R. Rios, and J. Lopez, "Adecuación de soluciones de anonimato al problema de la privacidad de localización en WSN", *XII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2012)*, pp. 309-314, 2012.
NICS Lab. Publications: https://www.nics.uma.es/publications

Adecuación de soluciones de anonimato al problema de la privacidad de localización en WSN

Ruben Rios
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: ruben@lcc.uma.es

Javier Lopez
Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: jlm@lcc.uma.es

***Resumen*—Los patrones de tráfico característicos de las redes inalámbricas de sensores (WSNs) dan lugar al problema de la privacidad de localización. De manera similar, el tráfico de los usuarios en Internet revela información sensible que puede ser protegida mediante sistemas de comunicación anónima (ACS). Por ello, este trabajo analiza la posibilidad de adaptar las soluciones de anonimato tradicionales al problema particular de las redes de sensores. Hasta el momento estas soluciones habían sido rechazadas sin un análisis riguroso, argumentando simplemente que eran demasiado exigentes computacionalmente para los nodos sensores. Nuestros resultados demuestran que, en general, algunos ACS no cumplen los requisitos de privacidad necesarios en WSNs mientras que otros, que si los cumplen, se valen de una cantidad de recursos que superan la capacidad de los sensores.**

I. Introducción

Las redes inalámbricas de sensores (WSNs) son redes compuestas de dispositivos embebidos (nodos sensores o sensores) con capacidades de cómputo, memoria y comunicación limitadas. Estos nodos sensores son capaces de medir ciertas propiedades físicas en su entorno y comunicar la presencia de eventos (i.e., fenómenos de interés) a un dispositivo colector llamado estación base, que se encarga de procesar la información [1]. Estas características hacen de las WSNs una tecnología muy versátil capaz de adaptarse a multitud de escenarios.

Sin embargo, la naturaleza desatendida y sus limitados recursos hacen de las WSNs un claro objetivo para atacantes que amenazan con destruir la red o aprovecharse de sus recursos [2]. En particular, un atacante puede limitarse a observar el funcionamiento de la red y deducir información sensible de la propia red así como del contexto que la rodea.

La localización de los nodos que reportan eventos y la localización de la estación base es información contextual de gran relevancia. Un adversario capaz de determinar el nodo que genera un mensaje obtiene la localización de los fenómenos monitorizados que, dependiendo del escenario de aplicación, podrían referirse a individuos, a recursos de gran valor o estratégicamente relevantes. Esta información podría ser utilizada para fines maliciosos, desde acoso o daño físico hasta robo o espionaje industrial. Por otro lado, localización de la estación base permite a un atacante comprometer su integridad o incluso destruirla, dejando inservible a toda la red. Además de la protección física, la ubicación de la estación base proporciona información de carácter estratégico, ya que al tratarse de un dispositivo crítico, suele encontrarse en dependencias privilegiadas. Estos problemas son extensibles a cualquier escenario de WSNs, sin embargo, la importancia del problema se pone de manifiesto en escenarios de elevada criticidad, como la vigilancia de conflictos bélicos, el seguimiento de mercancías, y la protección de infraestructuras críticas.

El origen del problema se encuentran en los marcados patrones de comunicación de las WSNs, que relevan información de a pesar de que el contenido de los paquetes esté debidamente protegido mediante técnicas de confidencialidad. Dado que los sistemas de comunicación anónima (ACS) tradicionales fueron diseñados para dificultar el análisis de tráfico, estos sistemas son a priori una solución plausible al problema. A pesar de ello, la literatura en WSNs [3], [4], [5] establece que estos sistemas no son aplicables en este dominio. Los argumentos presentados en estos trabajos son demasiado vagos, centrándose únicamente en la limitación física de los recursos de los sensores. Estamos convencidos de que es necesario realizar un análisis más riguroso antes de descartar estas soluciones, especialmente si consideramos el nivel de madurez que han alcanzado los ACS. En particular, creemos que un análisis más estricto permitirá el desarrollo de nuevas y mejoradas soluciones para WSNs.

El objetivo de este trabajo es realizar un análisis meticuloso de los requisitos, objetivos y técnicas propuestas por los sistemas tradicionales para determinar la potencial aplicación de estas soluciones al problema de la privacidad de localización en WSNs. Para ello, el resto de este trabajo se organiza de la siguiente forma. En la Sec. II se ofrece una definición detallada del problema de la privacidad de localización y las características de las WSNs que originan el problema, así como de los modelos de adversario. Seguidamente, la Sec. III hace un repaso sobre las propiedades de los ACS tradicionales y las necesidades de privacidad particulares en WSNs. En la Sec. IV se analizan las características principales, requisitos y limitaciones de tres notables ACS en relación al escenario de WSNs. La Sec. V ofrece una breve discusión antes de concluir nuestro trabajo en la Sec. VI.

II. Privacidad de localización en WSNs

Esta sección proporciona una descripción de las causas que dan lugar al problema de privacidad de localización.

Asimismo, se describen los diferentes modelos de atacante que pueden amenazar tanto a los nodos origen de eventos (nodos fuente) como a la estación base.

A. Naturaleza del problema

Las redes de sensores suelen utilizar mecanismos criptográficos que protegen el contenido de los paquetes frente a escuchas no autorizadas. No obstante, un adversario puede obtener información sensible sobre la red y su contexto simplemente observando el comportamiento de la misma.

Existe gran cantidad de meta-información asociada a diversas características de las comunicaciones en WSNs [6]. Así, por ejemplo, conocer la frecuencia de transmisión permite a un observador determinar el tipo de sensor ya que diferentes plataformas utilizan bandas de frecuencia diferente. Por otra parte, la tasa de envío y el tamaño de los paquetes ofrece información relativa a la naturaleza de los eventos. Además, los protocolos de encaminamiento revelan información sobre la topología de la red y, más concretamente, la localización de los nodos que se comunican.

En particular, conocer la localización de determinados nodos ofrece información sensible sobre la propia red y el entorno monitorizado. Considérese, por ejemplo, un escenario en el que una WSNs se despliega para el seguimiento de mercancías en un área comercial. Un atacante que observa las comunicaciones y obtiene la localización de los nodos fuente puede seguir el movimiento de las mercancías y, por tanto, deducir la organización de la planta así como las relaciones entre distintos proveedores. Por otra parte, el atacante podría desear destruir o comprometer la red para su propio beneficio con lo que le bastaría determinar la localización de la estación base.

B. Modelos de Atacante

El modelo de atacante determina directamente las medidas de protección necesarias. En concreto, en este dominio los atacantes suelen limitarse a observar las comunicaciones sin interferir en el comportamiento normal de la red. Estos atacantes pasivos suelen distinguirse por su radio de escucha.

Los atacantes con capacidad para monitorizar las comunicaciones de un número limitado de sensores son conocidos como atacantes locales. Este tipo de atacantes es capaz de contar el número de paquetes en su entorno así como medir el ángulo de llegada de los mismos. Esto les permite determinar los nodos que envían los paquetes en su entorno. Además, el atacante aprovecha que las rutas seguidas por los paquetes suelen permanecer inalteradas ya que se trata de utilizar el camino más corto para minimizar así el consumo energético. A partir de esta información, el atacante elige una estrategia de movimiento dependiendo de si su objetivo es determinar la localización de nodos fuente o de la estación base. En el primer caso, el atacante esperará a escuchar mensajes y seguirá el flujo generado de manera inversa, acercándose un salto por cada paquete recibido. Cuando el objetivo es localizar la estación base, el atacante relaciona los tiempos de envío entre un nodo y sus vecinos para determinar el sentido de la comunicación. Asimismo, otra estrategia es avanzar hacia los nodos con mayor tasa de envío dado que los nodos próximos a la estación base reenvían un mayor número de paquetes.

Los atacantes globales son capaces de observar las transmisiones de todos los nodos de la red. Bajo este modelo, los nodos fuente pueden ser fácilmente detectados ya que generan nuevo tráfico inmediatamente después de detectar un evento. En particular, al comparar el número de paquetes entrantes y salientes en un nodo, el atacante puede distinguir fehacientemente entre nodos fuentes e intermediarios. Asimismo, la localización de la estación base es fácilmente identificable al encontrarse en una zona con un gran volumen de tráfico.

Además de atacantes pasivos, existe la amenaza de adversarios que comprometen ciertos nodos y los utilizan para controlar algunos flujos de comunicación. Estos atacantes, al formar parte de la propia red, tienen acceso a los secretos compartidos. Por tanto, los atacantes internos pueden recuperar el contenido y cabecera de los paquetes que observan en su entorno, lo cual les permite conocer la identidad del nodo que originó el mensaje.

III. Requisitos de privacidad en WSNs

En esta sección se ofrece un breve repaso sobre algunas propiedades muy relevantes en el ámbito de privacidad. Seguidamente, se discute la adecuación de estas propiedades al problema de la privacidad de localización en WSNs.

A. Repaso de propiedades de anonimato

La privacidad es un concepto muy amplio que abarca diferentes aspectos [7]. Una de estas perspectivas se refiere a la privacidad como la capacidad de mantener el control frente a la adquisición, revelación y uso de información personal. A este respecto se han desarrollado diferentes técnicas que se sustentan sobre la consecución de las diferentes propiedades [8] que describimos a continuación.

El *anonimato* es la capacidad de un sujeto de no ser suficientemente identificable entre un grupo de individuos con los mismos atributos que éste. En otras palabras, los mecanismos de anonimato preservan la identidad del individuo que realiza una acción haciéndolo indistinguible de un grupo de actores potenciales. En el ámbito de las comunicaciones, la acción normalmente se refiere al envío o recepción de un mensaje.

De especial importancia es también la propiedad de no-enlazabilidad o *unlinkability*. Esta propiedad se refiere a la incapacidad de un atacante para distinguir fehacientemente si dos o más objetos de interés están relacionados. En un sistema de comunicación estos objetos de interés podrían ser mensajes o incluso un participante. Los ACS suelen esforzarse por proporcionar esta propiedad porque permite ocultar con qué entidad se comunican los participantes del sistema. Además, esta propiedad sugiere que si dos entidades son identificadas como participantes del sistema, no es posible determinar que se comunican entre ellas. Es, por tanto, una propiedad más fuerte que el anonimato.

Por último, las propiedades de indetectabilidad e inobservabilidad se centran en la protección de los objetos de interés por si mismos. La indetectabilidad o *undetectability* evita que un atacante pueda tener la certeza de que un objeto de interés existe. Por otra parte, la inobservabilidad o *unobservability* proporciona además anonimato a otras entidades relacionadas con el objeto de interés. Por tanto, la indetectabilidad oculta la existencia de mensajes reales mientras que la inobservabilidad además implica que si los mensajes son descubiertos, sus emisores y receptores no pueden ser identificados.

B. Propiedades necesarias en WSNs

El problema de la privacidad de localización es una clara consecuencia de los marcados patrones de tráfico en las WSNs que exponen al origen y destino de las comunicaciones. Si bien una de las características fundamentales de los ACS es que proporcionan mecanismos para dificultar el análisis de tráfico, no todos estos sistemas persiguen las mismas propiedades. Del mismo modo, no todas las propiedades descritas en la sección anterior son de utilidad en WSNs.

La función del anonimato en WSNs es bastante limitada, siendo incluso contraproducente en ciertas situaciones. La estación base debe conocer en todo momento la identidad de los nodos fuente ya que esto permite relacionar un evento con su ubicación. En consecuencia, si la identidad de un nodo no es dada a la estación base, la red dejar de ser de utilidad. No obstante, el anonimato del emisor es conveniente frente a observadores externos así como frente a atacante internos. Si el adversario conoce el identificador del emisor podrá determinar su ubicación. Por tanto, el anonimato de nodos fuente sólo es de interés en determinadas ocasiones.

Por otro lado, la propiedad de unlinkability entre fuente y destino no tiene mucho sentido en WSNs ya que es bien sabido que todos los nodos se comunican con una única estación base. Por el contrario, en otros modelos de comunicación, como Internet, esta propiedad es mucho más relevante porque impide a un atacante determinar con quién se comunica un usuario. En cambio, en las WSNs la enlazabilidad es problemática si el atacante es capaz de determinar que un paquete pertenece a un nodo determinado ya que esto le guiaría directamente a la zona de la red donde se produce el evento. En tal caso, estamos ante la misma situación que la presentada anteriormente para la propiedad de anonimato.

La propiedad más natural para la protección de la información de localización en WSNs es la inobservabilidad. Es necesario ocultar la existencia de los nodos que emiten o reciben mensajes. En particular, si el atacante es incapaz de observar la presencia de mensajes de evento tampoco podrá determinar la localización de los nodos que se comunican. Incluso si el atacante fuera capaz de determinar qué mensajes son reales, el origen y destino deberían permanecer secretos.

En definitiva, no todas las propiedades mencionadas son adecuadas al problema de la privacidad de localización en WSNs. A continuación analizaremos varios sistemas de anonimato tradicionales con el fin de determinar si los mecanismos propuestos así como el consumo de recursos se adecuan al dominio de las redes de sensores.

IV. Análisis de sistemas de anonimato en WSNs

Los sistemas de comunicación anónima tienen como principal objetivo dificultar el análisis de tráfico para proteger la privacidad. Entre los numerosos sistemas existentes hemos elegido tres soluciones notables que, además de cubrir un amplio abanico de técnicas, persiguen diferentes propiedades de anonimato. A partir de esta muestra realizamos un análisis pormenorizado de las características y limitaciones principales de los ACS así como de su potencial aplicación a las particularidades del problema de la privacidad de localización en WSNs.

A. Onion Routing y Tor

Onion routing [9] es un modelo centralizado formado por un conjunto de dispositivos, onion routers, que se sitúan entre los posibles emisores y receptores para encaminar el tráfico. La función principal de estos dispositivos es ocultar la correspondencia entre los mensajes que reciben y envían. Para ello, a cada salto, se introducen pequeños retardos y se cambia la apariencia de los mensajes mediante el uso de criptografía. Cuando un emisor necesita enviar información es necesario establecer una ruta o circuito dentro del sistema. El circuito lo establece el emisor mediante una estructura de datos formada por varias capas de criptografía asimétrica que contienen las claves que cada intermediario usará para descifrar el flujo de datos y el siguiente nodo del circuito. En una versión posterior, Tor [10], se realiza de manera incremental mediante intercambios de clave con cada nodo del camino. Una vez establecido el circuito, el origen cifra repetidamente los datos con las claves simétricas establecidas con los miembros del camino, que irán eliminando las capas hasta que el router del extremo finalmente entregue los datos al destino.

En WSNs la transmisión de datos es costosa y, con este modelo, la carga recae especialmente en los nodos fuente, que deben añadir una capa de criptografía por cada nodo del circuito. Además de los requisitos computacionales también se requiere una elevada cantidad de memoria en los sensores. El motivo es que los emisores no sólo necesitan saber las claves de cada onion router sino también la topología de la red para poder aplicar las claves en el orden correcto. Por otra parte, si se opta por la creación incremental del circuito, el nodo debe contactar con cada nodo de la ruta para el intercambio de claves, lo cual supone un aumento en el consumo energético ya que esto implica un mayor trasiego de mensajes.

Los onion routers participan tanto en el establecimiento del circuito como en el reenvío de datos. En ambos casos su labor es eliminar una capa criptográfica de los datos recibidos, que en el primer caso es asimétrica y en el segundo caso es simétrica. Nótese que un mismo nodo podrá formar parte de varios circuitos de manera simultánea. Además, en el diseño original, los onion routers mantienen enlaces cifrados simétricamente con todos sus vecinos para mantener un flujo constante de paquetes de tamaño fijo. Esto pretende que

TABLA I
SOBRECARGA IMPUESTA POR ONION ROUTING

Nodo	Requisitos		
	CPU		RAM
	Circuito	Envío	
Nodos fuente	$N * PK$	$N * SK$	$N * M * P_K + N * S_K$ + *topología*
Onion routers	$1PK$	$1SK + LE$	$P_K + R * L_K + S * S_K$

TABLA II
SOBRECARGA IMPUESTA POR CROWDS

Nodo	Requisitos	
	CPU	RAM
Inicial	$1SK$	$N * S_K$
Intermedio	$2SK + 1RN$	$N * S_K + R * circuitos$
Final	$1SK + 1RN$	$N * S_K$

los paquetes sean indistinguibles entre si, pero supone una sobrecarga importante en una red con recursos limitados.

En la TABLA I se resumen de las imposiciones dadas por las soluciones de onion routing para WSNs. Esta tabla considera tanto el establecimiento ocasional de circuitos como el periodo de envío de datos. Por razones de legibilidad, se obviarán algunas operaciones como el padding y la reordenación de paquetes, que sólo se llevan a cabo en Onion routing. La terminología utilizada en la tabla es la siguiente: N es el número de nodos del circuito, PK y SK se refieren a operaciones de clave pública y simétrica, mientras que P_K y S_K son las respectivas claves. Además, distinguiremos LE y L_K para los enlaces cifrados simétricamente y su clave correspondiente. Por último, R es el número de vecinos con los que un nodo mantiene enlaces y S el número de circuitos que un onion router maneja. Se obviarán también las comunicaciones desde la estación base al nodo fuente, ya que no son relevantes en WSNs para la monitorización de eventos.

Además de los elevados requisitos computacionales existen otros impedimentos para la aplicación de este modelo a WSNs. Los sistemas de onion routing tienen como objetivo evitar que un atacante pueda determinar si dos entidades se están comunicando. Sin embargo, en WSNs, para el atacante es suficiente determinar la localización del destino o de cualquier nodo fuente. Así pues, los puntos más críticos son los nodos de entrada y salida de la red de onion routers. Una vez alcanzado un punto de entrada, el atacante recibirá un flujo continuado de paquetes que le permitirán encontrar al emisor haciendo uso de las estrategias descritas en la Sec. II-B. De manera similar, el problema se repite si el atacante alcanza un nodo de salida. Además, al tratarse de un modelo centralizado en el que emisores y receptores no forman parte del sistema, un atacante global puede fácilmente detectar sus objetivos. Sin embargo, la utilización de capas criptográficas dificulta la tarea a posibles atacantes internos ya que no tienen acceso al contenido ni cabecera de los mensajes.

B. Crowds y Hordes

El modelo Crowds [11] propone un sistema descentralizado en el que los participantes son a la vez potenciales emisores e intermediarios de los mensajes generados por el grupo. Cuando un miembro del grupo recibe un paquete, decide con cierta probabilidad si enviarlo al destino o bien si enviarlo a otro miembro, el cual repetirá el proceso. De esta forma los circuitos dentro del sistema se establecen aleatoriamente, por lo que el receptor de un mensaje no es capaz de determinar suficientemente si el miembro que le envía los datos es el verdadero origen o un mero intermediario. Hordes [12] es una evolución de Crowds cuya principal aportación es el uso de mensajes multicast para la transmisión de las respuestas, por lo que nos centraremos en el modelo original.

La sobrecarga computacional introducida por Crowds es relativamente baja. En particular, las operaciones realizadas por cualquier nodo son: la elección aleatoria del siguiente miembro del camino, el reemplazo del identificador (ID) del emisor de los paquetes recibidos por el propio identificador, y la re-encriptación (descifrado y posterior cifrado) de los paquetes. Adicionalmente, el contenido de los paquetes puede ser cifrado con una clave compartida entre origen y destino para evitar que cualquier nodos intermedio pueda acceder al contenido de los mensajes.

Para realizar la re-encriptación, cada participante debe compartir claves con cada uno de los miembros del sistema. Esto supone un consumo de memoria dependiente del tamaño de la red. Además, los nodos deben almacenar una tabla que les permita relacionar los paquetes recibidos con el circuito o camino al que pertenecen. El tráfico de la red (número simultáneo de circuitos) determinará el tamaño en memoria requerido para almacenar esta tabla.

La TABLA II resume los recursos requeridos por el modelo Crowds. Nótese que un único nodo puede tener varios roles dependiendo de su posición en el circuito: emisor, intermediario y nodo final. Esta tabla se centra en los requisitos particulares de Crowds. No obstante, los requisitos del modelo Hordes son similares. La principal diferencia se encuentra en la forma de enviar las respuestas a los emisores, lo cual no es crucial en el modelo de comunicación (de muchos a uno) considerado en este trabajo. La terminología empleada en esta tabla es la siguiente: SK y S_K representan una operación de clave simétrica y su correspondiente clave; RN se refiere a la operación de renombrado de cabeceras, y por último, N y R se refieren al número de participantes del sistema y al número de caminos activos que mantiene un nodo.

El modelo Crowds impone unos requisitos computacionales asequibles para WSNs. Esto se debe principalmente al modelo de atacante considerado, que no solo es local sino estático, lo que permite la creación de circuitos estáticos, es decir, circuitos que una vez establecidos no serán alterados. La principal ventaja de optar por circuitos estáticos es que reduce el riesgo de tener adversarios internos en el camino. Sin embargo, permite a un atacante móvil hacer un seguimiento de los paquetes, como ocurre con el típico modelo de atacante considerado en WSNs. Por otra parte, el principal objetivo del renombrado de cabeceras es proporcionar anonimato al emisor

frente a cualquier otra entidad, en especial, frente al destino. Esto se convierte en una desventaja en WSNs ya que, para el correcto funcionamiento de la red, la estación base debe conocer el origen de los paquetes. En cualquier caso, este problema podría ser fácilmente solventado añadiendo el ID del nodo origen al payload del mensaje y cifrando los datos extremo a extremo. Por último, a pesar de ser un esquema descentralizado en el que se elimina el problema de los extremos de la red de anonimización, sigue siendo vulnerable a atacantes globales. El motivo es que los nodos generan nuevos caminos tan pronto tienen datos que transmitir a la estación base. Por tanto, un observador que se limite a controlar la frecuencia de envío de los sensores podría distinguir los nodos origen de meros intermediarios.

C. DC-nets y Herbivore

El esquema DC-nets [13] permite a un grupo de participantes compartir información al tiempo que se oculta al emisor real de los datos. Este modelo considera que cada par de miembros comparte un bit secreto de manera que, cada vez que se ejecuta el protocolo, cada miembro realiza la suma modulo 2 (i.e., la O-exclusiva o XOR) de todos sus secretos compartidos. Seguidamente, si uno de los miembros tiene algo que compartir con el resto, entonces hace pública la inversa del resultado obtenido anteriormente; en caso contrario, comunica el resultado[1]. El resultado final se obtiene haciendo nuevamente la XOR de todas las contribuciones. De esta forma, si ningún miembro comparte información, cada bit secreto es usado dos veces y el resultado final debe ser cero. El resultado será uno en caso contrario. Además, como los bits son secretos, es computacionalmente imposible determinar el emisor.

Existen múltiples impedimentos para la aplicación del modelo DC-nets a WSNs. En primer lugar, es un modelo muy sensible a errores y cambios en un único bit dan lugar a resultados irreparables. Por su parte, las WSNs se comunican de manera inalámbrica que resulta ser un medio de escasa fiabilidad y propenso a errores. Además, se requiere una precisa sincronización entre los sensores para permitir que las contribuciones de los participantes sean compartidas correctamente. Sin embargo, esto es difícil de conseguir. Asimismo, los sensores deben estar dentro del radio de transmisión del resto de participantes, entre los que debe encontrarse el destino. Para ello, los nodos deberían aumentar su potencia de transmisión, lo cual limitaría ampliamente la duración de sus baterías, o bien, organizarse jerárquicamente como propone Herbivore [14]. No obstante, aunque el uso de topologías jerárquicas permite reducir la complejidad del sistema y la potencia de transmisión, también introduce nuevos problemas de sincronización así como mayores tiempos en la entrega de paquetes.

[1]Este protocolo puede ser modificado levemente para permitir el envío de cadenas si en lugar de bits se comparten números aleatorios. Esto permite el envío de mensajes cifrados que sólo serán reconocibles por el destino. Aunque nuestro análisis se centra en la versión original, éste puede ser extendido fácilmente para la versión con números aleatorios.

TABLA III
SOBRECARGA IMPUESTA POR DC-NETS

	Requisitos
CPU	$2 * XORs\ (+1 * INV)$
RAM	$[2\ to\ N-1]$ bits
Otros	Topología, sincronización, medio no fiable, simultaneidad

Respecto al consumo de memoria, DC-nets requiere que por cada ejecución del protocolo cada nodo comparta una clave de un bit con cada vecino. Dado que el protocolo debe estar continuamente en ejecución, incluso si ningún participante tiene intención de transmitir, es necesario el almacenamiento de claves de gran longitud o bien la renovación de las mismas mediante funciones pseudo-aleatorias. En cualquier caso, el numero de claves depende de la topología de la DC-net, es decir, del número de vecinos de cada nodo. En el caso más simple, un anillo, cada nodo comparte una clave cada uno de sus dos vecinos. En el caso de una red con N nodos totalmente conectados, cada uno de ellos necesitará $N-1$ bits por cada transacción. La elección de una u otra topología depende de la resistencia del sistema frente a atacantes internos. A mayor número de enlaces mayor robustez.

Existe una limitación adicional que hace de DC-nets un modelo inapropiado para WSNs. DC-nets no soporta la transmisión simultánea de varios participantes, lo cual está en contra de la propia naturaleza de las WSNs ya que su objetivo principal es proporcionar un sistema de monitorización en tiempo real altamente distribuido. Para reducir este problema Herbivore introduce un protocolo para la reserva de slots de transmisión pero éste implica un mayor intercambio de mensajes con el consiguiente aumento del consumo energético. Además, esto no elimina completamente el problema ya que el número simultáneo de transmisiones puede ser muy elevado dependiendo del escenario. Todas las limitaciones se encuentran resumidas en la TABLA III, donde INV representa la inversión de la contribución. Nótese, además, que los valores presentados son para una única ejecución del protocolo, es decir, para la posible transmisión de un único bit de datos.

La sobrecarga computacional impuesta por DC-nets es especialmente reducida incluso para nodos sensores. Sin embargo, los requisitos de memoria, las restricciones topológicas impuestas por el rango de transmisión, y la imposibilidad de realizar múltiples transmisiones simultáneas, imposibilitan su aplicación a WSNs. A pesar de ello, el modelo se ajusta a la perfección a las propiedades requeridas por el problema de la privacidad de localización en WSNs ya que oculta al emisor y receptor frente a observadores externos e incluso frente a otros participantes. Esta característica podría resultar problemática para que la estación base identificase al nodo origen de los datos a menos que se haga uso del protocolo extendido para incluir su ID en el mensaje cifrado. Por último, los atacantes internos, como cualquier otro participante, son incapaces de determinar el emisor a menos que todos los miembros que comparten claves con un nodo colaboren para descubrirlo.

TABLA IV
RESUMEN DE SOLUCIONES PARA WSNS

	Limitaciones	Atacante		
		Global	Local	Interno
Onion routing	↑↑↑	×	×	√
Crowds	↓	×	×	≈
DC-nets	↑↑↑	√	√	√

V. DISCUSIÓN

Las secciones anteriores han profundizado en las características de varios ACS centralizados y descentralizados. En esta sección realizaremos una discusión final acerca de estas soluciones a la vez que destacamos los aspectos más importantes en relación con el escenario de WSNs.

Los sistemas centralizados pueden ser vistos como cajas negras donde los emisores se colocan en un extremo y los destinatarios en otro. Esto deja al descubierto a emisores y receptores frente a observadores globales. Del mismo modo, los observadores locales móviles pueden alcanzar los puntos de entrada o salida del sistema, esperar a la llegada o salida de paquetes y finalmente alcanzar su objetivo siguiendo el camino definido por los paquetes. Por último, los atacantes internos, sólo tienen una visión parcial de las comunicaciones y al ser utilizadas técnicas como el cifrado por capas sólo son capaces de determinar el nodo que inmediatamente lo precede y sucede. Por tanto, los puntos de entrada y salida de un sistema centralizado son especialmente críticos.

Los sistemas descentralizados tratan de prevenir los problemas anteriores haciendo a las partes comunicantes miembros del propio sistema. Es decir, cualquier participante es a la vez un posible emisor e intermediario, lo cual dificulta la tarea de determinar los extremos de la comunicación a posibles observadores. Sin embargo, esto propicia la aparición de sofisticados ataques internos ya que cabe la posibilidad de controlar un elevado número de participantes en el sistema.

En general podemos afirmar que las soluciones descentralizadas son más adecuadas para el problema de la privacidad de localización en WSN dada su naturaleza distribuida y su modelo de comunicación característico. Sin embargo, existen ciertas características en los modelos centralizados que podrían aplicarse en modelos distribuidos para mejorar algunos de sus puntos débiles.

En la TABLA IV ofrecemos un resumen de las soluciones analizadas en este trabajo. Las flechas ofrecen una representación visual de las limitaciones, técnicas y hardware, para la aplicación de estas soluciones a WSNs. Por otra parte, los símbolos $\surd, \times$ y $\approx$ se refieren a la capacidad de estas soluciones para proteger frente a los tres modelos de atacante considerados en WSNs.

VI. CONCLUSIÓN

Este trabajo investiga la adecuación de los sistemas de anonimato tradicionales al problema de la privacidad de localización en WSNs. En trabajos anteriores no se proporciona un análisis adecuado a este problema y se limitan a afirmar, de manera imprecisa, que los sistemas tradicionales son demasiado pesados para dispositivos con recursos tan limitados. Sin embargo, esto no es razón suficiente ya que en el futuro aparecerán sensores con capacidades muy superiores. Por ello, este trabajo proporciona un análisis riguroso que tiene en cuenta los pormenores del nuevo problema así como las particularidades de los escenarios de WSNs. Con todo esto hemos demostrado que las afirmaciones anteriores no era completamente ciertas. En particular, nuestro análisis establece que algunas soluciones tradicionales son lo suficientemente livianas para funcionar en sensores pero no se ajustan a los requisitos y atacantes específicos del nuevo dominio. Por el contrario, otras soluciones que si se adecuan al problema, resultan demasiado costosas y/o limitan la funcionalidad de la red. Nuestros planes de futuro incluyen abordar nuevas soluciones de anonimato y profundizar este estudio con nodos reales a fin de determinar la carga real de trabajo que son capaces de soportar. Asimismo, planeamos desarrollar soluciones de anonimato especialmente diseñadas para WSNs.

Agradecimientos: Este trabajo ha sido parcialmente financiado por la Comisión Europea y el Ministerio de Innovación y Ciencia mediante: NESSoS (FP7 256890), ARES (CSD2007-00004) y SPRINT (TIN2009-09237). SPRINT está cofinanciado por FEDER y el primer autor por el programa FPU del Ministerio de Educación.

REFERENCIAS

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292 – 2330, 2008.

[2] J. Walters, Z. Liang, W. Shi, and V. Chaudhary, *Security in Distributed, Grid, and Pervasive Computing*. Auerbach Pub, 2007, ch. Wireless Sensor Network Security: A Survey.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-Location Privacy in Energy-Constrained Sensor Network Routing," in *SASN '04: 2nd ACM workshop on Security of ad hoc and sensor networks*, Washington, DC, USA, 2004, pp. 88–93.

[4] K. Mehta, D. Liu, and M. Wright, "Location Privacy in Sensor Networks Against a Global Eavesdropper," in *ICNP'07: IEEE International Conference on Network Protocols*, Beijing, China, 2007, pp. 314–323.

[5] H. Wang, B. Sheng, and Q. Li, "Privacy-aware routing in sensor networks," *Comput. Netw.*, vol. 53, no. 9, pp. 1512–1529, 2009.

[6] S. Pai, S. Bermudez, S. Wicker, M. Meingast, T. Roosta, S. Sastry, and D. Mulligan, "Transactional Confidentiality in Sensor Networks," *IEEE Security & Privacy*, vol. 6, no. 4, pp. 28–35, July-Aug. 2008.

[7] J. Kang, "Information privacy in cyberspace transactions," *Stanford Law Review*, vol. 50, no. 4, pp. 1193–1294, 1998.

[8] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010, [Online] http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[9] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, May 1998.

[10] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," in *SSYM'04: 13th conference on USENIX Security Symposium*, San Diego, USA, 2004, pp. 21–21.

[11] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions," *ACM transactions on information and system security*, vol. 1, no. 1, pp. 66–92, 1998.

[12] B. N. Levine and C. Shields, "Hordes: A Multicast Based Protocol for Anonymity," *J. Comput. Secur.*, vol. 10, no. 3, pp. 213–240, 2002.

[13] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, vol. 1, pp. 65–75, 1988.

[14] S. Goel, M. Robson, M. Polte, and E. G. Sirer, "Herbivore: A Scalable and Efficient Protocol for Anonymous Communication," Cornell University, Ithaca, NY, Tech. Rep. 2003-1890, February 2003.