J. A. Onieva, R. Rios, and B. Palenciano, "Análisis y Desarrollo de un Canal Encubierto en una Red de Sensores", *XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI 2014)*, pp. 333-338, 2014.
NICS Lab. Publications: https://www.nics.uma.es/publications

Análisis y Desarrollo de un Canal Encubierto en una Red de Sensores

Jose A. Onieva
Dpto. de Lenguajes y Ciencias de la Computación
Universidad de Málaga
Email: onieva@lcc.uma.es

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

Bernardo Palenciano
Email: berni.sira@gmail.com

***Resumen*—Continuamente aparecen nuevos estudios así como nuevos desarrollos de canales encubiertos. Como veremos, existen más de cien diseños distintos para redes de ordenadores, pero no hemos encontrado en la literatura ningún análisis, diseño e implementación de canales encubiertos sobre redes de sensores. En este artículo presentamos los resultados del diseño e implementación de un canal multitasa basado en los tiempos de monitorización sobre una red de sensores. En este proceso se han establecido las principales propiedades necesarias y, en base a ellas, se desarrolla e implementa el canal encubierto. Se describe el proceso de desarrollo y se analiza su detectabilidad.**

***Palabras clave*—Canales encubiertos (covert channels), Detección de intrusos (Intrusion detection), Information Warfare, Redes de sensores (sensor networks), Seguridad de la Información (Information Security), Seguridad en redes (Network Security).**

I. Introducción

La noción de canal encubierto surgió hace varias décadas en el contexto de los sistemas de seguridad multinivel [1], donde procesos con distintos niveles de seguridad no deberían comunicarse entre sí. De esta forma, los canales encubiertos pueden definirse como "cualquier canal de comunicación que puede ser aprovechado por un proceso para transferir información de manera que viola la política de seguridad del sistema" [2]. Siendo una propiedad fundamental de estos canales que su presencia pase inadvertida ante un posible observador.

Si bien los canales encubiertos nacen en el contexto de los sistemas de seguridad multinivel, el ámbito de estudio fue evolucionando a medida que los sistemas se conectaban entre sí, dando origen a canales encubiertos en redes de comunicación [3]. No obstante, hasta donde alcanza nuestro conocimiento, no existen diseños en *redes de sensores*.

Quizás el estudio más próximo a nuestro trabajo se encuentre en [4], donde los autores presentan un análisis y diseño de canales encubiertos en protocolos de enrutamiento dinámico para redes ad-hoc. En efecto, las redes de sensores pueden ser consideradas como un tipo de red ad-hoc, pero presentan además un gran número de características específicas que obligan a focalizar el análisis y diseño de este tipo de canales sobre ellas. Más aún cuando las redes de sensores están siendo cada vez más utilizadas para la monitorización y control de individuos, ambientes y recursos en multitud de escenarios, tanto militares como civiles.

En este trabajo comenzamos ofreciendo una visión general de las características y particularidades tanto de los canales encubiertos como de las redes de sensores (sección II). Seguidamente, en la sección III analizamos los requisitos necesarios que debería ofrecer un canal encubierto basado en redes de sensores a partir de un escenario ficticio. Asimismo, presentamos el diseño de un canal encubierto multitasa que se ajusta a los requisitos establecidos anteriormente. En la sección IV demostramos la viabilidad del diseño a partir de una prueba de concepto sobre una red de sensores. A continuación se presenta un analisis de la detectabilidad del canal (sección V). Por último, se presentan las conclusiones y posibles líneas de trabajo futuro.

II. Preliminares

II-A. Canales Encubiertos

Los canales encubiertos pertenecen al campo de la ocultación de la información. A diferencia de la criptografía, que se preocupa de mantener desconocido el significado de la información, esta disciplina tiene como objetivo evitar el descubrimiento de la información en sí.

Para entender mejor el concepto de canal encubierto se suele acudir al problema de los prisioneros (*prisioners' problem* [5]): Alice y Bob se encuentran en prisión y están intentando desarrollar un plan para escapar. Se les permite comunicarse a condición de que Walter, el guardián, pueda inspeccionar todas las notas que se intercambian. En el caso de que Walter detectara algún indicio de que Alice y Bob están planeando fugarse, éste no les permitiría seguir comunicándose. Así pues, podemos ver que los canales encubiertos facilitan un medio de comunicación que pase inadvertido a los ojos de un posible examinador del contenido o del formato en el que se realiza una comunicación aparentemente normal.

Existen numerosos estudios que aglutinan y clasifican los distintos tipos de canales en base a diversos criterios [6], [7]. Sin embargo, la clasificación más utilizada, y que adoptamos en este artículo, se fundamenta en las técnicas de ocultación utilizadas:

- Canales de almacenamiento (*Storage Channels*): son aquellos que permiten que un proceso escriba en una zona de memoria para que otro proceso recupere tal información mediante la lectura de tal zona.

ISBN: xxx-xx-xxxx-xxx-x

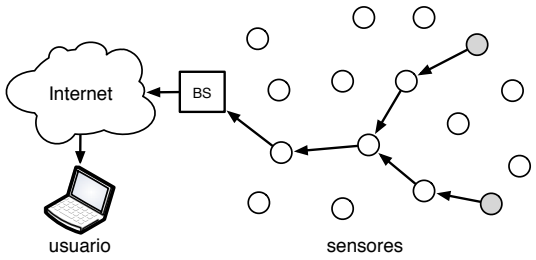


Figura 1. Red de sensores

- Canales de temporización (*Timing Channels*): en estos canales un proceso codifica información mediante la modulación de su propio comportamiento de manera que otro proceso al observar estos cambios es capaz de recuperar la información señalizada.

Si bien esta clasificación es muy general y está orientada a procesos, es igualmente válida para canales encubiertos en redes de comunicación, teniendo en cuenta que las zonas de memoria referidas en los canales de almacenamiento se corresponden a determinados campos de los paquetes de red y la modulación del comportamiento en los canales de temporización puede hacerse evidente cambiando la tasa de envío de paquetes.

II-B. Redes de Sensores

Una red de sensores [8] es un sistema distribuido formado por un gran número de dispositivos de capacidad y tamaño reducido (denominados *nodos* o *motas*) cuyo objetivo es monitorizar un determinado fenómeno físico gracias a los sensores que incorporan. Una vez detectada información de relevancia, ésta es transmitida de manera inalámbrica hasta un dispositivo (conocido como estación base o *sink*) que se encarga de procesarla y ofrecerla a los usuarios de la red, como se muestra en la Figura 1.

Dado que la estación base es la encargada de obtener toda la información de los sensores, el modelo de comunicación más habitual es de muchos a uno, donde caben dos opciones dependiendo del número de sensores desplegados y el rango de transmisión de estos. En el modelo de un *único salto* todos los nodos de la red transmiten directamente a la estación base sin necesidad de realizar enrutamiento. Es más simple, pero sólo es posible cuando el número de nodos y el área de despliegue es reducida. En el modelo *multisalto*, los nodos que se encuentran alejados utilizan a sus vecinos para hacer llegar sus datos a la estación base. Normalmente utilizando el camino más corto o protocolos de inundación.

Por otro lado, existen diferentes modos de funcionamiento o de notificación de eventos. Por lo general, suelen distinguirse las tres alternativas [9]. En la monitorización *continua* los nodos envían información sobre el entorno de manera periódica, mientras que en el modelo de monitorización *basado en eventos* se transmite información únicamente cuando un parámetro alcanza un valor excepcional (i.e., ocurre un evento). Además, existe un modo de monitorización *basado en consultas* en el que los nodos responden a las consultas realizadas por los usuarios de la red.

La versatilidad de estas redes y su reducido tamaño hace de ellas una solución ideal para multitud de aplicaciones de monitorización y control, donde los dispositivos se integran discretamente en el entorno. De hecho, este tipo de redes ya ha sido aplicada con éxito en multitud de escenarios [10], lo que las convierte en sistemas cada vez más aceptados.

Al mismo tiempo, esto puede suponer un mayor interés por explotar este tipo de redes con fines maliciosos. Se hace necesario por tanto un minucioso estudio sobre la viabilidad de desarrollar canales encubiertos en redes de sensores, pues su utilización repercutiría negativamente en la seguridad y privacidad de los entornos donde se desplieguen estos sistemas.

III. Estudio y Análisis

III-A. Escenario

Para la creación de un canal de comunicación oculto, en primer lugar, es necesario plantearse su aplicabilidad, y para ello lo más indicado es idear un escenario de uso ficticio en el que podría ser utilizado.

Supongamos una empresa dedicada al cultivo y venta de mejillones en el Estrecho de Gibraltar. La empresa hace uso de una red de sensores en la zona con el objeto de monitorizar las condiciones del medio marino y conseguir así un mejor producto. Sin embargo, ésta no es la única actividad desarrollada por la compañía. Aprovecha su situación privilegiada para llevar a cabo un transporte ilegal de sustancias en contenedores.

Supongamos además que Alice y Bob son agentes de la Guardia Civil que sospechan de las actividades ilegales desarrolladas por la empresa citada anteriormente. Con el fin de destapar el tráfico de sustancias, Alice se infiltra en la compañía y necesita informar a Bob del contenedor donde se transportan las sustancias ilegales para que pueda atraparlos en el acto. Alice, que teme por su integridad física si fuese descubierta informando de esta actividad, decide idear un mecanismo de comunicación oculta utilizando la red de sensores. Sin embargo, por cuestiones geográficas, Bob sólo tiene acceso a un número limitado de sensores.

Nuestro canal oculto de comunicación debería ser de utilidad para que Alice pueda informar a Bob del contenedor en el que se encuentran las sustancias ilegales sin ser delatada.

III-B. Requisitos del canal

A continuación analizamos los requisitos que serían deseables para el tipo de canal encubierto que necesitarían Alice y Bob a fin de alcanzar su objetivo en el escenario propuesto.

- Grado de detectabilidad. El canal de comunicación oculto debe ser difícilmente detectable. Esta característica se ve facilitada por el hecho de ser las redes de sensores un campo bastante inexplorado en la búsqueda de este tipo de canales[1].

[1]Como hemos indicado previamente, en este trabajo presentamos el primer canal encubierto para redes de sensores.

- Ancho de banda moderado. La capacidad del canal no se considera un factor esencial ya que la intención es el envío de pequeñas cantidades de información, como por ejemplo, la referencia de un contenedor.
- Integridad. Debido a que la información enviada es sensible, es necesario que ésta sea recibida correctamente.
- Sentido de la comunicación. Basta con crear un canal unidireccional, pues el propósito no es realizar un intercambio de datos sino, simplemente, comunicar información desde un punto a otro.

Estas particularidades determinarán el ámbito de aplicabilidad del canal, y a su vez éste puede condicionar la decisión del tipo de canal a implementar.

III-C. Configuración de la red

El escenario de aplicación determina el modo de funcionamiento y configuración de la red, y esto, a su vez, influye en el tipo de canal encubierto que es más conveniente desarrollar dado los requisitos establecidos anteriormente.

Debido a que el objetivo de nuestra red de sensores es la de tomar valores de diferentes parámetros del agua cada cierto intervalo de tiempo, el modo de funcionamiento más conveniente es el de monitorización continua.

Por otra parte, dado que los sensores se encontrarán desplegados en un área extensa se hace imposible el uso de un modelo en un único salto, ya que el rango de transmisión de estos haría imposible que se comunicaran directamente con la estación base. Así, el modelo de enrutamiento multisalto es el más adecuado para nuestro escenario.

En cuanto al sistema operativo de la red de sensores, cabe destacar Contiki [11] y TinyOS [12]. En este trabajo nos hemos decantado por Contiki debido a las bondades de su simulador.

III-D. Diseño de un canal multitasa

Debido a que el cambio en la frecuencia de monitorización de los sensores es normal para atender a las distintas circunstancias que se producen en el medio, a los requisitos de consumo de energía y a las necesidades de procesamiento de la estación base, utilizar estos cambios para la implementación de un canal encubierto parece prometedor.

Al diseñar un canal de temporización podemos optar por una canal *binario*, tal y como se hiciera en [13], o podemos inclinarnos por un canal *multitasa*. En un canal binario, cada cierto intervalo de tiempo, el emisor puede enviar un paquete o mantenerse en silencio. El receptor monitoriza cada intervalo de tiempo para determinar si un paquete fue recibido o no. El resultado es un código binario donde un 1 representa la detección de un paquete en el intervalo y un 0 representa la ausencia del mismo. En un canal multitasa, emisor y receptor acuerdan dos conjuntos (intervalos de tiempo, carácter) y la correspondencia entre ellos. Así, cada intervalo de tiempo distinto corresponderá a un único carácter (ver Figura 2). Pueden producirse errores de decodificación si los tiempos de los distintos intervalos son muy parecidos. Es decir, en este último caso haría falta una sincronización muy fiable, o la integridad exigida al canal sería difícil de conseguir.

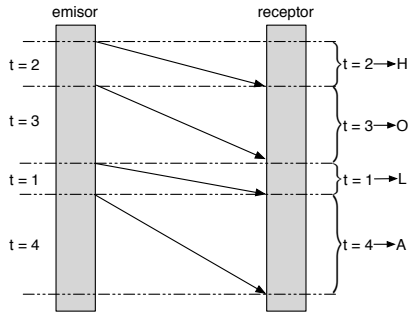
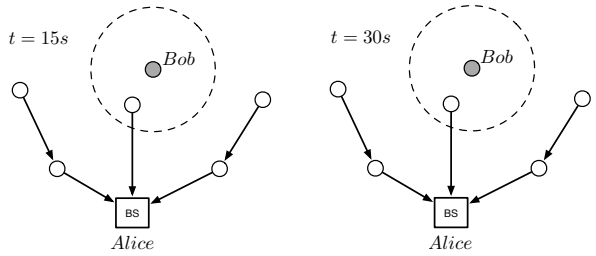


Figura 2. Codificación y sincronización



(a) Estado inicial (canal sin actividad) (b) Cambia el intervalo (canal activo)

Figura 3. Funcionamiento del canal multitasa

Para desarrollar un canal multitasa en nuestra red de sensores, puesto que su funcionamiento es en modo monitorización continua y se envían paquetes de forma periódica siguiendo un tiempo preestablecido *t*, se tiene que cambiar el tiempo de monitorización según sea necesario. En nuestro escenario, Bob observa constantemente los mensaje enviados en la red de sensores. Mientras la estación base no envíe información oculta, los nodos estarán configurados para enviar mensajes cada intervalo *t*. En otro caso, la estación base comunicará a los nodos la supuesta intención de reconfigurar los tiempos de monitorización con la excusa de cambiar la estrategia de toma de datos. Los nodos no volverán a comunicarse con la estación base hasta pasado el tiempo ordenado, como se muestra en la Figura 3, donde inicialmente los nodos transmiten cada $15s$ y más tarde se cambia el intervalo de notificación a $30s$. De esta forma, Bob podrá interpretar los distintos cambios en el intervalo de monitorización y finalmente obtendrá su mensaje.

A pesar de que hemos investigado otras posibilidades de ocultación, teniendo también en cuenta la posibilidad de desarrollar canales de almacenamiento, estos últimos suponen cambios que podrían degradar el uso de la red de sensores (e.g. por cambios en los parámetros de enrutamiento) y la vida útil de la misma, además de ser susceptibles a varias técnicas de detección. Si bien para los canales de temporización desarrollados hasta ahora en redes de datos convencionales también se han desarrollado técnicas de detección basadas en la regularidad del envío de los paquetes de datos [14], éstas no son aplicables a las redes de sensores que, por diseño, en el caso de redes de monitorización continua, ya

Tabla I
CODIFICACIÓN DE CARACTERES

Carácter	Tiempo	···	Carácter	Tiempo
FINAL	15	···	f	130
cambio	20	···	z	135
e	25	···	j	140
a	30	···	x	145
(espacio)	35	···	w	150
o	40	···	k	155
s	45	···	···	···

presentan patrones de envío regulares. En cualquier caso, la detectabilidad del canal diseñado se tratará más detenidamente en la sección V.

IV. DESARROLLO DE UN CANAL MULTITASA

El desarrollo de un canal encubierto multitasa requiere establecer una tabla de equivalencias entre intervalos y caracteres. Asimismo, es necesario calcular previamente un intervalo de funcionamiento normal de la red. Este tiempo vendrá determinado por el tipo de aplicación y en nuestro caso lo fijaremos en $t = 15$ segundos, en un intento de alcanzar un balance entre la actualidad de los datos y el tiempo de vida de las motas[2].

Tras realizar pruebas de precisión con el simulador de Contiki (más tarde confirmadas sobre la implementación que hemos realizado con motas Tmote Sky de Moteiv) un nodo que haga las funciones de *sniffer*[3] para Bob tiene un error de precisión de $1 \sim 2$ segs en el cálculo del intervalo de envío de paquetes. Por ello, y para asegurar el requisito de integridad (en contra del ancho de banda) hemos seleccionado un incremento de 5 segundos en los intervalos que diferencian a los distintos caracteres, como puede apreciarse en la tabla I.

En dicha tabla se ha utilizado un conjunto de caracteres reducido del castellano y se ha aplicado una codificación de Huffman [16] según la frecuencia de aparición de estos con el fin de reducir el retraso de las comunicaciones, aumentando así el ancho de banda efectivo del canal. Además, como puede verse, cuando el intervalo de envío de datos por parte de las motas vuelve al original (i.e. 15 segundos), se produce el final del mensaje enviado.

Para implementar el sniffer en el simulador de Contiki es necesario que los nodos de la red se comuniquen en modo broadcast y que sea a nivel de aplicación donde se decida si un paquete está dirigido a un nodo u otro. Es decir, el identificador del nodo destino va incluido en la carga útil de datos o payload de los paquetes pero sólo el autentico destinatario lo procesa cuando observa su identificador. Así, el nodo que hace las funciones de sniffer puede observar y procesar todos los paquetes, aunque no estén dirigidos hacia él a nivel de aplicación.

En nuestro diseño final decidimos utilizar repeticiones con el fin de aumentar la integridad del canal. Por ejemplo, sabiéndose que el intervalo de transmisión de la letra 'a' es de 30 segundos, podemos estar seguros de que pasados 90 segundos desde que la estación base mandó la orden de monitorizar cada 30 segundos, se habrá transmitido tres veces el carácter 'a'. Y este tiempo de 90 segundos (tiempo del carácter $\times$ 3) será diferente para otro carácter. El motivo de enviar tres veces cada carácter es intentar reducir a cero el porcentaje de errores. Y es que en la implementación del canal nos hemos encontrado con un feroz enemigo: las colisiones.

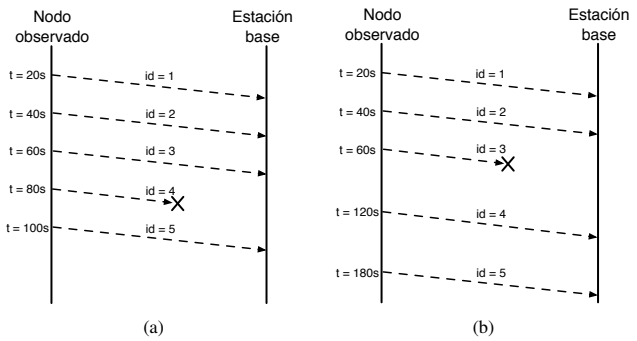


Figura 4. Diferentes circunstancias de colisiones

Debido a que el medio de transmisión inalámbrico es compartido, si un sensor recibe simultáneamente dos mensajes, ambos colisionan y por lo tanto ambos mensajes se vuelven incomprensibles. Esto puede llevar a confusiones por parte del sniffer a la hora de medir los tiempos transcurridos.

Las colisiones pueden afectar al nodo observado por Bob tanto durante el envío como durante la recepción de paquetes. Tras múltiples tests en nuestro escenario de pruebas (similar al de la Figura 3) se constata que las colisiones de los paquetes recibidos en este nodo suponen un 5 % del total de las colisiones. Sin embargo, las que más nos interesan, y que suponen un 95 % del total de las colisiones, son las que afectan a los paquetes que envía el nodo. A fin de detectarlas, los paquetes han de contar con un identificador en la cabecera para que el sniffer pueda compararlo con el identificador de paquetes consecutivos. Si el sniffer recibe el paquete con identificador 3 y a continuación recibe el paquete con identificador 5, calcula que entre ambas recepciones se perdió un paquete.

Las pérdidas de paquetes individuales pueden darse en dos circunstancias diferentes:

1. Se pierde un paquete durante un intervalo de tiempo en el que la tasa de envío se mantiene inalterada.
2. Se pierde el primer paquete que cambiaba el intervalo de tiempo respecto a su predecesor.

En la Figura 4 se observan las dos circunstancias posibles en un escenario en el que suponemos inicialmente $t = 20$ segundos y un cambio posterior a $t = 60$ segundos. En la primera se ve como el nodo espiado envía cuatro paquetes a la estación base, los tres primeros cada 20 segundos y un último paquete 40 segundos después del tercero. El nodo sniffer detecta la colisión del cuarto paquete, por lo que sabe que entre el instante 60 segundos y el instante 100 segundos

[2]La tendencia actual es incorporar células solares para alargar su vida útil (e.g. ECS310 de enocean®).

[3]En el mercado existen varias soluciones que permiten esta funcionalidad, como es el caso de Jackdaw [15]

se ha perdido un paquete. Tenemos que el tiempo transcurrido entre el envío del paquete tres y el envío del paquete cinco es 40 segundos. Si se supone, como es el caso, que el paquete que se ha perdido fue enviado transcurrido el mismo intervalo que el último recibido, sólo tenemos que coger los 40 segundos y dividirlos por 2, obteniendo que el intervalo transcurrido entre el paquete colisionado y el quinto paquete es de 20 segundos.

Para la segunda circunstancia, si utilizáramos la misma solución se obtendría que el tiempo transcurrido entre el paquete colisionado, el número tres, y el paquete cuatro es de 40 segundos, por lo que obtendríamos un tiempo erróneo. Esta circunstancia se soluciona almacenando en cada captura de tráfico el intervalo del último envío y restándoselo al tiempo transcurrido entre las dos últimas transmisiones con éxito. En este caso, con la captura del paquete número dos almacenaríamos el intervalo 20 segundos, al recibir el cuarto paquete transcurridos 80 segundos detectaríamos la colisión y a estos 80 segundos le restaríamos el intervalo almacenado anteriormente de 20 segundos, obteniendo el resultado de 60 segundos.

Aunque se sabe como solucionar ambos casos, el gran problema es que resulta imposible saber durante la ejecución en que circunstancia nos encontramos. Por ello, optando por alguna de las dos soluciones conseguiremos reducir el número de errores aunque no por completo. Además, este esquema podría requerir un pequeño cambio en el código de la aplicación de las motas de forma que se puedan numerar los paquetes (si el propio protocolo de envío de paquetes de la aplicación de las motas no lo hace por defecto). Si bien, el cambio es mínimo, como veremos en la sección V, de producirse, éste aumentaría la detectabilidad del canal por parte de agentes locales.

Dado que el requisito de integridad de los datos es esencial en nuestro escenario, en una segunda implementación del canal encubierto hemos debido corregir las colisiones mediante la replica de intervalos (y el control de estas repeticiones para mantener la integridad del mensaje decodificado), reduciendo así, desafortunadamente, el ancho de banda de manera drástica. No obstante, como habiamos extraido en III-B, se trata del requisito menos estricto de todos.

Tras multiples simulaciones, en esta segunda implementación hemos logrado un ancho de banda de $1/230$ caracter/seg. Esto significa que para comunicar en nuestro escenario el identificador de referencia de un contenedor de 10 caracteres, por ejemplo; Alice necesitaría unos 38 minutos[4]. La tasa de error detectada inherente al escenario y el funcionamiento que realiza es del 4 %.

V. Estudio de detectabilidad

Debido a la naturaleza inalámbrica de las redes de sensores, un atacante podría escuchar las transmisiones e incluso inyectar tráfico en la red; especialmente si la red está desplegada en un entorno hostil. Por ello, la seguridad en redes de sensores se centra en proteger cuatro aspectos: confidencialidad, integridad, disponibilidad y la vida de la batería. Dado que nuestro canal no afecta a ninguno de estos servicios, eludiría la mayoría de las soluciones de seguridad actuales.

Como ya se ha comentado con anterioridad, las redes de sensores son un tipo de red ad-hoc inalámbricas cuyas diferencias hacen inviable la aplicación de IDSs (*Intrusion Detection Systems*) desarrollados para redes ad-hoc. Para empezar, la capacidad de los nodos impide instalar un agente de detección completo. Por ello, se usan soluciones parciales como:

- Analizar las fluctuaciones en las lecturas de los sensores
- Analizar la integridad del código
- Vigilar la información intercambiada entre los sensores

Ante un IDS dedicado al análisis de las lecturas de los sensores, nuestro canal encubierto pasaría totalmente desapercibido puesto que no altera dichos valores. De igual forma, la vigilancia de la información intercambiada entre los sensores no pondría de manifiesto el canal encubierto puesto que no se modifica ninguno de los campos de los paquetes. A su vez, un exhaustivo estudio del código que forma el programa de las motas tampoco supondría un problema, ya que la única funcionalidad sospechosa (los envíos de cambios de tiempo de monitorización) se realizarían desde la estación base y sin necesidad de modificar su código.

En [17] se propone una solución de IDS específico para redes de sensores. Esta solución considera dos tipos de agentes: locales y globales. Los agentes locales monitorizan tanto las operaciones realizadas como la información enviada y recibida por el nodo. Por tanto, los agentes locales detectarían los ataques que afecten la integridad física o lógica de la mota así como el intento de influenciar en la recogida de datos por parte de entidades no autorizadas.

Por otro lado, los agentes globales vigilan las interacciones con sus vecinos inmediatos, comportándose a modo de guardián que analiza y procesa el contenido paquetes. Estos agentes serían capaces de detectar si un nodo está borrando o modificando algún campo de los paquetes intercambiados por las motas antes de retransmitirlo. En el caso de detectar alguna amenaza de seguridad, el agente generaría información de alerta y la enviaría a la estación base.

Dado que nuestro canal no modifica el estado de los nodos ni la información contenida en los paquetes de manera arbitraria, los agentes descritos no serían capaces de detectarlo. Sí podrían levantar ciertas sospechas los continuos mensajes de actualización de la tasa de transferencia por parte de la estación base. Aunque la estación base es un nodo autorizado, y, además, su comportamiento entraría dentro del uso normal de la red. No obstante, continuos cambios en estos tiempos (si queremos enviar un mensaje oculto con 10 caracteres, se cambiarían los tiempos de monitorización 20 veces en un intervalo de tiempo relativamente corto, ya que utilizamos también un carácter de *cambio* por cada cambio de caracter), si el mensaje enviado en el canal encubierto es muy largo, podrían levantar sospechas en el caso de que se produzca un análisis detallado de esta frecuencia.

Una posible solución ante este problema sería utilizar varias motas para enviar los datos ocultos. De esta forma, cada uno

[4]La adecuación del tiempo necesario para transmitir un mensaje será relativo al objetivo que se persigue en la comunicación oculta.

de los nodos no recibiría un volumen notorio de notificaciones de cambio de intervalo, y los agentes locales de estos nodos no verían como una situación anómala el recibir un número dado de notificaciones, que se vería reducido en función del número de motas utilizadas.

Para que esta solución tuviese sentido es necesario que el sniffer pueda monitorizar varios nodos de manera simultánea, ya sea porque la ganancia de su antena se lo permite o porque tiene varias antenas en distintas ubicaciones. Asimismo, sería necesario establecer una secuencia predefinida de motas a observar por parte de Bob, por lo que la implementación y sincronización del canal se hace más compleja. Nótese que en este último caso se abren nuevas vías de ocultación. Se podría investigar, por ejemplo, desarrollar un canal encubierto de conteo (i.e., se codifican los caracteres en función del número de nodos que envíen en un intervalo) o bien un canal de ordenación (i.e., el orden de envío indica la información).

El empleo de técnicas de detección dependerá siempre de las características de la aplicación y del escenario concreto sobre el que dicha aplicación se ejecuta. Dada la sobrecarga que pueden introducir estos mecanismos, en términos de transmisión sobre el medio inalámbrico y de procesamiento y almacenamiento en los nodos, su uso puede resultar justificable únicamente en aplicaciones con fuertes requisitos de seguridad y en las que los dispositivos involucrados dispongan de la suficiente capacidad y autonomía como para que la ejecución de un sistema de detección no imponga una limitación intolerable sobre las prestaciones ofrecidas al usuario final.

Así pues, se puede concluir que nuestro canal de comunicación oculto es lo suficientemente difícil de detectar como para pasar desapercibido ante sistemas de detección usuales. No obstante, agentes locales que llevaran a cabo un análisis en la estadística de los cambios de frecuencia en los mensajes de monotorización de las motas podrían elevar las alertas necesarias para comenzar a investigar la existencia de dicho canal.

VI. Conclusiones

En este artículo hemos diseñado una canal encubierto sobre una red de sensores con un ancho de banda muy limitado pero, hasta donde alcanza nuestro conocimiento, es el primer intento de análisis, diseño e implementación de este tipo de canales en este entorno.

Para ello hemos ideado un escenario ficticio y extraído los requisitos principales del canal. A partir de estos se ha desarrollado un canal de temporización multitasa y se ha llevado a cabo un estudio sobre la detectabilidad de este tipo de comunicaciones en redes de sensores. Si bien el ancho de banda del canal es mejorable, hemos preferido, acorde con los requisitos extraídos, primar la integridad de los datos enviados.

Asimismo hemos encontrado nuevas vías de ocultación que estamos analizando en la actualidad. En concreto, se tratan de canales de almacenamiento y modificación del enrutamiento; por lo que habrá que analizar detenidamente sus implicaciones a nivel de detectabilidad y de funcionamiento de la red. Más específicamente, tres son los candidatos (que presentan sus desventajas y ventajas asociadas): canal encubierto sobre uIP, utilización de los campos de protocolos de enrutamiento (RSSI y LQI), y modificación de las rutas seguidas por los paquetes.

También resulta de interés indicar que se ha llevado a cabo la implementación del canal propuesto como prueba de concepto sobre el simulador de Contiki y evaluado su funcionamiento desplegándolo sobre un número muy reducido de motas físicas. Se hace por tanto necesario llevar a cabo un despliegue sobre una red de sensores real con objeto de hacer mediciones más fiables.

Agradecimientos

Este trabajo ha sido sido financiado parcialmente por el Ministerio de Ciencia e Innovación y de la Junta de Andalucía a través de los proyectos ARES (CSD2007-00004) y FISICCO (P11-TIC-07223), respectivamente.

Referencias

[1] B. W. Lampson, "A Note on the Confinement Problem," *Commun. ACM*, vol. 16, no. 10, pp. 613–615, 1973.

[2] S. L. Brand, "Department of Defense Trusted Computer System Evaluation Criteria - The Orange Book," U.S. Department of Defense, Tech. Rep. DoD 5200.28-STD, 1985. [Online]. Available: http://csrc.nist.gov/publications/history/dod85.pdf

[3] Center for Advanced Internet Architectures, "Covert Channels in Computer Network Protocols Bibliography," March 2014. [Online]. Available: http://caia.swin.edu.au/cv/szander/cc/cc-cnetworks-bib.html

[4] S. Li and A. Ephremides, "Covert channels in ad-hoc wireless networks," *Ad Hoc Networks*, vol. 8, no. 2, pp. 135 – 147, 2010.

[5] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," in *Advances in Cryptology: Proceedings of CRYPTO*, ser. LNCS, D. Chaum, Ed. Santa Barbara, California, USA: Plenum Press, August 21-24 1983, pp. 51–67.

[6] C. Meadows and I. S. Moskowitz, "Covert Channels – A Context-Based View," in *Proceedings of the First International Workshop on Information Hiding*. London, UK: Springer-Verlag, 1996, pp. 73–93.

[7] J. Shen, S. Qing, Q. Shen, and L. Li, "Optimization of Covert Channel Identification," in *SISW '05: Proceedings of the Third IEEE International Security in Storage Workshop*. Los Alamitos, CA, USA: IEEE Computer Society, 2005, pp. 95–108.

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

[9] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6 – 28, dec. 2004.

[10] L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman, and M. Yarvis, "Design and deployment of industrial sensor networks: Experiences from a semiconductor plant and the north sea," in *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, ser. SenSys '05. New York, NY, USA: ACM, 2005, pp. 64–75. [Online]. Available: http://doi.acm.org/10.1145/1098918.1098926

[11] "Contiki: The open source os for the internet of things." [Online]. Available: http://www.contiki-os.org/

[12] "Tinyos official website." [Online]. Available: http://www.tinyos.net/

[13] S. C. Cabuk S., Brodley C.E., "Ip covert timing channels: Design and detection," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*. ACM Press, 2004.

[14] S. Cabuk, C. E. Brodley, and C. Shields, "Ip covert channel detection," *ACM Trans. Inf. Syst. Secur.*, vol. 12, pp. 22:1–22:29, April 2009.

[15] "Rzraven usb stick (jackdaw)." [Online]. Available: http://www.ibr.cs.tu-bs.de/projects/mudtn/doxygen/a01892.html

[16] D. Huffman, "A method for the construction of minimum-redundancy codes," in *Proceedings of the I.R.E.*, editor, Ed., pp. 1098–1102.

[17] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in *IEEE Consumer Communications & Networking Conference (CCNC 2006)*, IEEE. Las Vegas (USA): IEEE, January 2006, pp. 640–644.