente de datos considerando restricciones para usuarios no autorizados. Sin embargo, estos trabajos sirvieron de fundamento para algunos de los mecanismos propuestos:

- the Onion Routing tOR Dingledine y otros (2004) .
- Crowds Reiter y Rubin (1998).
- Tarzan Freedman y Morris (2002).

III.3.5 Técnicas de encaminamiento Oportunista

En muchas de las aplicaciones de redes de sensores, los nodos forman redes no-conectadas debido a la movilidad de los nodos, la forma como los nodos son desplegados en el escenario y la pérdida de la conexión por la atenuación de la señal, cese de transmisiones, recepción con la intensión de conservar energía, entre otras condicionantes que dan como resultado la pérdida de la conectividad.

En el contexto antes descrito, surgen los protocolos de encaminamiento oportunista, los cuales siguen un patrón de encaminamiento *almacenar, cargar y enviar después* (Store-Carry-Forward), por

lo que se consideraran decisiones en las retransmisiones de forma local e independiente. La Figura III.7 muestra la interacción de un nodo con sus vecinos temporales. Por la forma como interactúan con el contexto se clasifican como: (i) Sin consciencia del contexto (ii) Parcialmente conscientes del contexto (iii) Totalmente conscientes del contexto. Sus principales aplicaciones son: (i) redes Redes tolerantes al retardo (DTN) (Fall, 2003) (ii) Redes de intercambio de datos en dispositivos de bolsillo (PSN) (Hui y otros , 2005) (iii) red con consciencia de las relaciones sociales en la comunidad (socio-aware community network) (Dinh y otros , 2009).

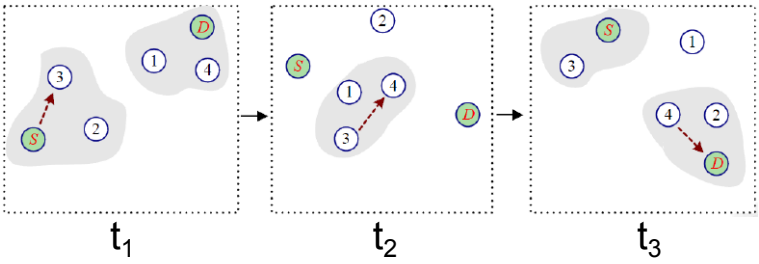

Figura III.7: Proceso de encaminamiento de paquetes, usando encaminamiento oportunista.

Los autores Spachos y otros (2010) proponen usar técnicas de *encaminamiento oportunista*; considerando las condiciones cambiantes del medio inalámbrico y las características de los dispositivos (ancho de banda y disponibilidad de los nodos). Los paquetes toman diferentes rutas para alcanzar el nodo sumidero ya que existen cambios en los nodos intermedios (nodos seleccionados para transmitir los datos). Mediante este mecanismo se alcanzan dos objetivos: Los paquetes seleccionan las mejores rutas, según los parámetros de selección definidos, y como segundo objetivo es que proveen oportunidad y privacidad para el tránsito de los paquetes a través de la red, ya que para los adversarios les es muy complejo perpetrar su ataque, debido a que los paquetes de forma constante cambian de ruta Ozturk y otros , 2004 y Kamat y otros , 2005. En sus resultados ellos demostraron en su solución mejor desempeño que el algoritmo propuesto por Kamat y otros , 2005, ambos tomando decisiones según información que en cada paso encuentran en el vecindario. No considerando información anterior o la que podría proporcionar una visión global del escenario.

III.3.6 Síntesis de las estrategias analizadas

	Propuesta	Paquetes perdidos	Latencia
A	(Kamat y otros , 2005), inundación probabilística (70% probabilidad de retransmisión)	Valor relacionado con la probabilística inundación. Un 30% de los paquetes no se retransmiten en el escenario.	Para una separación de 60 saltos entre el nodo fuente y el nodo sumidero, además el valor de h_{walk} es 0, la Latencia promedio del mensaje (AML) es de 70. Al asignar a h_{walk} el valor de 20, la AML se incrementa hasta 91. Finalmente, con h_{walk} igual a 40 la AML es 110 (unidades: saltos).
B	(Xi y otros , 2006b), *Caminar Aleatorio* usando una heurística voraz	Los autores definen $t^{-(5\div 8)}$ como la probabilidad de que dos caminos aleatorios se crucen; considerando que la longitud un un camino generado por un movimiento Browniano es t. Bajo el anterior escenario la probabilidad de que se pierdan paquetes es menos del 5%.	La suma de t y la distancia entre el nodo de intersección y el nodo sumidero define la AML (unidad: segundos). Sus resultados muestran que el 80% de los paquetes llegan al nodo sumidero después de 12 segundos, En tanto que para Phantom es de un segundo.
C	(Li y Ren, 2010), Selección de un nodo intermedio	La longitud del paquete, la frecuencia de generación de paquetes y la longitud de la ruta afectan el valor del parámetro R_m. El peor caso para este parámetro es 0.35% y el mejor caso es 0.05%.	El rendimiento es igual al de Phantom, cuando los autores restringen la distancia entre el nodo intermedio y el fuente. El resto de las técnicas tienen peor rendimiento que Phantom.
D	(Li y Ren, 2010), Múltiple selección de nodos basado en un ángulo intermedio	El número de paquetes perdidos se incrementa (0.1%, a 0.4%) para ángulos de 0 hasta 200 grados.	Este algoritmo puede transmitir 128 bytes por 480 metros con la AML de 0.039 segundos en el mejor caso, en tanto que el peor caso es de 0.109 segundos.
E	(Spachos y otros , 2010) Encaminamiento oportunista	Los autores definen este parámetro en 0, porque consideran que teniendo activado el mecanismos de ACK entre los nodos vecinos es suficiente.	Cuando la ruta tiene una longitud 50 saltos, la AML es de 28 saltos, en tanto que para una ruta de longitud 35, la AML es de 20 saltos.

Tabla III.4: Síntesis de las propuestas revisadas en el estado del arte

Tabla III.4 muestra que la latencia en la propuesta **A** es muy similar a la propuesta de **C**. La propuesta **B**, tiene un comportamiento pobre en este aspecto frente a las anteriores, pero no usa técnicas de inundación, por lo que su consumo de energía es bajo. En **E**, los autores demuestran que su propuesta no incrementa la latencia y teniendo un mejor comportamiento que **A**, este algoritmo agrega una selección dinámica de los nodos, al considerar el estado del enlace para la selección del nodo siguiente.

Además la Tabla III.4 muestra un incremento en los paquetes perdidos asociado al mecanismo de privacidad, condición no presente en **E**. Finalmente se debe considerar el tamaño de los *buffers* para el almacenamiento temporal de los paquetes, en aplicaciones, donde los paquetes contienen datos y no solamente un indicador de presencia. Las propuestas (**A,B,C,D**) usan diferentes rutas para llegar al nodo destino, sin restricciones en su longitud. Esta condiciona produce oscilaciones importantes en el tiempo de arribo de los paquetes ACK (Acknowledgement packets).

III.4 Técnicas de Encaminamiento de Múltiples Caminos

Las técnicas de encaminamiento que ofrecen como resultado múltiples caminos, dan oportunidad de solución a una amplia gama de problemas en las tecnologías de red. Nuestro interés en ellas fue buscar formas para la solución al problema planteado a través de técnicas de reconocida efectividad, ya que las soluciones propuestas en la literatura para la solución del problema de interés, contienen retos importantes para su implementación y uso.

Abrahamsson y otros , 2002 usan esta clase de algoritmos para solucionar problemas relacionados con *ingeniería de tráfico en redes IP* evitando el uso de algoritmos de encaminamiento cuyo resultado es el camino más corto entre dos puntos, sin una consciencia de las demandas del tráfico o carga en los enlaces. La propuesta se basa en un protocolo de encaminamiento sensible a las demandas de tráfico, por lo que el problema de encaminamiento se convierte en un problema de optimización de flujos, ofreciendo como solución un algoritmo de encaminamiento basado en *optimización de flujos por medio de múltiples servicios*. Para proveer calidad en el servicio y consciencia en el consumo de energía, los autores Heikalabad y otros , 2011 proponen QEMPAR que es un protocolo para aplicaciones en redes de sensores. Este algoritmo después de ejecutar el proceso de descubrimiento de caminos

o rutas, divide los datos a transmitir en pequeños paquetes enviándolos por todas las rutas disponibles.

Lou y otros , 2009 proponen un algoritmo llamado SPREAD. Su objetivo es proveer seguridad en la transmisión de datos, dividiendo el mensaje en partes mediante la técnica de secreto compartido y transmitiendo los paquetes resultantes por múltiples caminos. Otro uso de estos algoritmos fue propuesto por Gera y otros , 2010. Los autores proponen una solución a problemas de seguridad relacionados con adversarios activos, que dañan los paquetes en transito; reducen el daño por medio de la utilización de múltiples caminos, evitando de esta forma el uso de rutas con nodos suplantados. Con otra filosofía en el diseño del algoritmo, pero con la intención de generar múltiples caminos.

Los autores Ducatelle y otros , 2005 proponen AntHoc, un protocolo de encaminamiento que provee un conjunto de rutas para transmitir datos, los cuales son actualizadas continuamente por un conjunto de hormigas que exploran la situación de las rutas y en caso de falla realizan las adecuaciones necesarias para reactivar las rutas dañadas. La oportunidad a la actualización constante en las rutas fue una de las características que nos llevo a estudiar los algoritmos basados en colonia de hormigas ya que proponen la posibilidad de cambios en las rutas durante el proceso de transmisión, además de múltiples caminos de forma natural.

III.5 Inteligencia Computacional

El termino Inteligencia Computacional se define a través de cinco paradigmas: Redes Neuronales Artificiales (RNA) (Hopfield, 1988), Computación Evolutiva (CE) , Inteligencia Colectiva (InC) (Talbi, 2009), Sistemas Inmunológicos Artificiales (SIA) (Leandro Nunes de Castro, 2002) y Sistemas Difusos (SD) (Cox y otros , 1998). Para nuestra investigación, el area de interés es un algoritmo clasificado dentro del paradigma de Inteligencia Colectiva (InC). En especifico abordaremos el tema del algoritmo de optimización basado en hormigas ACO (Ant Colony Optimization) propuesto por Dorigo y otros (1996).

Esta clase de algoritmos emulan la dinámica de sistemas biológicos, así como las leyes que los gobiernan; normalmente cuentan con un número reducido de reglas genéricas muy simples, que les permite ser grupos altamente organizados en la tarea que desempeñan, sin la necesidad de una entidad encargada de controlar el cúmulo de tareas. Las características enumeradas les permiten ser herramien-

tas útiles para resolver problemas relacionados con redes y sistemas de información como: ciudades inteligentes y servicios de e-salud basados en procesos distribuidos, entre otras aplicaciones.

III.6 Inteligencia colectiva con algoritmos ACO

La inteligencia colectiva es una rama de la inteligencia artificial contenida en el área de Inteligencia computacional, (Kulkarni y otros , 2011). En esta área se estudia el comportamiento colectivo y propiedades emergentes de complejidad, auto-organización, en los sistemas descentralizados que consideran una estructura social. Estos sistemas consisten de agentes simples que interactúan entre si y se organizan en pequeñas sociedades (swarms). Sin embargo cada agente tiene un espacio muy limitado para su actuación, no se considera una entidad central que controle el actuar de cada uno de estos individuos. El comportamiento que sigue todo el colectivo muestra tanto trazas de inteligencia, así como la habilidad para reaccionar a cambios en el medio ambiente y capacidad de tomar decisiones.

La principal inspiración de estos algoritmos proviene de la naturaleza, como los bancos de peces, parvadas de pájaros, rebaños de animales y las colonias de hormigas. Cada uno de estos grupos tiene grandes capacidades de organización descentralizada y reacciones, comportamientos colectivos que no pueden ser descritos por simple agregación del comportamiento de cada uno de los miembros del grupo sino por el estudio de las reglas y procedimientos que promueven comportamientos inteligentes a través de la colaboración y la competencia entre los individuos a dado un gran crecimiento a los campos de la inteligencia colectiva y los emergentes. Los humanos también comparten muchas de las propiedades observadas en animales.

En el marco de la optimización, la inteligencia colectiva comprende los algoritmos de optimización por colonia de hormigas, búsqueda por difusión estocástica y optimización por medio de un cumulo de partículas. Aun cuando la filosofía y la operación de estos algoritmos contiene importantes diferencias entre el computo evolutivo y los algoritmos de inteligencia colectiva, estos fueron clasificados como enfoques de computación evolutiva en los años noventa. Esta asociación fue realizada debido a sus similitudes, tales como el comportamiento estocásticos, el uso de poblaciones, los campos de aplicación, así como las áreas científicas que estaban interesadas en estos tres algoritmos (Parsopoulos, 2009).

En esta seccion se introduce el algoritmo *ACO*, sus bases y el modelo matemático que permitieron retomar dos de sus heurísticas para aplicarlas a nuestra propuesta .

Los autores definen al algoritmo *ACO* como un *Proceso Autocatalítico*, caracterizado por un *Ciclo de Retroalimentación Positiva*. El termino catálisis define las acciones que tienen la capacidad de incrementar la velocidad con la cual se ejecuta una reacción. Las hormigas generan este comportamiento al ir dejando trazas de feromona en su paso, ya que conforme la concentración de estas sustancias en una area de interés se incrementa, estas areas, en particular las rutas seguidas por las hormigas se vuelven más atractivas, produciendo que un mayor número de hormigas la seleccionen como su ruta en consecuencia, —*Retroalimentación Positiva*. Este fenómeno causa una rápida convergencia, si no existe un mecanismo que controle el proceso; para no llegar a la saturación máxima de la feromona en la ruta ocasionando la explosión en el sistema. Tal estado modifica las condiciones del problema inicial, alcanzando el equilibrio en un estado diferente. Para evitar esta clase de circunstancias, existe un mecanismo natural, —*la evaporación de la feromona*, el factor que introduce desequilibrio en el escenario.

El modelo matemático de ACO fue propuesto y explicado por Dorigo y otros (1996), usando como problema a resolver *El problema de optimización del agente viajero*. La función que provee la probabilidad de moverse de una población fuente i a una población destino en particular j, esto considerando a una hormiga k y se presenta en la Ecuación III.1, siendo esta una de las partes de mayor relevancia en el algoritmo:

$$P_{ij}^{k} = \begin{cases} \dfrac{[\tau_{ij}(t)]^{\alpha} \times [\eta_{ij}]^{\beta}}{\sum_{k \in allowed_k} [\tau_{ik}(t)]^{\alpha} \times [\eta_{ik}]^{\beta}} & Si\ j \in allowed_k \\ 0 & en\ otro\ caso \end{cases} \tag{III.1}$$

donde:

η_{ij} denota la conveniencia basada en la heurística de elegir el nodo j estando actualmente en el nodo i, $i, j \in \{1, \ldots, n\}$, donde N es el número de nodos.

τ_{ij} es el valor conocimiento adquirido para seleccionar un nodo j estando en el nodo i. se asocia con la cantidad de feromona acumulada.

α y β son los parámetros que controlan la importancia relativa de la heurística y el conocimiento adquirido respectivamente. $0 \geq \alpha, \beta < 1$

$allowed_k$, es la lista de los nodos permitidos para ser agregados en la ruta por la hormiga k (Lista blanca). $k = 1, \ldots, K$, donde K es el número total de hormigas.

El algoritmo ACO divide el proceso de solución del problema. El primer segmento incluye *la iteración del algoritmo*, el cual se ejecuta cuando todas las hormigas han seleccionado la ubicación siguiente al tiempo t, es decir, al tiempo $t+1$. El segundo segmento inicia después de n iteraciones del algoritmo, siendo N el tamaño del problema y $n = N$; en este instante cada hormiga ha finalizado un *tour*, y el algoritmo ha finalizado un *ciclo*; y de acuerdo a la Ecuación III.2, la intensidad de la feromona debe ser actualizada:

$$\tau_{ij}(t+n) = \rho \times \tau_{ij}(t) + \Delta\tau_{ij} \tag{III.2}$$

donde:

$\Delta\tau_{ij}$ es la cantidad de feromona que las hormigas depositan por unidad de medida en la ruta.

ρ Parámetro que indica el nivel de evaporación en el escenario, tomando valores en el rango de $0 \leq \rho < 1$.

El objetivo de del parámetro parámetro ρ es evitar la acumulación ilimitada de feromona en las rutas. De tal forma que $(1-\rho)$ representa la evaporación que se produce en el camina entre un tiempo t y $t+n$.

Una vez que una hormiga ha completado un *tour* deposita un valor predefinido de feromona a lo largo del camino. El valor de la feromona a depositar por nodo se define por medio de la Ecuación III.3.

$$\Delta\tau_{ij}^{k} = \begin{cases} \dfrac{Q}{Lk}, & \text{Si la k-ésima hormiga usa la arista(i-j) en el tiempo (t,t+n)} \\ 0, & \text{en otro caso.} \end{cases} \tag{III.3}$$

donde:

Q es una constante definida como el máximo nivel de feromona para los caminos y estrechamente relacionado con la configuración del problema.

Lk es la longitud del tour de la k-ésima hormiga.

El número de hormigas a considerar en la búsqueda de caminos al nodo sumidero, es un parámetro clave. Para su definición es necesario analizar cuidadosamente el escenario y las restricciones impuestas en él. Un número alto de hormigas genera caminos con altos niveles de feromona, que corresponden a soluciones subóptimas. Por otro lado, un número reducido de ellas, podrían no depositar suficiente feromona, como para poder motivar la cooperación entre ellas (Dorigo y otros , 1996).

La oportunidad que se detecto para diseñar un algoritmo que provee privacidad surgió al analizar la estrecha relación entre la cantidad de tráfico en un camino y el nivel de feromona. Así, caminos con alto nivel de feromona son sumamente atractivos para ser seleccionados por una mayor cantidad de hormigas. Por otro lado, ρ (parámetro de evaporación) decrece ese nivel en el escenario; con lo cual cumple con su objetivo de evitar la saturación de feromona en los caminos, haciéndolos menos atractivos para las hormigas.

Ambos parámetros denotan cantidad de tráfico en un camino; así, niveles altos de feromona indican caminos con gran cantidad de tráfico, que finalmente el algoritmo *ACO* los ofrece como una solución, ya que implican caminos cortos entre un nodo fuente y el nodo destino. Este análisis final permitió visualizar las modificaciones que al algoritmo *ACO* debe realizar para ser capaz de proveer privacidad y a la vez heredar alguna de sus fortalezas respecto a la efectividad en la generación de caminos, aprovechando el trabajo en equipo y a la simplicidad en los mecanismos de decisión.

III.7 Discusión.

En las aplicaciones criticas, en las cuales el contenido de los paquetes es importante, los mecanismos de ofuscación, como la generación de paquetes falsos, la técnica usada por Xi y otros (2006a) y encaminamiento por medio de inundación usado por Kamat y otros (2005), se consideran como las técnicas no aplicables en las soluciones antes mencionadas. Debido a que el tráfico falso comparte el mismo canal con el tráfico real, incrementando la posibilidad de colisiones, paquetes perdidos y paquetes tirados por las pilas en los dispositivos intermedios.

Los trabajos publicados en la literatura que proponen una solución al problema de *Obtención no autorizada de la ubicación de la fuente de datos en WSN* por ejemplo Villalba y otros (2010), se enfocan en proponer algoritmos con capacidad de ofrecer tantos caminos como paquetes que se

deban transmitir. Sin embargo, existe un algoritmo polinomial que es capaz de resolver el problema, encontrando todos los caminos que existen entre los pares de nodos en la red. Este algoritmo presenta un buen comportamiento considerando condiciones estáticas en los parámetros de interés de la red, descritas en la Tabla III.4. Sin embargo, esta es una condición no común en las redes inalámbricas múltisalto.

Los algoritmos que forman parte de los paradigmas de Inteligencia Computacional, tienen consciencia plena sobre la existencia de condiciones dinámicas en los enlaces de la red, más aun la adaptación se considera como una posibilidad a una mejor calidad de la solución que se ofrecen, estos algoritmos. Como ya anteriormente se menciono, mediante la sinergia del grupo ejecutando procesos caracterizados por reglas simples para lograr realizar tareas complejas. Características presentes en la arquitectura de los dispositivos embebidos, se proponen en el estándar IEEE 802.15.4 LAN/MAN Standards Committee (2006), por lo cual se tiene la hipótesis de que pueden ser una solución a la medidas en las redes de interés para esta investigación.

CAPÍTULO IV

NUKU ENCAMINAMIENTO Y PRIVACIDAD

NUKU, vocablo constituido por Nucú, nombre vulgar que se le da a la hormiga *atta cephalotes* en el sur de México y de la expresión *Keeps Un-tracking*. NUKU es nuestra propuesta para resolver el problema que en la literatura se refiere como la *Obtención no autorizada de la ubicación de la fuente de datos en WSN* (Rios y Lopez, 2011), (Ozturk y otros , 2004), (Kamat y otros , 2005). Este problema surge debido a los patrones de transmisión en las WSNs; ya que una vez que un evento es detectado por un nodo, este lo procesa y busca un nodo a través del cual poder hacerlo llegar al *nodo sumidero*.Es posible seguir las trazas que dejan los datos transmitidos en el canal de comunicación, detectando la fuente inmediata de la transmisión. Para un adversario que ejecuta un ataque pasivo, significa que se localiza la fuente de los datos si cuenta con suficientes transmisiones como para localizar el camino que estos siguen.

IV.1 Consideraciones en el diseño

El algoritmo *ACO* (Dorigo y otros , 1996) descrito en la Sección III.6, es una herramienta utilizada en redes para resolver problemas de encaminamiento, considerando condiciones dinámicas en los enlaces de la red y los rastros de feromona que las hormigas dejan a su paso, para después de una secuencia de exploraciones ofrecer como resultado una ruta óptima entre un nodo fuente y un nodo destino (ver Figura IV.1 como un ejemplo del proceso).

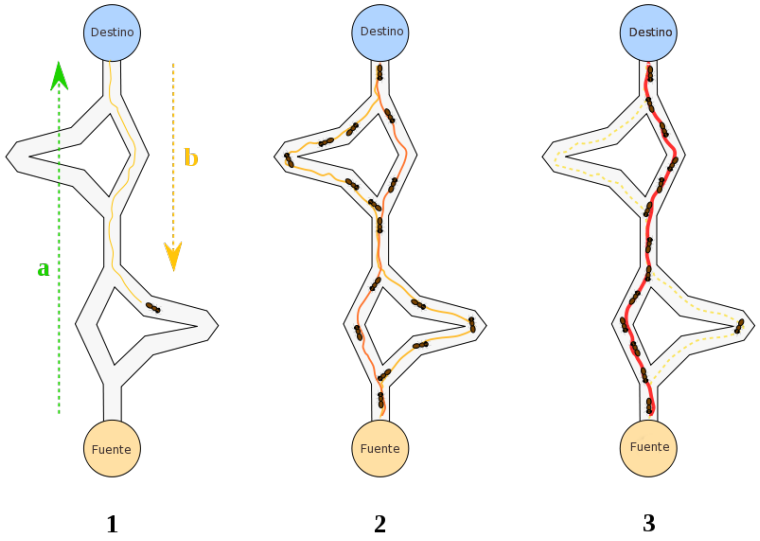

Figura IV.1: Formación del camino mas corto tras el proceso de optimización de las hormigás

Con el objetivo de emplear las capacidades del algoritmo para proponer una solución al problema descrito en el Capitulo I. En una exploración inicial propusimos la siguiente pregunta de investigación:

Es bien conocido que el algoritmo ACO provee soluciones eficientes para el encaminamiento de paquetes en una red Caro y otros (2004); Pero ¿Cúales son sus capacidades respecto a la protección de la privacidad y la seguridad?

Para las condiciones que esperábamos la respuesta fue: Que no es posible lograr ese objetivo de forma directa ya que desde la perspectiva de un adversario, existen condiciones muy atractivas para la consolidación exitosa de un ataque, siguiendo la estrategia del adversario descrita en el Capitulo III y el camino mas corto que ofrece el algoritmo como solución.

Una característica positiva para agregar privacidad en la ubicación, se observo durante el proceso de optimización que ejecuta el algoritmo ACO en busca de la ruta mas corta. Este proceso de optimización se ejecuta explorando un conjunto de rutas, sin embargo tiene una desventaja importante, la subutilización de rutas. Para explicar este problema utilizaremos el siguiente escenario: Se tiene un conjunto de rutas desde el nodo fuente al nodo destino. El conjunto de rutas son sometidas a un proceso de selección y reordenamiento de los elementos de las rutas (ver Figura IV.1 para observar la modificación en las rutas durante el proceso de optmización) hasta obtener como solución una ruta ajustada a las restricciones definidas en el algoritmo. En el proceso de optimización algunas rutas dejan se ser usadas o parte de ellas, para el resto formar parte de la solución que propone el algoritmo.

La estrategia común de solución al problema objeto de estudio en esta investigación, es el uso de múltiples rutas para evitar que las transmisiones usen nodos que sean objeto de un ataque pasivo. Por lo que dejar de usar rutas o partes de ellas y proponer solo una, como lo hace ACO, reduce la cantidad de lugares que el adversario debe atacar y por tanto, la probabilidad de éxito del adversario se incrementa de forma substancial.

Tomando en cuenta lo anterior, la siguiente tarea consistió en analizar procesos que afectan el comportamiento de las hormigas en su exploración. Un proceso de interés fue la evaporación, ACO en sus procesos la considera para generar desequilibrio en el escenario. El estudio de esta heurística permitió visualizar una relación entre un nivel bajo de feromona, ruta o parte de una ruta poco atractiva para la selección; con rutas con una probabilidad alta de contener un ataque pasivo en progreso.

Para asociar niveles bajos de feromona con zonas poco atractivas en el modelo matemático de ACO debido a un ataque en proceso, mientras era posible maximizar la cantidad de paquetes a transmitir se concluyo que era necesario saturar las rutas durante su activación *(niveles altos de feromona,)* para después borrarlas mediante un proceso de evaporación local, nodo a nodo, activado por las hormigas en su paso.

Con esta idea se planteo el uso del proceso de evaporación como un mecanismo para ecualizar la selección de los caminos existentes. Evitando patrones fijos en la transmisión de paquetes como lo es el camino mas corto entre dos puntos, resultado del algoritmo ACO.

IV.1.1 Requerimientos para el Diseño del algoritmo

1. Debe ser capaz de reducir el daño ocasionado por los ataques pasivos descritos en el Capitulo III.

2. Consciencia del nivel de privacidad requerido por transmisión.

3. Deben existir consideraciones respecto al parámetro de paquetes perdidos, de tal forma que sea tan bajo que no se pierda información de los datos transmitidos.

IV.1.2 Que no se pretende del Diseño del algoritmo

1. Las capas superiores en el nodo fuente *i* deben generar una etiqueta para relacionar los datos con los objetos a monitorizar en el mundo real. Esta relación debe ser protegida por las capas antes mencionadas, por lo que no es considerado en este trabajo.

2. El algoritmo debe evitar el uso de mecanismos de ofuscación como los descritos en el Capitulo III.

3. Ocultar a un dispositivo cuando este se conecta a la red.

4. Proveer de nuevos mecanismos de cifrado.

5. Modificar el estándar IEEE 802.15.4a 2006.

6. Definir políticas o comportamientos en la capa de aplicación.

7. Condicionar a caminos disjuntos.

Con la pregunta de investigación planteada en el Capitulo I y considerando las restricciones en los dispositivos del estándar IEEE 802.15.4a 2006, este trabajo de investigación propone una solución de capa de red al problema de privacidad descrito en el mismo capitulo.

IV.2 Descripción del Algoritmo Propuesto

El algoritmo propone dos estructuras: El Circuit-Path y la Zona-δ. Junto con estas estructuras existe el proceso de evaporación activado por las hormigas al transitar por los nodos que permite ecualizar la selección de las rutas por el nodo fuente. Este proceso se ilustra en la Figura IV.2.

El nivel de feromona denota el nivel de privacidad que se tiene al transitar por un camino en particular; alcanzar un umbral mínimo, no es seguro enviar más paquetes. Esta condición se evalúa mediante la Ecuación III.1 durante el proceso de selección del siguiente nodo que forma parte de la ruta a emplear.

Para la generación de rutas se proponen dos restricciones: El valor del parámetro Tiempo de Vida (TTL) y el numero máximo de hormigas a emplear en el procedimiento de búsqueda de rutas (K). El parámetro TTL define el número máximo de retransmisiones que una hormiga tiene capacidad realizar para alcanzar el nodo destino.

De tal modo que el numero de hormigas define que tan exhaustiva debe ser la búsqueda, tomando en cuenta las restricciones asociadas al ahorro de energía, control de la latencia en las trasmisiones y el control de colisiones en la red.

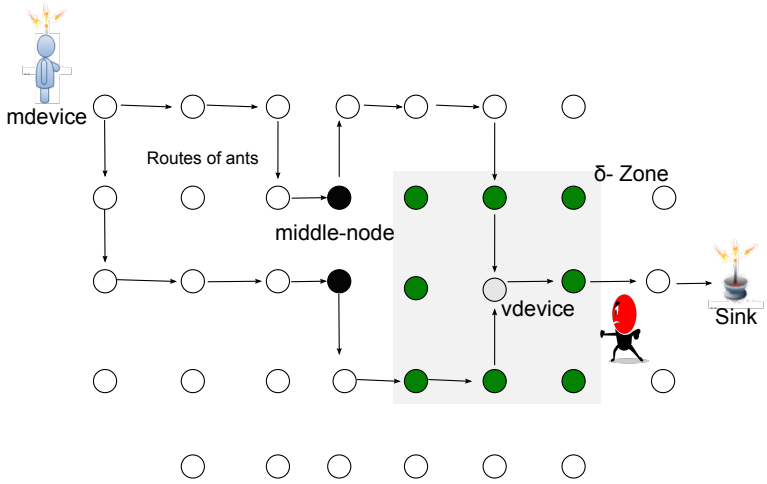

Figura IV.2: Ilustrando la técnica de encaminamiento de NUKU

El Algoritmo 1 muestra de forma general cada uno de los procesos de NUKU, para dar paso a la descripción detallada del funcionamiento de cada uno de ellos, las estructuras de privacidad que lo

Algorithm 1: algoritmo NUKU

```
Data: Hormigas, TTL
Result: Paquetes Protegidos
while condiciones de parada no alcanzadas do
    Búsqueda de rutas al vdevice;
    Activación de rutas exitosas;
    while no camino peligroso y transmitiendo do
        Transmisión de paquete;
        while no vdevice y no camino peligroso do
            Selección de nodo para retransmisión;
        end
    end
end
return solution;
```

componen y el modelo matemático.

IV.2.1 Modelo Matemático

NUKU al igual que ACO (Dorigo y otros , 1996), hace uso de la Ecuación III.1. En la definición de los elementos que componen al algoritmo NUKU tiene las siguientes propiedades en comparación con *ACO*:

- NUKU considera el tamaño del vecindario para los cálculos, en tanto que *ACO* refiere el tamaño total del problema.
- Para la lista definida por la variable $allowed_k$, que define sobre cuales nodos la hormiga actual puede hacer una evaluación para su selección, se convierte en una *lista negra (nodos no permitidos para la hormiga ant_k)*. En lugar de la lista blanca del algoritmo *ACO* (nodos permitidos).
- Los valores de los parámetros α y β están asociados al tipo de nodo en el escenario (ver Tabla II.1), en tanto que el algoritmo *ACO* considera una estrategia de valores fijos.

- El proceso de evaporación es local, nodo a nodo, esto significa que no se aplica una reducción de la feromona constante en su valor y a través del tiempo a intervalos también constantes sino que las hormigas a su paso por un nodo que pertenece a una ruta provocan este efecto.

Usando la ecuación IV.1 se realiza la modificación de la intensidad de los senderos, conforme los paquetes transitan a través de ellos:

$$\tau_i(t+1) = \tau_i(t) - \Delta\tau_i(t). \tag{IV.1}$$

donde:

$\Delta\tau_i(t)$ cantidad de feromona retirada del nodo i al tiempo t.

$\tau_i(t)$ es el nivel de intensidad de la feromona en el nodo i al tiempo t.

$\tau_i(t+1)$ la intensidad del camino en el nodo i al tiempo $t+1$.

El parámetro de evaporación ρ no se incluye en la Ecuación IV.1, a diferencia de la Ecuación III.2) propuesta por Dorigo y otros (1996). Este cambio se debe a que NUKU sólo intensifica las rutas en el momento de activación, por lo que la acumulación ilimitada de feromona en los senderos no se presenta.

Con el objetivo de controlar el tráfico de paquetes por las rutas, e introducir un proceso selectivo de los caminos mas seguros. NUKU usa $\Delta\tau_i$ como el parámetro de evaporación. Ello implica que no existe una constante de evaporación en el escenario. Así, cada vez que un paquete selecciona un nodo como su siguiente paso en el camino que sigue, la intensidad de la feromona decrece en $\Delta\tau_i(t)$ unidades. El objetivo es proveer información sobre la capacidad de protección en la ruta en tiempo real. Condición no presente en el algoritmo ACO tradicional, ya que la actualización de este parámetro la realiza el finalizar el recorrido.

En la generación de rutas, NUKU no considera exclusivamente caminos disjuntos, por lo tanto es necesario definir la evaporación que se aplicara en los nodos que forman parte de mas de una ruta. Para realizar ese calculo NUKU usa la Ecuación IV.2, que le permite contabilizar el numero total de saltos en los caminos que se cruzan en un nodo i.

$$LenghtCrossingRoutes = \sum_{c=1}^{C} [Lk]_c \tag{IV.2}$$

Donde:

C es el total de circuitos cruzando al tiempo t en el nodo i.

Lk es la longitud de la ruta hecha por la *k-ésima* hormiga.

$LenghtCrossingRoutes$ es la suma de la longitud de los circuitos que cruzan por el nodo i

$$\Delta\tau_i = \begin{cases} \left[\dfrac{Q}{Lk \times f(p)}\right](\phi_f(t_0)), & \text{Si la hormiga k pasa por i} \\ \left[\dfrac{Q}{LenghtCrossingRoutes \times f(p)}\right](\phi_f(t_0)), & \text{Si una hormiga } k \text{ pasa por } nci \\ 0, & \text{de otra manera.} \end{cases} \tag{IV.3}$$

donde:

Q es el valor máximo de feromona asignado considerando el tipo de nodo en el escenario.

nci es un nodo común a al menos dos rutas.

Lk es la longitud de la ruta ofrecida por la hormiga k.

$LenghtCrossingRoutes$ es la suma de la longitud de las rutas que comparten un nodo i.

$f(p)$ define el nivel de privacidad en la ubicación de la fuente a utilizar en una transmisión de datos, $0 < f(p) \leq 1$

$\phi_f(t_0)$ define una transmisión como en claro o privada al tiempo t_0, y toma valores $+1$ $y-1$.

La Ecuación IV.3 define la cantidad de feromona que se evaporara cuando un paquete deje el nodo actual, considerando el nivel de privacidad requerido por el usuario y el valor máximo de Q, el cual varia de acuerdo al tipo de nodo, como se muestra la Tabla IV.1, en la columna *umbral superior*. La función $f(p)$ provee un valor que relaciona la longitud de la ruta y un valor especifico en el nivel de privacidad en la ubicación de la fuente. Ademas considera dos parámetros, Lk y $LenghtCrossingRoutes$; el primero, la longitud de la ruta encontrada por la hormiga k y el valor del segundo parámetro se obtiene de la Ecuación IV.2. Finalmente la función $\phi_f(t)$ permite ejecutar las transmisiones considerando

la privacidad en la ubicación de la fuente o realizando transmisiones en claro, como se requiere cuando se da un evento de emergencia. La ultima consideración no se describe porque su comportamiento es el ejecutado por el algoritmo ACO.

IV.2.2 Estructuras de Privacidad de NUKU

Los modelos matemáticos antes mencionados, requieren de condiciones adicionales en el escenario para lograr su objetivo; NUKU propone para ello, dos estructuras, El *Circuit-Path* y la Zona-δ, cada una con características especificas respecto a el proceso de encaminamiento y los umbrales de feromona.

Circuit-Path

Un *Circuit-Path* es un subconjunto de nodos que pertenecen a G y forman un camino desde un nodo s a un nodo destino d $(v_s, v_{s+1}, v_{s+2} \dots v_d) \in V$ (también llamado simple-path). NUKU construye un *Circuit-Path* D_{sd} usando el procedimiento mostrado en la Figura IV.3, y el Algoritmo 2. Respecto a la carga útil de los paquetes se considera cifrada, para evitar que usuarios no autorizados accedan a ella. La dirección que siguen los paquetes está definida en el encabezado; sin embargo, información relacionada con la fuente se debe proteger por mecanismos en las capas superiores.

Zona-δ

Mecanismo basado en el algoritmo de Lumer y Faieta (1994) que utiliza una heurística para agrupar objetos, este comportamiento se ve en grupos de hormigas que se encargan de la limpieza de los hormigueros, comportamiento que es dirigido por una sustancia que motiva a las hormigas a hacer montículos en áreas particulares. Los montículos en las zonas limítrofes tiene un nivel bajo de la sustancia que motiva el comportamiento de agrupación de objetos y conforme se aproxima al centro su nivel se intensifica.

En esta investigación el objetivo de la inclusión de esta estructura en el escenario es incrementar la probabilidad de selección de las rutas exitosas entre el nodo *vdevice* y el fuente, además coadyuva en el aseguramiento de la privacidad en la ubicación del nodo fuente.

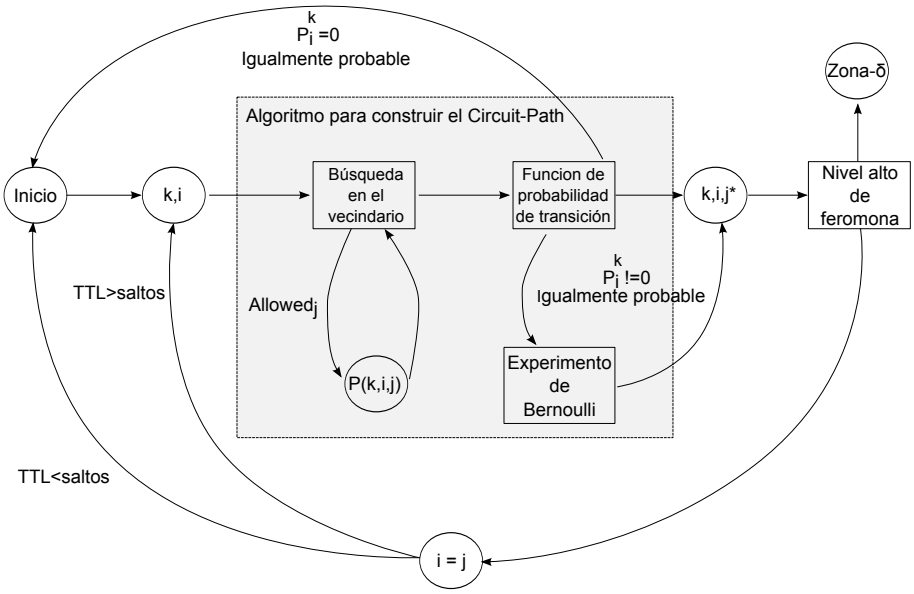

Figura IV.3: Construcción de un Circuit-Path

La Zona-δ coadyuva a mejorar la privacidad a través de una técnica de encaminamiento en la frontera de la Zona-δ y un mecanismo de confianza que controla el crecimiento de las estructuras de Zona-δ. Este último mecanismo hace que un dispositivo al final del un *Circuit-Path*, llamado *middle-node* adquiera feromona para convertirse en un nodo en prueba "node on proof." Este nodo divide la estrategia para alcanzar el nodo *vdevice* —en su primera fase usa los *Circuit-Path*, mientras que en la segunda fase emplea las condiciones de encaminamiento ofrecidas en la Zona-δ.

En la segunda fase los nodos que pertenecen al *Circuit-Path* evalúan el comportamiento del *middle-node*, por lo que una vez que la ruta ya no es segura para transitar por ella y el *middle-node* ha probado su efectividad para desempeñar sus funciones, su nivel de feromona es incrementado. Después de varias tareas cumplidas de forma efectiva, el nodo forma parte de la estructura de la Zona-δ. La probabilidad de encontrar una ruta se incrementa conforme mas nodos se agregan a esta zona como se puede ver en la Figure IV.4 en color gris, donde se muestra un escenario base con 8 nodos y altos niveles de feromona conforme se avanza hacia el centro. La Figura IV.5 muestra los diferentes niveles que se encuentran en los nodos.

Algorithm 2: Algoritmo para el construir el *Circuit-Path*

Data: k, α, β, i, r

Seleccionando j en el vecindario de tamaño r por la hormiga k

Result: $i, j*, k$ al tiempo t+1

for $(j = 1; j < r; j++)$ **do**

  if *j es permitido a moversedesde i* **then**

    $P_{ij}^{k} = Function\_Selec\_Node()$;

  else

    Unselected link;

  end

end

if P_i^k *es igualmente probable y diferente de 0* **then**

  if *Bernoulli Tray* **then**

    $P_{ij}^{k} = RandomLink()$;

  else

    if *circuit exist* **then**

      select circuit link;

    else

      if $RandomLink() \geq links$ **then**

        $return(-1)$; cerrar la ruta

      end

    end

  end

else

  return nodo con la mayor probabilidad en el vecindario

end

P_{ij}^{k} probabilidad de que una hormiga k se mueva de i a j.

P_i^k es el conjunto de probabilidades que tiene una hormiga k en su vecindario estando en el nodo i.

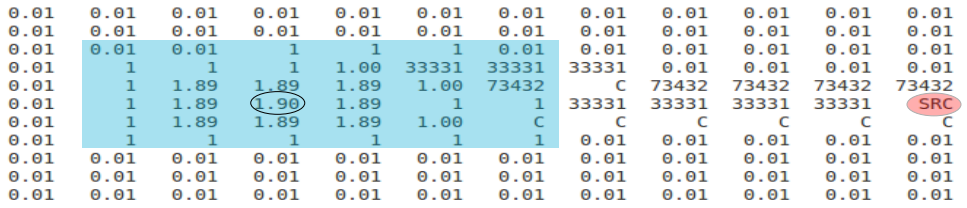

Figura IV.4: Una pantalla del programa de NUKU, mostrando la estructura de privacidad Zona-δ

Encaminamiento en la Zona-δ

Los paquetes antes de ingresar a la Zona-δ, ejecutan una serie de saltos alrededor de ésta (∂ *Zona* − *delta*). La intención de este mecanismo es mejorar el nivel de privacidad que en esta zona ofreció. Como una primer forma de probar su efectividad, a continuación se muestra un análisis matemático del proceso:

Primero proponemos a X, una variable indicador que nos permite contabilizar el número de paquetes que pasan a través del nodo j, que se encuentra a h saltos de un nodo intermedio: $X_{jh} = I\{node\,j\}$, un paquete pasa a través el nodo j, después de alejarse h saltos del *middle-node*; $h = \{1,2,\ldots h_z\}$, donde h_z se refiere al numero de saltos alrededor de la Zona-δ; $j = \{1,2,\ldots c\}$, donde c es el numero máximo de saltos ejecutados alrededor de las Zona-δ.

La ecuación IV.4 define un vector H, que almacena el número de paquetes recibidos por el nodo que se ubica a k saltos del nodo *middle-node*.

$$H_h = \sum_{j=1}^{c} X_{jh} \tag{IV.4}$$

La variable indicador X_{jh} es igual a 1 con una probabilidad $\frac{1}{h_z}$ y 0, con probabilidad $\left(1 - \frac{1}{h_z}\right)$:.

$$E\left[X_{jh}\right] = 1 \times \frac{1}{h_z} + 0 \times \left(1 - \frac{1}{h_z}\right)$$

En el siguiente procedimiento se analizan dos posibles escenarios, el primero con un *middle-node*, y el valor esperado se define mediante la Ecuación IV.5:

$$E\left[X_{jh}\right] = \frac{1}{h_z} \tag{IV.5}$$

El segundo caso considera dos middle-node en la Zona-δ. La selección del número de pasos a ejecutar tiene una distribución uniforme, ello significa que seleccionar cualquier valor en el rango de $\{1, \ldots, c\}$ es equiprobable. Así, cuando otro *middle-node* se localiza en una posición $y \neq j$, las variables X_{yv} y X_{jv} registran el comportamiento de dos eventos independientes, y el valor esperado de la probabilidad de ambos eventos tomen el valor de v es:

$$E\left[X_{jh}X_{yh}\right] = E\left[X_{jh}\right]E\left[X_{yh}\right]$$
$$E\left[X_{jh}\right]E\left[X_{yh}\right] = \left(\frac{1}{h_j}\right)\left(\frac{1}{h_y}\right)$$

Por lo tanto:

cuando existen mas de un *middle-node*, la probabilidad de encontrar la fuente de un flujo de datos esta afectada Ecuación IV.6:

$$E\left[X_{jh}\right]E\left[X_{yh}\right] = \frac{1}{h_j h_y} \tag{IV.6}$$

Considerando que el número de *middle-node* en (∂ *Zona* $-$ *delta*) se incrementa, el valor esperado de que dos paquetes accedan a la Zona-δ por el mismo nodo tiende a 0. Similares consideraciones existen cuando los nodos que conforman la frontera de la Zona-δ se incrementan. Si c tiene un valor máximo menor que el numero de nodos en ∂ *Zona* $-\ \delta$, la probabilidad de seleccionar un nodo que se localiza a $c+1$ saltos del *middle-node* es 0.

Función Objetivo

La función objetivo de NUKU maximiza el número de paquetes transportados a través de un conjunto de rutas, mientras un adversario definido en el *modelo de adversario*, intenta descubrir la ubicación de la fuente de transmisiones.

Establecer los parámetros, restricciones y la función objetivo como siguen:

TTL es numero máximo de saltos que una hormiga puede realizar en un proceso de búsqueda.

K el número de hormigas buscando la Zona-δ.

s es un conjunto de soluciones, donde $\{s = 1,2...S\}$ y S es el número total de soluciones.

TTL_s es la longitud total del conjunto de soluciones s.

a denota el número de s, toma valores desde 1 hasta ∞.

$TTLs_p$, tamaño del conjunto soluciones s modificada en longitud por la función $f(p)$.

$F_{a_v}, \{a = 1,2...\infty\}, \{v = 1,2...TTLs_p\}$ una variable indicadora, esta toma 1 cuando se ha realizado una transmisión exitosa, en otro caso el valor es 0, en la transmisión v del conjunto s.

$f_i(t)$ un flujo de datos a transmitir al tiempo t.

i la ubicación del nodo fuente.

j la ubicación del nodo donde esta el adversario.

b número de paquetes transmitidos.

Función Objetivo $f(F_{a_v})$.

$$MAXf(F_v) = \sum_{a=1}^{\infty} \sum_{v=1}^{TTLs_p} F_{a_v} \tag{IV.7}$$

s.t.

$$TTL \geq La\ longitud\ de\ la\ solucion\ ofrecida\ por\ las\ hormigas$$

$$0 < f(p) \leq 1$$

$$f_i(t) > b$$

$$nodo\ i \neq nodo\ j$$

IV.2.3 Parámetros de configuración α, β, Q y K

Para Yuan y otros , 2012, *el problema de la calibración del algoritmo*, "tuning algorithm", se presenta en algoritmos de optimización conteniendo parámetros que deben ser configurados de forma apropiada. Para configurar los parámetros α, β y Q en NUKU, se utilizaron experimentos empíricos, tal y como lo realizo Dorigo y otros , 1996. Terminar esta tarea llevo gran cantidad de tiempo, por lo que una consideración en esta investigación es agregar en el trabajo a futuro; la implementación de las técnicas propuestas por Huang y otros , 2006 y Ling y Luo, 2007 para *la calibración del algoritmo* considerando criterios de privacidad.

NUKU contiene diferentes técnicas para el encaminamiento de los paquetes, técnicas sujetas a las estructuras de privacidad y umbrales para los niveles de feromona (ver Figura IV.5). El uso de

Proceso	Tarea que ejecuta	α	β	Umbrales de feromona
0	Inicialización	1	5	0.01
1	Circuit-Path	1	1	(0.01,1]
2	Viaje en los limites de la Zona-δ	0	2	(0.01,1]
3	Zona-δ	1	0	(1.1,1.90]

Tabla IV.1: Parámetros de configuración de NUKU

valores fijos para los parámetros α y β generaran un escenario estático en las decisiones de NUKU, supeditado solamente a los cambios que se dieran en los enlaces de los nodos. En la Tabla IV.1 se describe los diferentes valores, así como las zonas donde se aplican.

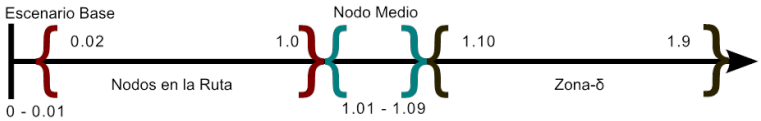

Figura IV.5: Umbrales de feromona en el escenario

Cuando el algoritmo se activa, el primer proceso que se ejecuta es la búsqueda de rutas, siendo la visibilidad el parámetro con mayor peso. Lo anterior se debe a que, nodos con altos niveles de feromona, pueden contener un ataque de tipo pasivo en progreso. El nivel mínimo de feromona (0.01), se considera para evitar valores de cero, ya que debido a la forma como planteamos nuestra solución, puede producir errores al aplicar la Ecuación III.1.

La segunda Linea, muestra los umbrales (0.01,1] de *Circuit-Path*. Esta se presenta cuando una transmisión esta en progreso. El nivel de feromona igual a 1 es el umbral superior en un *Circuit-Path*, una vez habilitado. Valor que se decrementa conforme los paquetes se transmiten a través de él hasta el punto donde no le es posible asegurar la privacidad en el *s*. La función de decisión considera de igual peso las condiciones de visibilidad en el escenario y el nivel de feromona; esto se debe a que un nodo con alto nivel de feromona que atiende un numero alto de transmisiones no es una opción adecuada cuando requerimos un balance entre privacidad y la oportunidad en la entrega de paquetes.

Los paquetes en la frontera de la Zona-δ, encuentran los parámetros mostrados en la tercera linea, al ejecutar su viaje alrededor de ésta, siendo β la condición de mayor peso en las decisiones, debido

a que la visibilidad ésta asociada con el tipo de nodo; lo que permite guiar el tránsito de los paquetes a través de un tipo especifico de nodos sin hacer otra consideración. Los umbrales en la Zona-δ son (0.01,1.1]. Sin embargo, esto no modifica la decisión, debido a que el valor de α es 0. Finalmente, una vez que los paquetes entran en la Zona-δ, estos siguen los niveles más altos de feromona, hasta alcanzar el nodo *vdevice*, su objetivo final.

IV.3 El modelo del sistema

La aplicación es un servicio de monitorización usando una WSN, de forma similar como lo describen los autores Ameen y otros , 2012 e involucrando los actores que se describen a continuación y en la Figura I.2.

1. Un *mdevice* m_i es un dispositivo que esta fijo o por un tiempo t en el área de cobertura de un *cdevice*.

2. El portador del dispositivo m_i sera monitorizado por el personal del servicio que se ofrece.

3. Existe un dispositivo sumidero $s1$.

4. El conjunto de nodos móviles M enviará datos hasta el nodo destino $s1$. El numero de paquetes esta definido por $p = f(m_i)$, donde $f(m_i)$ es una función que identifica el tipo de dato y m_i es el dispositivo fijo o móvil ejecutando una tarea de adquisición de datos.

5. Existe un conjunto de estrategias A definidas en el *Modelo del Adversario* (explicado en la sección *El modelo del adversario*); cuyo objetivo es conocer la ubicación de la fuente de datos m_i.

El *modelo de red* propuesto es una red publica de dispositivos inalámbricos múltisalto que forman una WSN para la transición de datos. Esta red provee la infraestructura de telecomunicaciones, para la transmisión de paquetes conteniendo parámetros fisiológicos. La WSN tiene posibilidades de habilitar conexiones entre cada uno de los dispositivos que la componen; a esta red nosotros la denominamos como el grafo G; G=$\{V,E\}$, donde V es el conjunto de nodos, y el conjunto de enlaces entre los nodos es E. En cada nodo, solo cuenta con una interfaz física, usando el mismo canal inalámbrico de

comunicaciones; así, un nodo V_i en su área de cobertura puede tener un enlace y no mas en un tiempo t_n con otro nodo V_j. Sin embargo, es posible que el nodo V_i hubiera compartido información con otros nodos $V_{1\ldots J}$ en su cobertura en diferentes instantes $t_1 \ldots t_{n-1}$, como lo muestra la Figura IV.6, donde $\mid J \mid$ dice el tamaño del vecindario y r el número de interacciones.

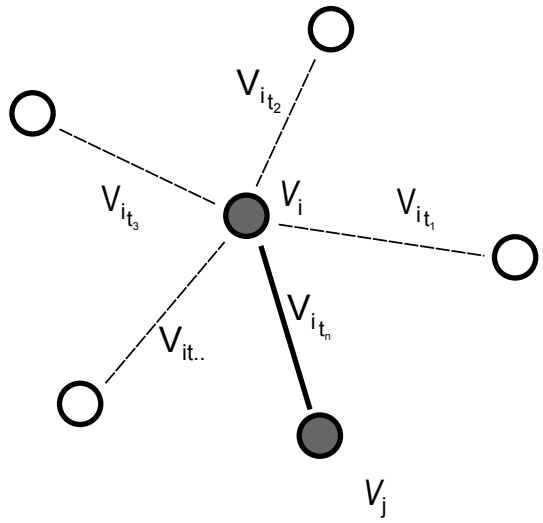

Figura IV.6: Una interfaz inalámbrica, provee restricciones para la interacciones entre diversos dispositivos en el vecindario

El *Modelo de Datos* hace las siguientes consideraciones: Un usuario con un dispositivo portátil m_i, transmite paquetes a intervalos prefijados. Asumimos la existencia de mecanismos de seguridad encargados de cifrar el contenido de los paquetes. Una vez cifrada la información no es posible obtener información adicional respecto a la relación *datos-portador-dispositivo*. Se genera un flujo de paquetes a intervalos fijos; si el portador el dispositivo desea hacer una transmisión en claro *(no cifrada)* se genera un flujo adicional que no se ajusta a los intervalos referidos en los flujos de datos cifrados. La dirección del tráfico se controla mediante una etiqueta en el encabezado de cada paquete. Cada dispositivo *cdevice* cuenta con un identificador único protegido mediante una *cadena hash* y un mecanismo de llave publica, ambos mecanismos ofrecidos por la capa de aplicación.

El Modelo de Adversario A (definiciones del termino adversario y sus características referirse a la Sección III.1).Siguiendo los *principios de Kerckhoff* (Trappe y Washington, 2002), consideramos que los adversarios tienen toda la información respecto a los protocolos de red y los mecanismos

de privacidad. Esto es, la privacidad no se sustenta en el desconocimiento de los procesos por el adversario, si no que la proveé el comportamiento de los mecanismos propuestos.

Adicional a las estrategias propuestas en la literatura para el problema de privacidad en la ubicación del nodo fuente (ver la descripción de los adversarios en la Sección III.1.2), se propone un tercer tipo de adversario denominado *Adversario Inteligente,* a_e. El objetivo de este adversario es probar las capacidades de NUKU ante condiciones adversas especificas para la estrategia de defensa del algoritmo. Este adversario inicia su ataque en el nodo *vdevice* y al igual que el resto de los adversario reacciona ante la presencia de un evento en su esfera de cobertura.

a_e no tiene restricciones respecto a la dirección del paquete, al escuchar un evento se mueve a la fuente inmediata de él. Este adversario también considera un buffer que le permite recordar cuales nodos ya ha visitado y solo vuelve a un nodo ya visitado, si ha transcurrido un tiempo t y no recibió ningún evento en su ubicación actual. La actitud que presenta este adversario lo hace mas agresivo para NUKU, debido a que no pierde tiempo esperando a que el destino de un paquete sea el nodo en el que se ubica actualmente. La estrategia del adversario se describe en el Algoritmo 3.

Los adversarios conocen la ubicación del *vdevice*, por la concurrencia del tráfico hacia ese lugar. Respecto al hardware, los adversarios no tienen restricciones de energía, además cuentan con suficiente capacidad de computo y almacenamiento para perpetrar un ataque de tipo pasivo. Una vez que el adversario detecta un evento, son capaces de determinar el emisor inmediato analizando la fuerza de recepción y la dirección de la señal recibida. Los adversarios tiene la capacidad de moverse de un punto a a un punto b de tal forma que el tiempo en ejecutar tal acción es despreciable.

IV.4 Conclusión.

En la figura IV.4, se muestra una visión simplificada del algoritmo, con la intención de mostrar los elementos que lo componen, en tanto mantiene las características de los algoritmos bioinspirados: número reducido de reglas y simplicidad en sus relaciones.

Las diferencias principales entre el algoritmo de NUKU y el algoritmo ACO propuesto por Dorigo y otros (1996) son:

1. El proceso de optimización de rutas empleado por ACO para encontrar el camino mas corto,

Algorithm 3: Adversario: Adversario Inteligente

```
Data: f(m_i)
Result: 1|0
location = sink
prev_location = sink;
next_location = sink;
while (location! = source) do
    reason = TimedListen(next_location, interval);
    if (reason == MSG_ARRIVAL) then
        msg = HeardMessage();
        if (IsNewMessage(msg)) then
            next_location = CalculateImmediateSender(msg);
            if Isnovisited(next_location) then
                MoveTo(next_location);
                location = next_location;
            end
        end
    else
        next_location = prevlocation;
        prevlocation = LookUpPrevLocation(prevlocation);
        MoveTo(next_location);
    end
end
return 1
```

permite a NUKU hacer la transmisión de paquetes con consciencia de la privacidad.

2. El proceso de evaporación local controla el nivel de privacidad que existe en los caminos.

3. Una estructura jerárquica en la seguridad mejora el rendimiento de NUKU.

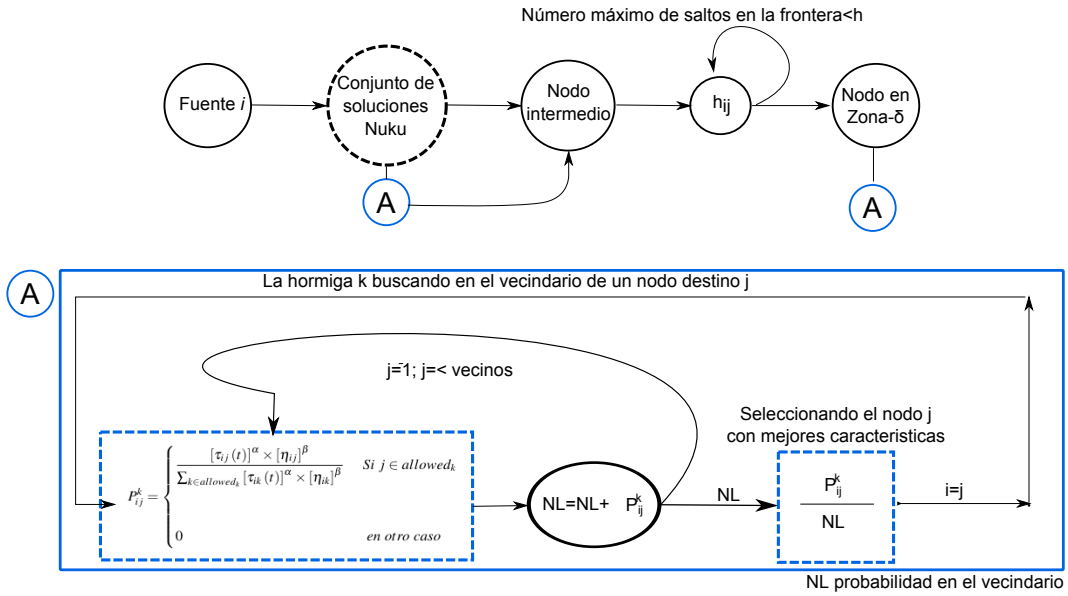

Figura IV.7: Diagrama general del Algoritmo NUKU

4. Se propone una estructura para incrementar la visibilidad de los nodos sumidero. En los mecanismos que componen esta estructura existe uno que realiza la valoración del comportamiento de los nodos propuesto para ser parte de la Zona-δ.

CAPÍTULO V

RESULTADOS

En esta sección se caracteriza la solución, se explican las métricas y se describen la forma como se obtuvieron dichos resultados.

En la literatura, los criterios para medir el comportamiento de las heurísticas, tienden a estar agrupados en tres grandes áreas: la calidad de la solución, el costo computacional y la robustez de la solución Barr y otros (1995). En este trabajo se consideran los tres aspectos, ya que en dispositivos embebidos requieren un balance, entre el tiempo de vida de la red y las condiciones del servicio.

V.1 Métricas de Evaluación

Para medir el comportamiento de NUKU se consideraron las siguientes métricas:

1. **Tamaño del conjunto solución** *Ss*. Esta métrica se mide el número de rutas, *s*, permite saber el número de opciones que se tiene para seleccionar diferentes rutas. Para el algoritmo propuesto el tamaño de este conjunto esta directamente relacionado con el numero de hormigas que con éxito alcanzaron el nodo *vdevice*

2. **Relación de mensajes entregados y los transmitidos** R_m. Es la relación entre los paquetes entregados y el total de paquetes transmitidos en el escenario.

3. **Número de transmisiones por mensaje entregado** T_m. Es el cómputo de los saltos requeridos para alcanzar el nodo destino. Este parámetro nos permite analizar la cantidad de energía consumida por el proceso de transmisión, el numero de colisiones y el balance entre transmisiones y procesamiento.

4. **Latencia promedio en los mensajes** T_l este parámetro ofrece información respecto al numero de saltos promedio requeridos por un paquete para alcanzar el nodo destino, en cada uno de los escenarios configurados. Para NUKU, este parámetro es también ofrecido por T_m, sin embargo, en este trabajo se incluye por comparabilidad con la propuesta de Kamat y otros (2005).

5. **Periodo de Seguridad** P_t. Este parámetro indica el numero de paquetes que es posible transmitir antes de que el adversario definido en *el Modelo del Adversario, definido en el Capitulo III.1* logre su objetivo.

6. **Probabilidad de Captura, C**. Este valor es la relación entre el peor resultado en el parámetro P_t, y el mismo resultado en cada uno de los escenario configurados.

V.1.1 Escenario para la simulación

Para generar los resultados del algoritmo NUKU que se proponen en esta sección, se implementaron en lenguaje C *el modelo del adversario*, el algoritmo de encaminamiento NUKU y el escenario; las im-

plementaciones anteriores se ejecutaron una computadora PII, con 2 Gb en RAM y sistema operativo Ubuntu 10.10.

El escenario se construyo en una matriz de 100×100 nodos, el parámetro TTL se relaciono con la distancia entre el nodo fuente y el nodo destino mas una distancia de holgura, la distancia de holgura se considero con la intención de permitir una mayor área de exploración a las hormigas y por lo tanto diversidad en los caminos que producen. El tamaño máximo del vecindario para los nodos del escenario se fijo en cuatro (4), los nodos formaban una retícula y se considera la cobertura de los nodos un salto. El escenario se configuró con las tres (3) estrategias del modelo de adversario. Además, respecto a la ubicación de los *vdevices* se consideraron seis (6) distancias diferentes: 2, 4, 8, 16, 34 y 60 saltos al nodo fuente; finalmente respecto al número de *vdevices* en el escenario se tenían dos posibilidades uno o dos *vdevices*.

Los parámetros considerados para la distancia entre el nodo fuente y el destino en el escenario se justifican en la necesidad de comparabilidad con las soluciones al problema de privacidad en la ubicación de la fuente citadas en el Capitulo III.

El escenario con dos *vdevices* (ver Figura V.1) se implemento para demostrar la hipótesis siguiente: *Existe ventaja al utilizar múltiples* vdevice*, para la privacidad considerando, ya que el nodo fuente se asocia a más de un dispositivo destino, permitiendo mayor diversidad en las rutas.*

Los datos propuestos del algoritmo NUKU se derivan de 100 corridas independientes para las diferentes posibilidades de configuración y considerando las restricciones de la *la función objetivo* descrita en la Sección IV.2.2.

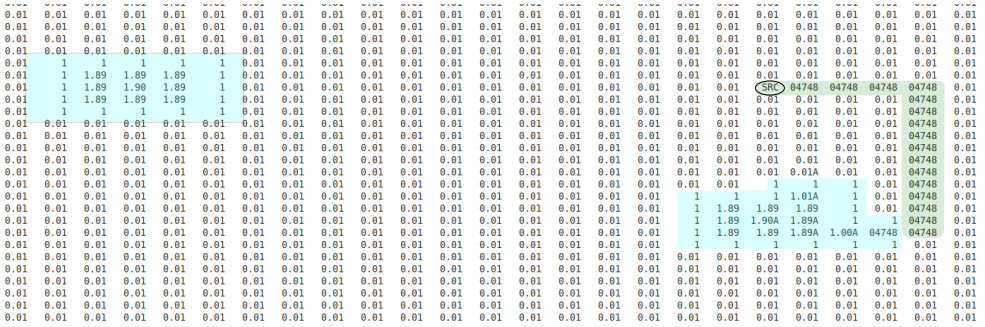

Figura V.1: Escenario con 2 Zonas-δ

V.1.2 Resultados

La Figura V.2 muestra el diagrama de flujo empleado para el procesamiento de la información generada por las simulaciones del algoritmo NUKU. La entrada principal al proceso es el Algoritmo con alguna de las configuraciones. Una vez ejecutado el algoritmo 100 veces, los datos obtenidos son usados como entrada a 7 subprocesos. El procesamiento de los datos se concluye con la generación de una archivo que integra la mayor parte de los resultados requeridos.

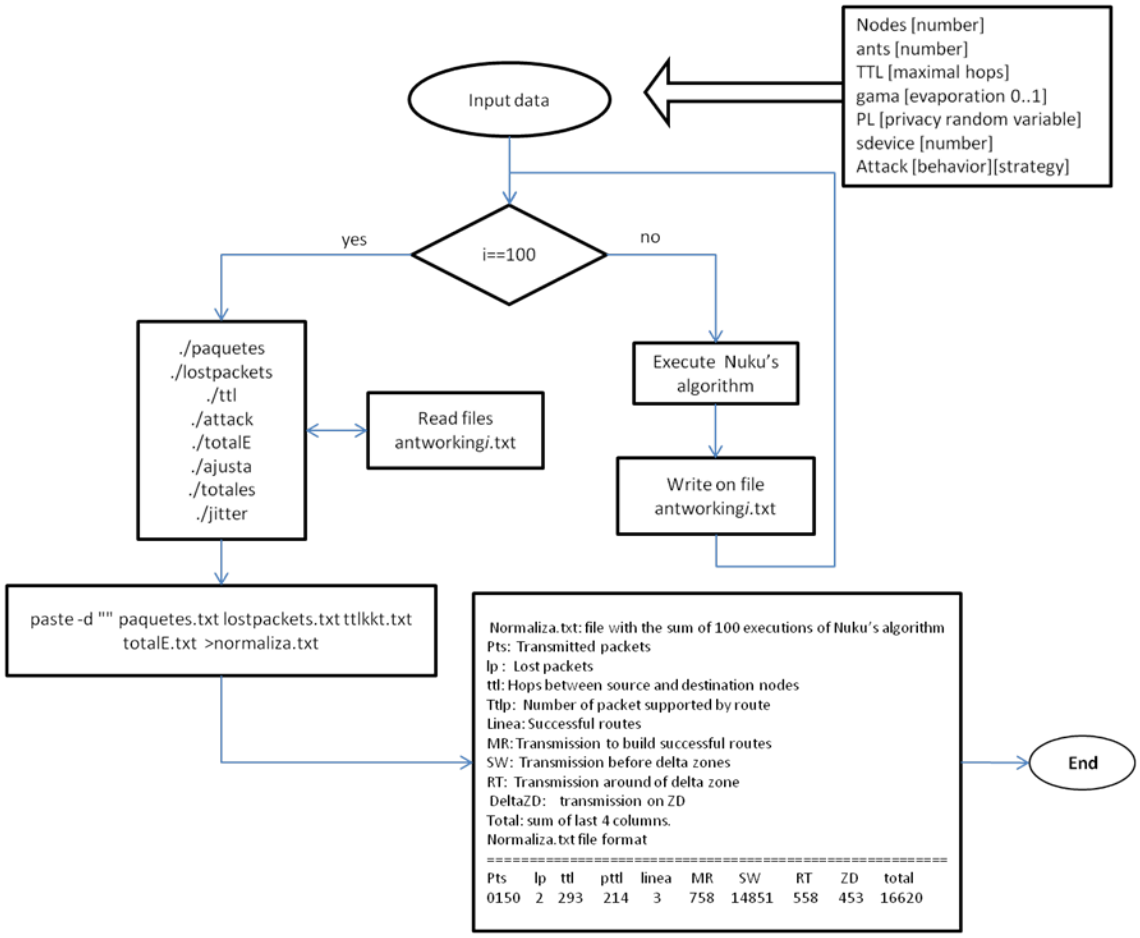

Figura V.2: Diagrama de flujo para el procesamiento de los datos

V.1.3 Consumo de energía por los paquetes protegidos

Para este análisis se considero un algoritmo que ofrece el camino más corto y el algoritmo de Phantom comparándolos con los datos de NUKU. Para este análisis solo se consideró las transmisiones requeridas para hacer llegar los paquetes a un nodo destino.

El consumo de energía en el algoritmo que ofrece el *camino más corto* involucra dos etapas: (a) la búsqueda del camino entre dos puntos, (b) la transmisión de los paquetes. Por otro lado el algoritmo Phantom tiene dos fases diferentes respecto al consumo de energía: (a) caminar aleatorio, relacionado con el valor del parámetro h_{walk} e (b) inundación proceso sumamente demandante de energía.

En NUKU el consumo de energía contempla tres aspectos: (a) Proceso de búsqueda y activación de rutas, (b) La transmisión de paquetes (c) Señalización, paquetes con los cuales el algoritmo informa del nivel de feromona en el nodo i a los nodos en el vecindario.

En el camino mas corto el consumo de energía esta dado por el numero de paquetes transmitidos multiplicado por el costo de transmitir un paquete y este resultado se multiplica por el total de retransmisiones. Con la intensión de que los resultados sean aplicables a diversas plataformas de implementación, los resultado ofrecidos no incluyen el costo en energía por transmitir a un salto.

En el caso de Phantom con una probabilidad de retransmisión del 70 % el consumo de energía solo se da en la transmisión del paquete, ya que no existe un proceso de activación o búsqueda de rutas previo a las transmisiones de paquetes de datos. Por lo tanto el costo de la transmisión se calcula como sigue: en la primera etapa se considera el número de paquetes multiplicado por el parámetro h_{walk}; la segunda etapa se considera el tamaño de la red, N y la probabilidad de retransmisión, P_f.

En NUKU para hacer el mismo análisis se incluyó en las tablas las transmisiones necesarias que el algoritmo proteja un flujo de paquetes. El escenario se configuro considerando una distancia de 34 saltos entre el nodo fuente y el nodo destino, ademas de un *vdevice*. Los datos son resultado de 100 corridas del algoritmo NUKU. La Gráfica V.3, muestra una síntesis de las datos que se incluyen en las tablas siguientes.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	1173.48	1185.61	156.00	6254.00
SW	18711.30	19600.58	1584.00	102795.00
RT	2583.92	2737.30	90.00	14713.00
ZD	1350.88	1488.85	123.00	7922.00

Tabla V.1: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (un *vdevice* y un adversario pasivo).

En los datos que se muestran en la Tabla V.1 para proteger un promedio 412.74 paquetes las hormigas exploradoras realizaron 18711 retransmisiones al transportar paquetes a un nodo sumidero antes de que un *adversario pasivo* en el escenario detuviera el algoritmo, el número de retransmisiones necesarias para llevar los paquetes a su destino hace el transporte de los paquetes en este segmento uno de los procesos más caros. Estos paquetes se transmitieron a través de un promedio de 11.74 rutas. El costo asociado a proveer de privacidad alrededor de la Zona-δ fue de 2583 retransmisiones, costo que se decrementa a 1350 retransmisiones al encaminar los paquetes en el interior de la Zona-δ.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	749.06	806.49	150.00	4360.00
SW	11851.41	13283.06	1372.00	69716.00
RT	1664.07	1887.36	43.00	9098.00
ZD	864.24	1042.22	104.00	5401.00

Tabla V.2: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (un *vdevice* y un adversario cauteloso).

En la Tabla V.2 para generar los datos se configuró un *vdevice* y la estrategia de un adversario cauteloso. En este escenario NUKU logro proteger 262.85 paquetes usando un promedio de 7.17 rutas. La capacidad de proteger paquetes se redujo en 149 al modificar la estrategia del adversario. El número de transmisiones para generar las rutas fue de 749 su valor promedio, respecto a las otras etapas mostradas en la Tabla V.2 las retransmisiones mantienen el mismo comportamiento observado en los valores de la Tabla V.1.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	685.10	737.23	168.00	5076.00
SW	10729.13	12147.37	1554.00	83985.00
RT	1468.57	1628.04	62.00	10981.00
ZD	745.95	884.48	102.00	5763.00

Tabla V.3: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (un *vdevice* y un adversario inteligente).

Los datos en la Tabla V.3 son resultado de configurar el escenario con un *vdevice* y un *adversario del tipo inteligente* ejecutando su estrategia de ataque. Bajo estas condiciones el valor medio de paquetes protegidos se reduce en 24 paquetes, diferencia de paquetes protegidos mínima aun cuando este último adversario debe considerar mayores recursos para un ataque exitoso. Respecto al número de rutas promedio este valor también se redujo, esto se debe a que el algoritmo detuvo su funcionamiento en un menor tiempo. Las retransmisiones en el segmento SW fueron 10729.13; 1122.28 menos que en la anterior estrategia, costo que podemos relacionar con la diferencia de paquetes protegidos en el escenario descrito por los datos de la Tabla V.2 y el descrito por la Tabla V.3.

Manteniendo la distancia de 34 saltos entre el *vdevice* y el dispositivo fuente se agrego al escenario un *vdevice*. Se propone la Gráfica V.4 con el mismo objetivo al expresado para la Gráfica V.3, permitir una visión global de los datos en el escenario configurado incluyendo las diferentes estrategias de ataque.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	929.94	1190.76	.00	8500.00
SW	13711.85	18053.09	1.00	125040.0
RT	2146.80	2791.39	58.00	18004.00
ZD	2053.54	9391.62	94.00	93924.00

Tabla V.4: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (dos *vdevice* y un Adversario Paciente).

Comparando los resultados de la Tabla V.4 con la V.1 existe una diferencia de más de 250 paquetes

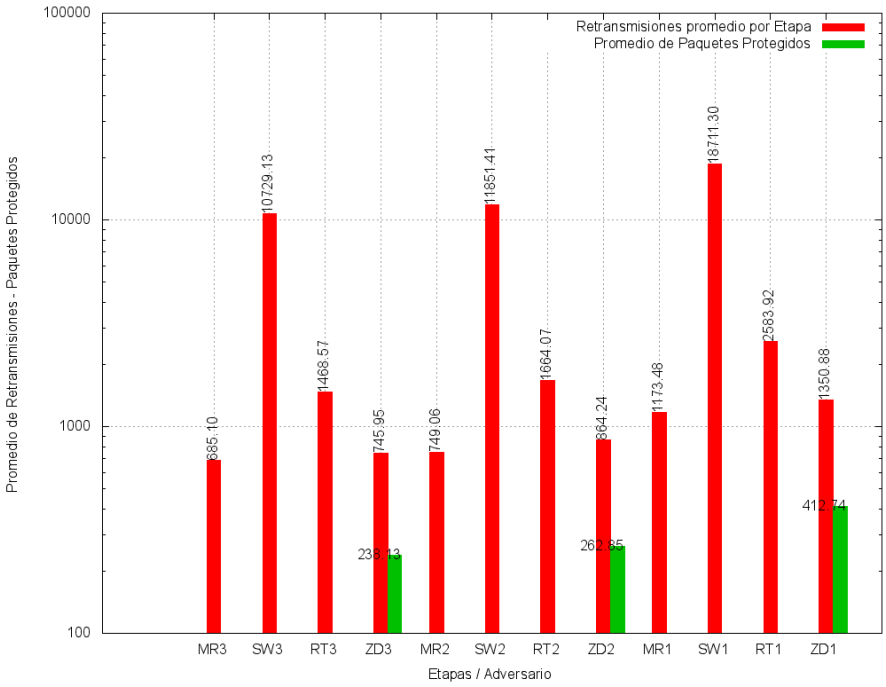

Figura V.3: Modelo del Adversario, (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ un *vdevice*.

protegidos por el escenario con dos *vdevice*. Con el objetivo de ofrecer una perspectiva practica de la cantidad de paquetes protegidos, se emplearan los parámetros de la Tabla V.5 para calcular el tráfico que un dispositivo de una WSN genera con una carga útil por paquete de 100 bytes; concluyendo que es posible proteger hasta $2s$ de datos adquiridos de una señal ECG.

Tasa de Transferencia de datos crudos	250 kbps
Biomedico	ECG (3 conductores)
Velocidad de Muestreo	250 Hz
Resolución de la Muestra	16 bits
ECG tasa de datos	12 kbps
Tamaño del paquete	100 bytes

Tabla V.5: Especificaciones en un nodo genérico, con un dispositivo de muestreo de una señal de un ECG.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	812.28	849.01	152.00	4830.00
SW	10514.81	11383.01	1478.00	64185.00
RT	1589.09	1625.27	44.00	9670.00
ZD	830.65	961.11	95.00	5851.00

Tabla V.6: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (dos *vdevice* y un adversario cauteloso).

En la Tabla V.6, el comportamiento en las retransmisiones es muy similar a los resultados mostrados en la Tabla V.2. Lo cual podría permitirnos concluir que ambos escenarios proponen condiciones similares a la privacidad, 257.04 de paquetes protegidos en un escenario con dos *vdevice* en tanto que con un *vdevice* el algoritmo protegió 262.85, cantidad inferior al comportamiento del anterior escenario. Una conclusión positiva es que aun es posible proteger al menos 1s de datos crudos obtenidos de un ECG.

Variable	Media	Desviación estándar	Valor mínimo	Máximo
MR	775.54	683.49	136.00	3312.00
SW	9963.61	9145.96	1320.00	43707.00
RT	1460.70	1397.46	46.00	6133.00
ZD	763.93	736.14	88.00	3693.00

Tabla V.7: Retransmisiones en: (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ (dos *vdevice* y un adversario inteligente).

Esta última tabla (Tabla V.7) muestra también un incremento en los paquetes protegidos, 238.13 con un *vdevice* contra 242.70 con dos *vdevice*, aun cuando la cantidad no es en definitiva lo esperado. Estos resultados, están asociados al tamaño promedio del conjunto solución, que como se vera en los siguientes párrafos tiene una relación directa en el número de paquetes protegidos.

Tamaño del conjunto de soluciones En la literatura, el nivel de privacidad ofrecido esta sujeto a dos condiciones: (a) La longitud del camino y (b) La variación al seleccionar la ruta que seguirán los

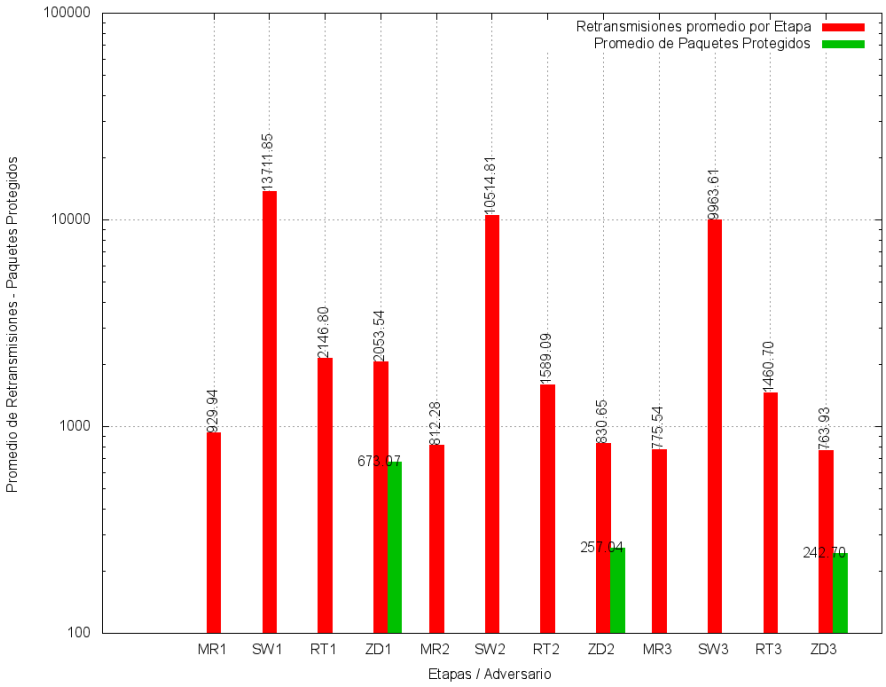

Figura V.4: Modelo del Adversario, (MR) Generando Rutas, (RT) Transmisiones alrededor de la Zona-δ, (ZD) Transmisiones en la Zona-δ dos *vdevice*.

paquetes. Para el *caso a* incluyendo los adversarios definidos en el Capitulo IV, se pudo concluir que efectivamente, rutas más largas favorecen la privacidad ofrecida. Sin embargo, la segunda condición permite alcanzar el mismo objetivo y más aun nos permite controlar la latencia en las transmisiones. Siendo lo anterior, una de las consideraciones en el diseño de NUKU fue importante para nosotros incluir; la segunda condición para lograr el balance Privacidad-Latencia. Como resultado se ve en la Gráfica V.5 cómo se asocia el nivel de privacidad ofrecido y el tamaño del conjunto de soluciones. Reforzando lo ya descrito en el Capitulo III, por Shaikh y otros (2010) se concluyo que una diversidad en la selección de los caminos permite incrementar el nivel de privacidad sin incrementar la latencia.

Relación entre mensajes entregados y los transmitidos Los autores Kamat y otros (2005) mostraron que las técnicas de encaminamiento por inundación y aquellas que construían el *camino más corto*, en el parámetro *relación de mensajes entregados y transmitidos* R_m era del 100 % de los paquetes transmitidos. Para la inundación probabilístico, el cual (Kamat y otros , 2005) consideraron en

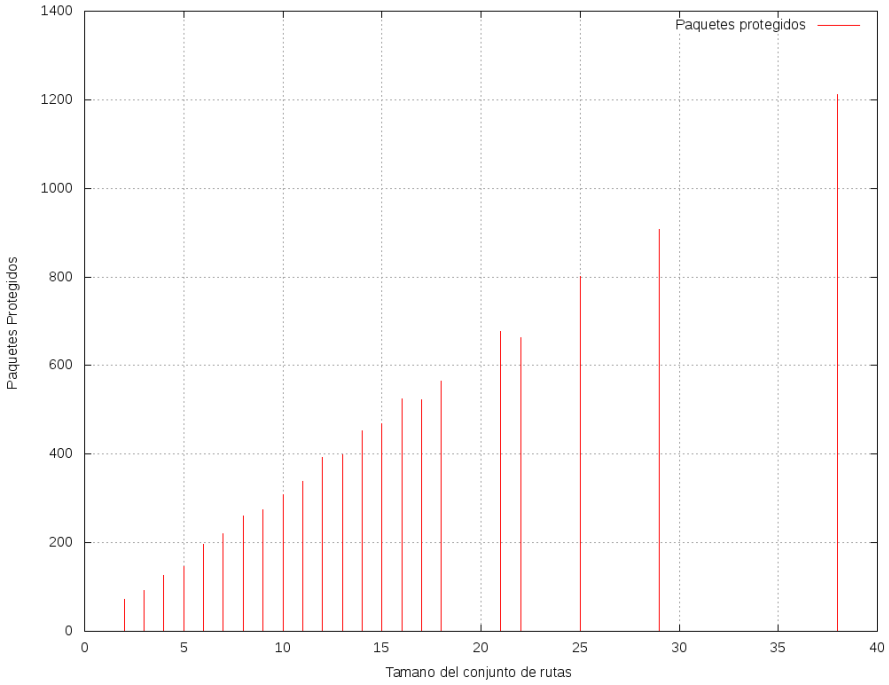

Figura V.5: Relación entre la diversidad de las rutas y los paquetes protegidos

su solución se alcanza una efectividad del 70 % en los paquetes entregados. La Figura V.6 muestra un comportamiento similar para el peor caso en el mismo parámetro en NUKU, considerando 8, 16, 34 y 60 saltos, entre el nodo fuente y el destino y diferenciando entre uno y dos *vdevice*. El peor caso mostraba un porcentaje de 90.5 % cuando la fuente estaba a 8 saltos de la Zona-δ.El mejor caso era del 99.3 % cuando la fuente se ubicaba a 34 saltos de la Zona-δ. Finalmente, como podemos ver, este parámetro se incrementa conforme, el número de saltos crece. Este parámetro decrece hasta alcanzar 98.2 %. El escenario que considera dos *vdevices* mostró resultados muy similares, teniendo mejores resultados cuando la distancia entre la fuente y el nodo destino era de 8 y 60 saltos.

Latencia promedio en los mensajes Respecto a T_l, Phantom obtuvo valores más altos en *latencia promedio en los mensajes* que el camino más corto, esta situación se presenta porque Phanton utiliza el caminar aleatorio e inundación como protocolos de encaminamiento. En el *caso base de phantom* (0 saltos en su primera fase, no se considera caminar aleatorio), el valor de la latencia es muy cercano

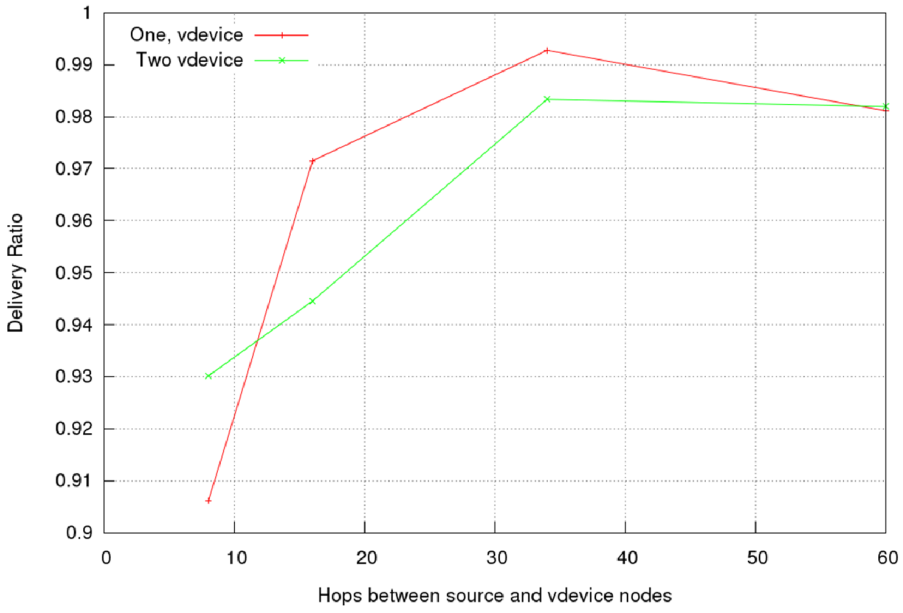

Figura V.6: relación de mensajes entregados y los transmitidos

al camino más corto, concluyendo que la latencia de Phantom se incrementa en relación directa a el número de saltos en su primera fase. En NUKU este parámetro está directamente relacionado con el valor de TTL. En la Figura V.7 se muestran los resultados de dos configuraciones del escenario, uno y dos *vdevice*, además cuatro diferentes distancias entre el nodo fuente y el nodo destino (8, 16, 34, y 60 saltos). Es importante notar que el valor de TTL se ajustó a la distancias antes mencionadas, esto es un nodo que estaba a 8 saltos del nodo sumidero. A TTL se le asigno un valor máximo de 15 saltos, la condición que se consideró para cada uno de los casos. El escenario con un *vdevice* la diferencia entre estos dos escenarios no es importante. T_l en 8 y 16 saltos es casi el doble que el requerido por la ruta más corta; sin embargo, este valor se reduce cuando el número de saltos es 34, T_l es igual a 50 saltos. Finalmente, la latencia de NUKU en 60 saltos se eleva hasta 103.

En los algoritmos de encaminamiento, cuya solución es el camino más corto entre dos puntos, *el número de transmisiones por mensaje entregado,* T_m es igual a la longitud de la ruta. Para Phantom, este valor esta relacionado con el número de saltos definidos en la primera fase, más las transmisiones que se requieren en la segunda, la cual esta definida por el tamaño de la red, multiplicado por la probabilidad de retransmisión: $n \times P_f$, donde n es el tamaño de la red y P_f se refiere a la posibilidad

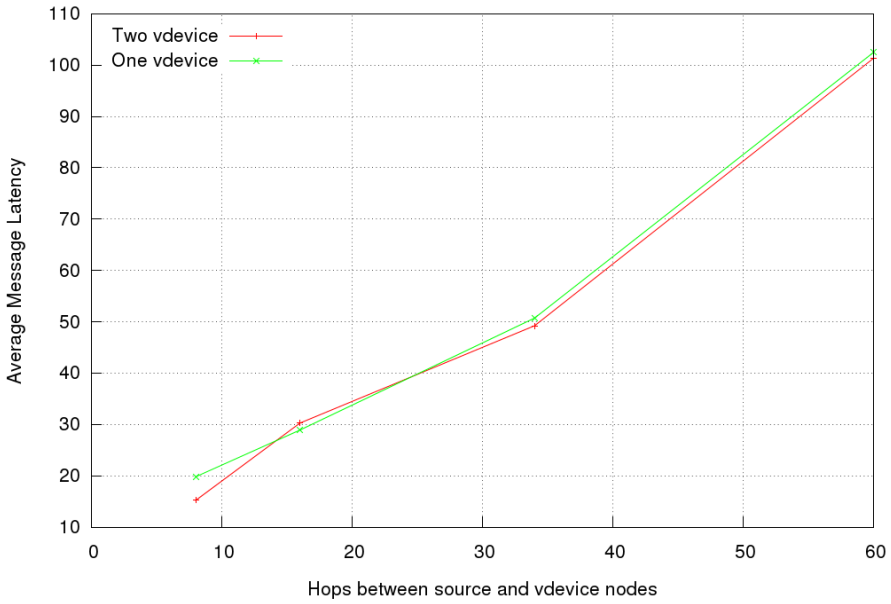

Figura V.7: Latencia promedio en los mensajes

de retransmisión por un nodo en la red, aun cuando esto no garantiza que cada uno de los mensajes alcance el nodo sumidero (Th. y otros , 2003). NUKU así como los algoritmos de encaminamiento que generan el camino más corto no usan mecanismos de ofuscación (ver Capitulo III) o los citados por Xi y otros (2006a), también del estudio que propone Kamat y otros (2005) respecto a protocolos de encaminamiento por inundación, esta muy relacionado con la longitud del camino más corto. La Figura V.7 provee información respecto a la latencia en numero de saltos, además del tráfico propio del algoritmo. No existen paquetes adicionales que hubieran sido generados por los mecanismos de ofuscación. Ello permite relacionar la latencia con el numero de retransmisiones, y concluir que NUKU usa menos transmisiones que Phantom durante la transmisión de información pese al proceso de señalización requerido por NUKU para mantener actualizada la información respecto a los niveles de feromona y las condiciones de visibilidad. NUKU incrementan el tráfico durante el proceso de búsqueda de rutas, valor directamente relacionado con el número de hormigas exploradoras.

La Tabla V.8 muestra una comparación entre los valores periodo de captura y la probabilidad de captura de los algoritmos NUKU y Phantom. Para Phantom, el mayor daño es causado por el *adversario paciente*, como se puede ver en los datos de los renglones uno y dos. Además, P_t en NUKU

es al menos tres veces más grande que en Phantom. Considerando el atacante de tipo 2, el periodo de seguridad en Phantom es mayor que en NUKU; sin embargo para el resto de las comparaciones NUKU presenta mejor comportamiento que Phantom. En esta investigación se incluye un tercer tipo de adversario llamado *Adversario Inteligente*. Este adversario se usó en NUKU, buscando ofrecer condiciones con un mayor reto para el algoritmo. Considerando este ultimo adversario, el periodo de seguridad ofrecido muestra su peor condición, cuando la distancia entre el nodo fuente y el destino es de 8 saltos. Para este último caso NUKU protegió 59 paquetes y 211 paquetes para la distancia de 34 saltos.

La probabilidad de captura en el escenario de 34 saltos es 0.28, mientras que para el escenario de 8 saltos, este parámetro se incrementa a 1.0. No fue posible realizar una comparación entre Phantom debido a que no se cuenta con información al respecto, sin embargo es posible deducir que en la fase de inundación, Phanton podría verse beneficiado, debido a su proceso de encaminamiento por inundación.

Tipo de Adversario	Distancia en saltos del Nodo destino al fuente	NUKU		Phantom	
		Periodo seguro P_t	Captura Probabilidad C	Seguro periodo P_t	Captura probabilidad C
1	34	396	0.15	90	1
1	8	154	0.38	32	1
2	34	249	0.24	301	0.6
2	8	67	0.88	54	0.9
3	34	211	0.28	ND	ND
3	8	59	1	ND	ND

Tabla V.8: NUKU y algoritmos Phantom consideraciones en el rendimiento, Secuencia para relacionar los tipos de adversario en la tabla (1) Pasivo (2) Cauteloso (3) Inteligente.

La Figura V.8, muestra la probabilidad de que un ataque sea exitoso, considerando *El modelo del adversario A,* y dos puntos desde los cuales un adversario iniciaría su ataque.

La Figura V.8 muestra la relación entre el peor caso ofrecido por todos los escenarios y P_t ofrecida por cada uno de ellos. Concluyendo que el adversario pasivo fue el que menos daño causo; ya que

la probabilidad de perpetrar un ataque exitoso fue del 0.4, cuando la distancia entre el *mdevice* y el *vdevice* es 8 saltos. Esta probabilidad decreció hasta 0.1, cuando se tenían 16 y 34 saltos de distancia. NUKU mostró el peor comportamiento ante el adversario de tipo 3; este tiene una probabilidad de 1 para alcanzar su objetivo, cuando la distancia entre el nodo fuente y el nodo destino es de 8 saltos. Para las distancias de 16 y 34 saltos, NUKU se comporta mejor.

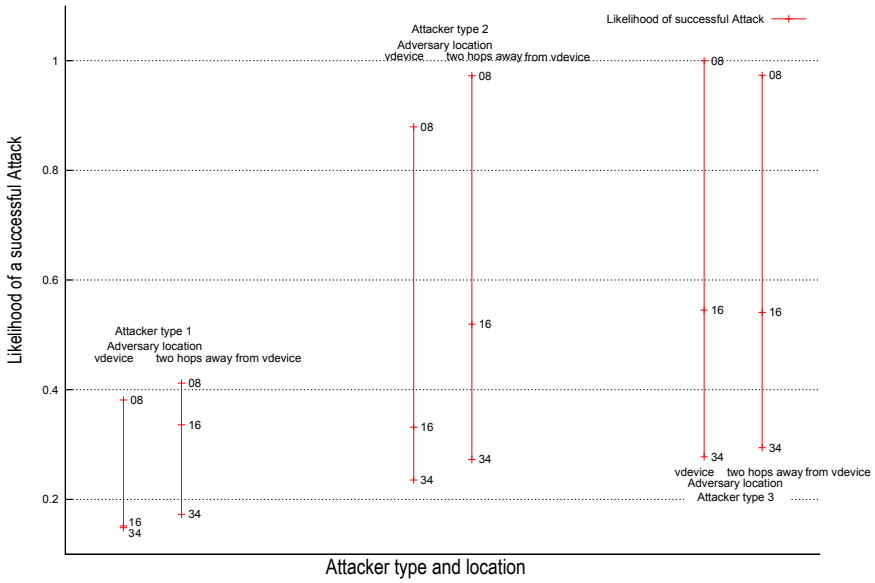

Figura V.8: Probabilidad de Ataques exitosos.

V.2 Patrones en las estrategias de ataque

Las siguientes figuras muestran las trazas de las tres estrategias que el adversario siguió, con el afán de obtener la información respecto a la ubicación del nodo fuente. Las Figuras V.9 y V.10, muestra una traza que sigue una dirección constante. Adversario espera que los paquetes lleguen al lugar donde él esta actualmente para continuar su ataque, aun cuando existe una consideración diferente respecto a la cantidad de *vdevice*, uno y dos en cada escenario.

Las Gráficas V.11 y V.12 muestran un patrón diferente, en este caso las trazas se distribuyen de

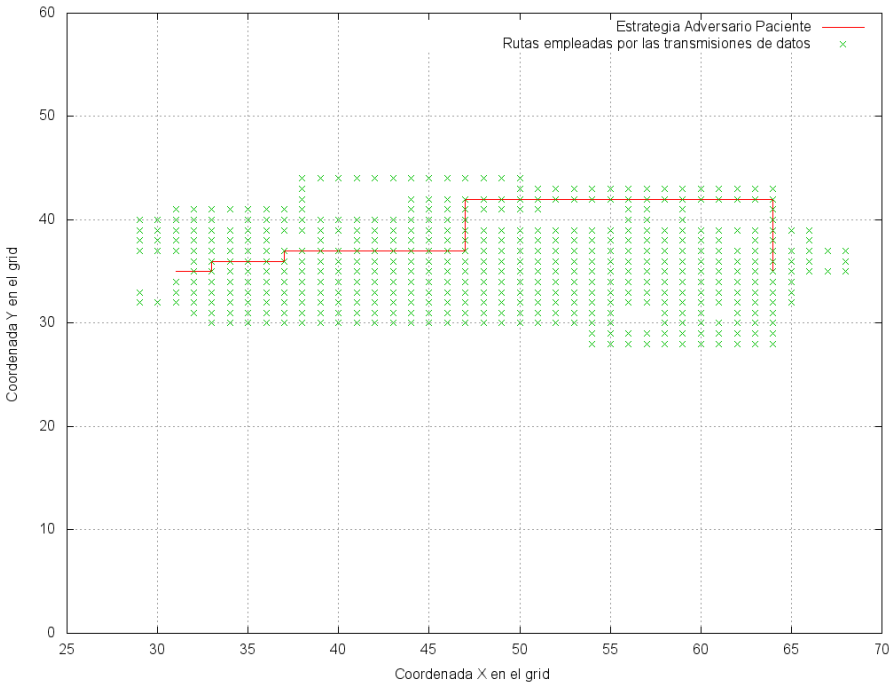

Figura V.9: Ruta generada por un Adversario siguiendo la estrategia Paciente para encontrar la fuente (1 *vdevice*).

una forma más amplia en las rutas que se utilizaron para la transmisión de paquetes.

Las Gráficas V.13 y V.14 presentan patrones de comportamiento muy dinámicos. Esta característica del adversario inteligente, le da mayor efectividad en el ataque como se demostró en las tablas y gráficas de la sección anterior.

Adicional al patrón de las estrategias en ataque, se indican las diferentes rutas generadas para la transmisión de paquetes. Este patrón sugiere un tipo de técnica de inundación por áreas. Por la estrategia que siguen las hormigas, ellas construyen caminos a seguir, mismos que son seleccionados considerando el nivel de feromona. Por esta razón la posibilidad de paquetes perdidos asociados a la saturación del canal es baja, como se muestra en la Tabla V.9

Los resultados obtenidos por NUKU para el parámetro paquetes perdidos se muestran en la Tabla V.9. El escenario se configuró con un vdevice y una fuente, repitiendo la misma estructura con diferentes distancias. El peor caso de paquetes perdidos se presentó cuando la distancia era de 60 saltos. En tanto el mejor caso se presento a una distancia de 4 saltos.

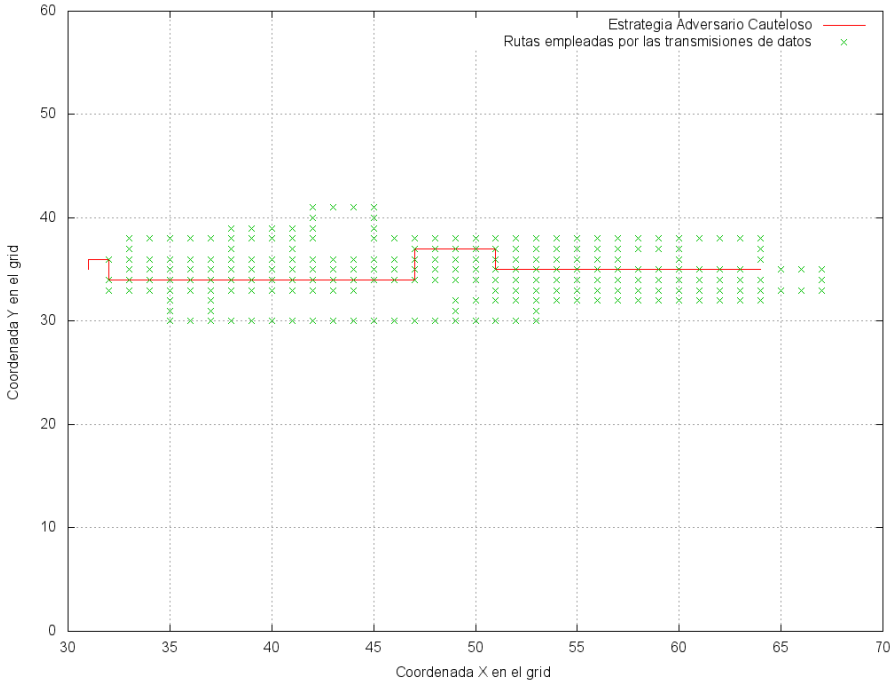

Figura V.10: Ruta generada por un Adversario siguiendo la estrategia Paciente para encontrar la fuente (2 *vdevice*).

Distancia en Saltos s-d	2	4	8	16	34	60
Paquetes	100	73806	10770	5872	21145	5017
Paquetes perdidos	0	606	278	66	214	996
Relación de paquetes perdidos	0	0.82 %	2.58 %	1.12 %	1.01 %	19.85 %

Tabla V.9: Paquetes perdidos durante la ejecución del algoritmo NUKU.

V.3 Conclusiones.

De los resultados obtenidos se concluye que NUKU cumple con el objetivo de proveer privacidad en la ubicación de la fuente. Sin embargo, encontrar el equilibrio entre el numero de hormigas que buscan un camino hacia el nodo sumidero no es una tarea trivial, ya que se busca diversidad en los caminos, entre las diferentes rutas que las hormigas ofrecen. Una gran cantidad de hormigas podría producir igual efecto que un encaminamiento por inundación. Adicional a ello tenemos el problema de

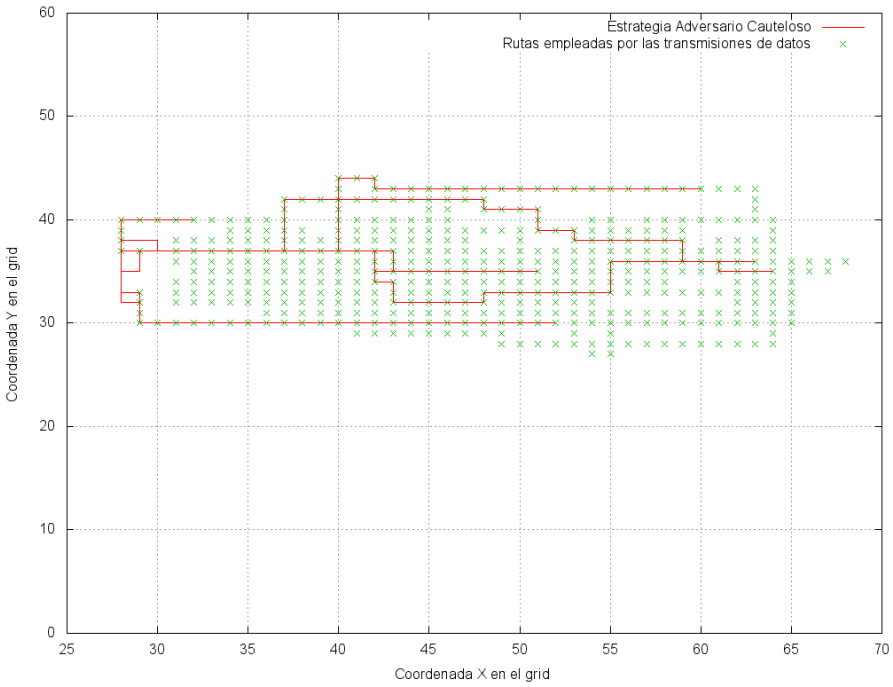

Figura V.11: Ruta generada por un Adversario siguiendo la estrategia Cauteloso para encontrar la fuente (1 *vdevice*).

latencia, ya que conforme los paquetes se transmiten por las rutas, los caminos mas cortos desaparecen, quedando los de mayor longitud activos hasta el final. Este ultimo problema se controla mediante el parámetro TTL, con lo cual del nodo fuente a un nodo sumidero virtual definimos el límite máximo de latencia en el escenario.

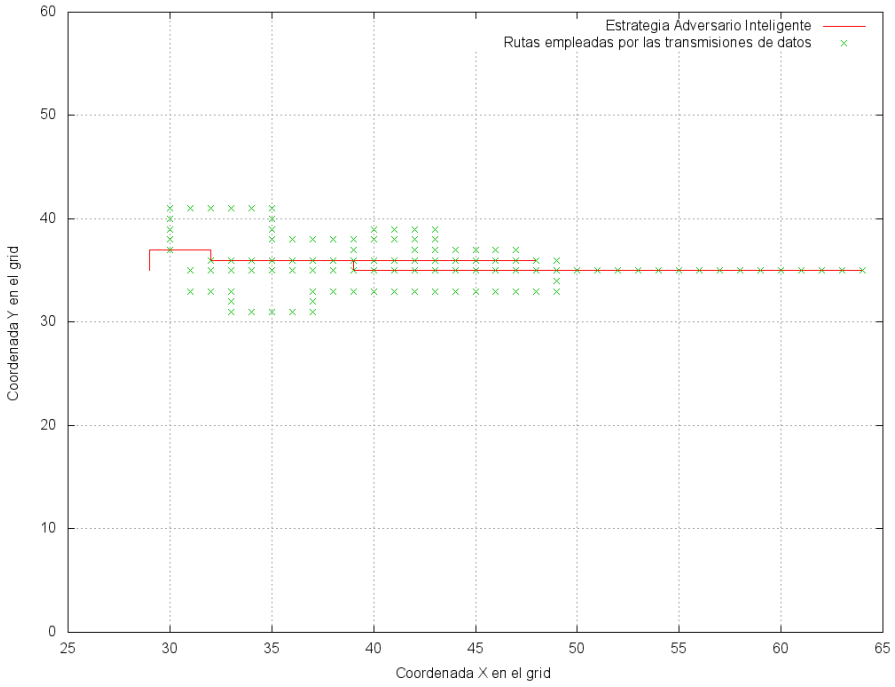

Figura V.12: Ruta generada por un Adversario siguiendo la estrategia Cauteloso para encontrar la fuente (2 *vdevice*).

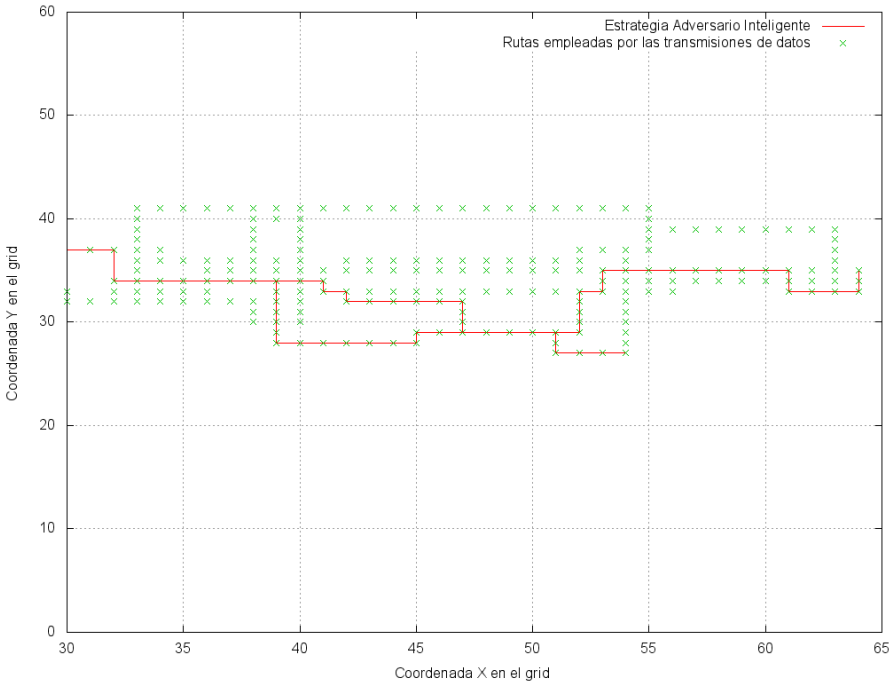

Figura V.13: Ruta generada por un Adversario siguiendo la estrategia Inteligente para encontrar la fuente (1 *vdevice*).

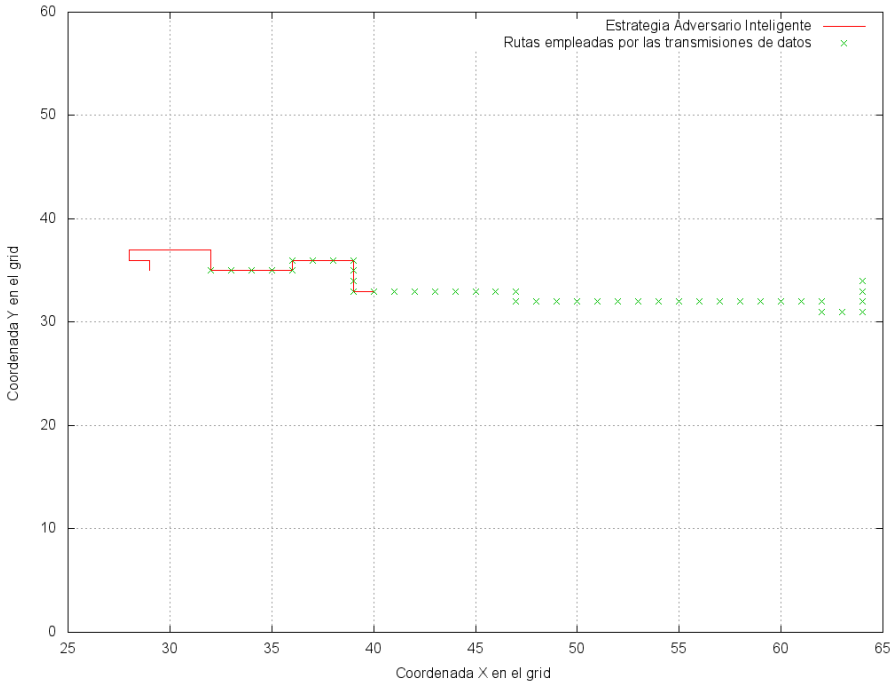

Figura V.14: Ruta generada por un Adversario siguiendo la estrategia Inteligente para encontrar la fuente (2 *vdevice*).

CAPÍTULO VI

CONCLUSIONES.

En esta tesis, a partir del estudio de heurísticas bioinspiradas se propuso un algoritmo para resolver problema de privacidad, en el de la ubicación de la fuente de datos.

El algoritmo propuesto NUKU se diferencia de otras soluciones por las siguientes características:

1. No hace uso de mecanismos de ofuscación como la técnica de inundación, los paquetes y fuentes falsas.
2. Reduce la probabilidad de ataques pasivos descritos en la sección *El Modelo de Adversario*.
3. Tiene consciencia del nivel de privacidad requerido por la transmisión.
4. Por el diseño NUKU no coopera al incremento del parámetro *paquetes perdidos*.

VI.1 Contribuciones y originalidad.

Las contribuciones de este trabajo se clasifican desde dos perspectivas: la metodológica y la implementación del algoritmo en dispositivos de bajo consumo de energía WSN.

VI.1.1 Contribuciones metodológicas.

Este trabajo contribuye con un algoritmo basado en una heurísticas bioinspirada para proveer la privacidad en la ubicación de los dispositivos fuente.

Adicionalmente, se propone una topología para los elementos de red que interacturán para el funcionamiento del algoritmo.

VI.1.2 Contribuciones de implementación

La arquitectura propuesta para la implementación de algoritmos de inteligencia computacional en dispositivos embebidos. Por *la Arquitectura* se refiere a la integración de los módulos del algoritmo con los elementos de hardware y software existentes en el dispositivo WSN.

VI.2 Trabajo a futuro

Se visualiza la posibilidad de adherir el tema de la privacidad a cuatro aspectos de investigación.

1. Distribución de llaves para el establecimiento de comunicaciones seguras. Nuestro interés reside en proteger los datos de control del protocolo de encaminamiento en soluciones distribuidas basadas en heurísticas bioinspiradas.

2. Métricas de privacidad. En una exploración inicial en este tema se encontró una gran número de mediciones con el objetivo y los métodos similares. Lo anterior refleja un problema ya visualizado en las aplicaciones para WSN con soluciones particulares a problemas muy similares. Justificadas en los recursos reducidos de los dispositivos.

3. En escenarios que integran la movilidad. Las trayectorias seguidas por dispositivos móviles y que son reveladas por las transmisiones que realizan hacia el nodo sumidero o estación base. Esta información permite deducir datos clasificados como personales la identificación del portador del mismo.

4. Configuración de los parámetros del algoritmo referido en la literatura como *Calibración del algoritmo*, haciendo énfasis en los requerimientos de privacidad.

Bibliografía

Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26–33, January 2005. ISSN 1540-7993. doi: 10.1109/MSP.2005.22. URL http://dx.doi.org/10.1109/MSP.2005.22.

Lorrie Cranor Alessandro Acquisti Janice Tsai, Serge Egelman. The effect of online privacy information on purchasing behavior: An experimental study. Electronic, june 2007. URL http://weis2007.econinfosec.org/papers/57.pdf.

I. Altman. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co., 1975. ISBN 9780818501685. URL http://books.google.com.mx/books?id=GLBPAAAAMAAJ.

Alastair R. Beresford and Frank Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55, January 2003. ISSN 1536-1268. doi: 10.1109/MPRV.2003.1186725. URL http://dx.doi.org/10.1109/MPRV.2003.1186725.

Charalampos Doukas and Ilias Maglogiannis. Intelligent pervasive healthcare systems. In Margarita Sordo, Sachin Vaidya, and Lakhmi Jain, editors, *Advanced Computational Intelligence Paradigms in Healthcare - 3*, volume 107 of *Studies in Computational Intelligence*, pages 95–115. Springer Berlin / Heidelberg, 2008. ISBN 978-3-540-77661-1. URL http://dx.doi.org/10.1007/978-3-540-77662-8_5. 10.1007/978-3-540-77662-8_5.

Sriram Lakshmanan and Raghupathy Sivakumar. Diversity routing for multi-hop wireless networks with cooperative transmissions. In *Proceedings of the 6th Annual IEEE communications society*

conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON'09, pages 610–618, Piscataway, NJ, USA, 2009. IEEE Press. ISBN 978-1-4244-2907-3. URL http://dl.acm.org/citation.cfm?id=1687299.1687368.

B. Schilit, N. Adams, and R. Want. Context-aware computing applications. In *Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications*, WMCSA '94, pages 85–90, Washington, DC, USA, 1994. IEEE Computer Society. ISBN 978-0-7695-3451-0. doi: 10.1109/WMCSA.1994.16. URL http://dx.doi.org/10.1109/WMCSA.1994.16.

Gregory D. Abowd, Anind K. Dey, Peter J. Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, HUC '99, pages 304–307, London, UK, UK, 1999. Springer-Verlag. ISBN 3-540-66550-1. URL http://dl.acm.org/citation.cfm?id=647985.743843.

R. Rios and J. Lopez. Analysis of location privacy solutions in wireless sensor networks. *Communications, IET*, 5(17):2518 –2532, 25 2011. ISSN 1751-8628. doi: 10.1049/iet-com.2010.0825.

Celal Ozturk, Yanyong Zhang, and Wade Trappe. Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, SASN '04, pages 88–93, New York, NY, USA, 2004. ACM. ISBN 1-58113-972-1. doi: 10.1145/1029102.1029117. URL http://doi.acm.org/10.1145/1029102.1029117.

P. Kamat, Yanyong Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*, pages 599 –608, june 2005. doi: 10.1109/ICDCS.2005.31.

IEEE LAN/MAN Standards Committee. *IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements–Part 15.4: Wireless MAC and PHY Specifications for Low-Rate WPANs*. IEEE, IEEE, 3 Park Avenue New York, NY 10016-5997, USA, revision ieee std 802.15.4-2003 edition, Septiembre 2006.

Jianliang Zheng and M J Lee. Will ieee 802.15.4 make ubiquitous networking a reality?: a discussion on a potential low power, low bit rate standard. *Communications Magazine, IEEE*, 42(6):140–146, June 2004. ISSN 0163-6804. doi: 10.1109/MCOM.2004.1304251.

Kazem Sohraby, Daniel Minoli, and Taieb Znati. *Wireless Sensor Networks: Technology, Protocols, and Applications*. 2007. URL http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471743003.html.

T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein. *Introduction To Algorithms*. MIT Press, 2001. ISBN 9780262032933. URL http://books.google.com.mx/books?id=NLngYyWFl_YC.

Stelios H Zanakis and James R Evans. Heuristic optimization:why, when, and how to use it. *Interfaces*, 11(5):84–91, 1981. URL http://interfaces.journal.informs.org/cgi/doi/10.1287/inte.11.5.84.

Godfrey C. Onwubolu and B. V. Babu. *New optimization techniques in engineering*, volume 141 of *Studies in Fuzziness and Soft Computing*. Springer, 2004. ISBN 978-3-540-20167-0.

Muhammad Saleem, Gianni A. Di Caro, and Muddassar Farooq. Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions. *Inf. Sci.*, 181(20):4597–4624, October 2011. ISSN 0020-0255. doi: 10.1016/j.ins.2010.07.005. URL http://dx.doi.org/10.1016/j.ins.2010.07.005.

L.J.G. Villalba, D.R. Cañandas, and A.L.S. Orozco. Bio-inspired routing protocol for mobile ad hoc networks. *Communications, IET*, 4(18):2187 –2195, 17 2010. ISSN 1751-8628. doi: 10.1049/iet-com.2009.0826.

Fred Glover. Future paths for integer programming and links to artificial intelligence. *Computers & OR*, 13(5):533–549, 1986.

Ibrahim H Osman and Gilbert Laporte. Metaheuristics : A bibliography. *Annals of Operations Research*, 63:513–623, 1996.

Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, 2003.

Riaz Ahmed Shaikh, Hassan Jameel, Brian J. DÁuriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song. Achieving network level privacy in wireless sensor networks. *Sensors*, 10(3):1447–1472, 2010. ISSN 1424-8220. doi: 10.3390/s100301447. URL http://www.mdpi.com/1424-8220/10/3/1447.

Ivan Stojmenovic. *Handbook of Sensor Networks : Algorithms and Architectures*. Wiley, 2005.

Anind Dey, Jeffrey Hightower, Eyal de Lara, and Nigel Davies. Location-based services. *Pervasive Computing, IEEE*, 9(1):11 –12, jan.-march 2010. ISSN 1536-1268. doi: 10.1109/MPRV.2010.10.

George Danezis, Roger Dingledine, David Hopwood, and Nick Mathewson. Mixminion: Design of a type iii anonymous remailer protocol. In *In Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, 2003.

Ying Jian, Shigang Chen, Zhan Zhang, and Liang Zhang. A novel scheme for protecting receiver's location privacy in wireless sensor networks. *Trans. Wireless. Comm.*, 7(10):3769–3779, October 2008. ISSN 1536-1276. doi: 10.1109/T-WC.2008.070182. URL http://dx.doi.org/10.1109/T-WC.2008.070182.

Alireza A. Nezhad, Ali Miri, and Dimitris Makrakis. Location privacy and anonymity preserving routing for wireless sensor networks. *Comput. Netw.*, 52(18):3433–3452, December 2008. ISSN 1389-1286. doi: 10.1016/j.comnet.2008.09.005. URL http://dx.doi.org/10.1016/j.comnet.2008.09.005.

Krishna Sampigethaya and Radha Poovendran. A Survey on Mix Networks and Their Secure Applications. *Proceedings of the IEEE*, 94(12), December 2006.

David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, February 1981. ISSN 0001-0782. doi: 10.1145/358549.358563. URL http://doi.acm.org/10.1145/358549.358563.

T. Dierks Certicom and C. Allen. The TLS Protocol Version 1.0. URL http://www.ietf.org/rfc/rfc2246.txt.

Xi Luo, Xu Ji, and Myong-Soon Park. Location Privacy against Traffic Analysis Attacks in Wireless Sensor Networks. *2010 International Conference on Information Science and Applications*, pages 1–6, 2010. doi: 10.1109/ICISA.2010.5480564. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5480564.

Yong Xi, L. Schwiebert, and Weisong Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, page 8 pp., april 2006a. doi: 10.1109/IPDPS.2006.1639682.

Yun Li and Jian Ren. Source-Location Privacy through Dynamic Routing in Wireless Sensor Networks. *2010 Proceedings IEEE INFOCOM*, pages 1–9, March 2010. doi: 10.1109/INFCOM.2010.5462096. URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5462096.

Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, page 21. USENIX Association, 2004. URL http://portal.acm.org/citation.cfm?id=1251375.1251396.

M.K. Reiter and A.D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security (TISSEC)*, 1(1):92, 1998. URL http://portal.acm.org/citation.cfm?id=290163.290168.

Michael J. Freedman and Robert Morris. Tarzan: a peer-to-peer anonymizing network layer. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS '02, pages 193–206, New York, NY, USA, 2002. ACM. ISBN 1-58113-612-9. doi: 10.1145/586110.586137. URL http://doi.acm.org/10.1145/586110.586137.

Kevin Fall. A delay-tolerant network architecture for challenged internets. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, SIGCOMM '03, pages 27–34, New York, NY, USA, 2003. ACM. ISBN 1-58113-735-4. doi: 10.1145/863955.863960. URL http://doi.acm.org/10.1145/863955.863960.

Pan Hui, Augustin Chaintreau, James Scott, Richard Gass, Jon Crowcroft, and Christophe Diot. Pocket switched networks and human mobility in conference environments. In *Proceedings of the 2005*

ACM SIGCOMM workshop on Delay-tolerant networking, WDTN '05, pages 244–251, New York, NY, USA, 2005. ACM. ISBN 1-59593-026-4. doi: 10.1145/1080139.1080142. URL http://doi.acm.org/10.1145/1080139.1080142.

Thang N. Dinh, Ying Xuan, and My T. Thai. Towards social-aware routing in dynamic communication networks. In *IPCCC*, pages 161–168. IEEE, 2009.

P. Spachos, Liang Song, and D. Hatzinakos. Opportunistic routing for enhanced source-location privacy in wireless sensor networks. In *Communications (QBSC), 2010 25th Biennial Symposium on*, pages 315 –318, may 2010. doi: 10.1109/BSC.2010.5472946.

Y. Xi, L. Schwiebert, and W. Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, pages 8–pp. IEEE, 2006b. ISBN 1-4244-0054-6. doi: 10.1109/IPDPS.2006.1639682. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1639682.

Henrik Abrahamsson, Bengt Ahlgren, Juan Alonso, Anders Andersson, and Per Kreuger. A multi-path routing algorithm for ip networks based on flow optimisation. In *Proceedings of the 3rd international conference on quality of future internet services and internet charging and QoS technologies 2nd international conference on From QoS provisioning to QoS charging*, QofIS'02/ICQT'02, pages 135–144, Berlin, Heidelberg, 2002. Springer-Verlag. ISBN 3-540-44356-8. URL http://dl.acm.org/citation.cfm?id=1754656.1754674.

Saeed Rasouli Heikalabad, Hossein Rasouli, Farhad Nematy, and Naeim Rahmani. Qempar: Qos and energy aware multi-path routing algorithm for real-time applications in wireless sensor networks. *CoRR*, abs/1104.1031, 2011. URL http://dblp.uni-trier.de/db/journals/corr/corr1104.html#abs-1104-1031.

Wenjing Lou, Wei Liu, Yanchao Zhang, and Yuguang Fang. Spread: Improving network security by multipath routing in mobile ad hoc networks. *Wirel. Netw.*, 15(3):279–294, April 2009. ISSN 1022-0038. doi: 10.1007/s11276-007-0039-4. URL http://dx.doi.org/10.1007/s11276-007-0039-4.

Poonam Gera, Kumkum Garg, and Manoj Misra. Trust based multi-path routing for end to end secure data delivery in manets. In *Proceedings of the 3rd international conference on Security of information and networks*, SIN '10, pages 81–89, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0234-0. doi: 10.1145/1854099.1854117. URL http://doi.acm.org/10.1145/1854099.1854117.

Frederick Ducatelle, Gianni Di Caro, and Luca Maria Gambardella. Ant agents for hybrid multipath routing in mobile ad hoc networks. In *Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services*, WONS '05, pages 44–53, Washington, DC, USA, 2005. IEEE Computer Society. ISBN 0-7695-2290-0. doi: 10.1109/WONS.2005.3. URL http://dx.doi.org/10.1109/WONS.2005.3.

J. J. Hopfield. Neurocomputing: foundations of research. chapter Neural networks and physical systems with emergent collective computational abilities, pages 457–464. MIT Press, Cambridge, MA, USA, 1988. ISBN 0-262-01097-6. URL http://dl.acm.org/citation.cfm?id=65669.104422.

E.G. Talbi. *Metaheuristics: From Design to Implementation*. Wiley Series on Parallel and Distributed Computing. Wiley, 2009. ISBN 9780470278581. URL http://books.google.es/books?id=SIsa6zi5XV8C.

Jonathan Timmis Leandro Nunes de Castro. *Artificial Immune Systems: A New Computational Intelligence Approach*. Springer, 1st edition. edition, November 2002. ISBN 1852335947.

Earl Cox, Michael O'Hagan, Rodman Taber, and Michael O'Hagen. *The Fuzzy Systems Handkbook with Cdrom*. Academic Press, Inc., Orlando, FL, USA, 2nd edition, 1998. ISBN 0121944557.

M. Dorigo, V. Maniezzo, and A. Colorni. Ant system: optimization by a colony of cooperating agents. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 26(1):29 –41, feb 1996. ISSN 1083-4419. doi: 10.1109/3477.484436.

R.V. Kulkarni, A. Fö andrster, and G.K. Venayagamoorthy. Computational intelligence in wireless sensor networks: A survey. *Communications Surveys Tutorials, IEEE*, 13(1):68 –96, quarter 2011. ISSN 1553-877X. doi: 10.1109/SURV.2011.040310.00002.

K.E. Parsopoulos. *Particle Swarm Optimization and Intelligence: Advances and Applications*. IGI Global, 2009. ISBN 9781615206674. URL http://books.google.com.mx/books?id=CSqZW327ekYC.

Gianni Di Caro, Frederick Ducatelle, and Luca Maria Gambardella. Anthocnet: An ant-based hybrid routing algorithm for mobile ad hoc networks. In Xin Yao, Edmund K. Burke, José Antonio Lozano, Jim Smith, Juan J. Merelo Guervós, John A. Bullinaria, Jonathan E. Rowe, Peter Ti no, Ata Kabán, and Hans-Paul Schwefel, editors, *Parallel Problem Solving from Nature - PPSN VIII, 8th International Conference, Birmingham, UK, September 18-22, 2004, Proceedings*, volume 3242 of *Lecture Notes in Computer Science*, pages 461–470. Springer, 2004. ISBN 3-540-23092-0. doi: http://springerlink.metapress.com/openurl.asp?genre=article\&issn=0302-9743\&volume=3242\&spage=461.

E D Lumer and B Faieta. Diversity and adaptation in populations of clustering ants. In J A Meyer and S W Wilson, editors, *Proceedings of the Third International Conference on Simulation of Adaptive Behavior From Animals to Animats 3*, pages 501–508. MIT Press, 1994. ISBN 0262531224.

Zhi Yuan, Marco Montes de Oca, Mauro Birattari, and Thomas Stützle. Continuous optimization algorithms for tuning real and integer parameters of swarm intelligence algorithms. *Swarm Intelligence*, 6:49–75, 2012. ISSN 1935-3812. URL http://dx.doi.org/10.1007/s11721-011-0065-9. 10.1007/s11721-011-0065-9.

Han Huang, Xiaowei Yang, Zhifeng Hao, and Ruichu Cai. A novel aco algorithm with adaptive parameter. In *Proceedings of the 2006 international conference on Computational Intelligence and Bioinformatics - Volume Part III*, ICIC'06, pages 12–21, Berlin, Heidelberg, 2006. Springer-Verlag. ISBN 3-540-37277-6, 978-3-540-37277-6. doi: 10.1007/11816102_2. URL http://dx.doi.org/10.1007/11816102_2.

Weixin Ling and Huanping Luo. An adaptive parameter control strategy for ant colony optimization. In *Computational Intelligence and Security, 2007 International Conferenceon*, pages 142 –146, dec. 2007. doi: 10.1109/CIS.2007.156.

Moshaddique Ameen, Jingwei Liu, and Kyungsup Kwak. Security and Privacy Issues in Wireless

Sensor Networks for Healthcare Applications. *Journal of Medical Systems*, 36(1):93–101, March 2012. ISSN 0148-5598. doi: 10.1007/s10916-010-9449-4. URL http://www.springerlink.com/index/10.1007/s10916-010-9449-4.

W. Trappe and L.C. Washington. *Introduction to cryptography: with coding theory*. Prentice Hall, 2002. ISBN 9780130618146. URL http://books.google.de/books?id=kVU_AQAAIAAJ.

Richard Barr, Bruce Golden, James Kelly, Mauricio Resende, and William Stewart. Designing and reporting on computational experiments with heuristic methods. *Journal of Heuristics*, 1:9–32, 1995. ISSN 1381-1231. URL http://dx.doi.org/10.1007/BF02430363. 10.1007/BF02430363.

Eugster P. Th., R. Guerraoui, S. B. Handurukande, P. Kouznetsov, and A.-M. Kermarrec. Lightweight probabilistic broadcast. *ACM Trans. Comput. Syst.*, 21(4):341–374, November 2003. ISSN 0734-2071. doi: 10.1145/945506.945507. URL http://doi.acm.org/10.1145/945506.945507.