Protocolo para la Notificación y Alerta de Eventos de Seguridad en Redes Ad-hoc

Leovigildo Sánchez-Casado, Roberto Magán-Carrión, Pablo Garrido-Sánchez, Pedro García-Teodoro
Departamento de Teoría de la Señal, Telemática y Comunicaciones
Universidad de Granada - CITIC
Email: sancale@ugr.es, rmagan@ugr.es, pablogs9@correo.ugr.es, pgteodor@ugr.es

***Resumen*—Las líneas de defensa de seguridad tradicionales para proteger un sistema dado son prevención, detección y respuesta. A pesar de que sobre el papel dichos módulos deben inter-operar a fin de conseguir una seguridad integral, por lo general se plantean y adoptan como soluciones independientes. El presente trabajo aborda el estudio y desarrollo de un protocolo de notificación y alerta de eventos de seguridad cuyo fin principal es servir de interfaz entre los módulos de detección y respuesta.**

Ideado específicamente para redes ad-hoc, su uso posibilita poner en conocimiento de los elementos constitutivos del entorno monitorizado la ocurrencia de un cierto comportamiento malicioso detectado. Este conocimiento será clave para la ejecución posterior de los mecanismos de respuesta oportunos.

También susceptible de ser usada para la distribución de información en procesos de detección/respuesta colaborativos, nuestra propuesta viene a cubrir una carencia manifiesta en el campo objeto de estudio.

***Palabras clave*—seguridad en redes (*network security*), redes ad-hoc (*ad-hoc networks*), intrusión (*intrusion*), detección (*detection*), respuesta (*response*), notificación y alerta (*notification and alert*)**

I. Introducción

Las redes ad-hoc constituyen en la actualidad un paradigma de comunicaciones de uso creciente. La ausencia de infraestructura y la posible adopción de rutas origen-destino multi-salto hacen este tipo de entornos altamente atractivos para aplicaciones de carácter medioambiental, militar, gestión de situaciones de crisis (p.e., terremotos, atentados terroristas), etc. de alta autonomía [1]. Esta versatilidad se ve incrementada cuando, además, los nodos que conforman la red tienen capacidad de movilidad, lo que constituye las denominadas MANET (*Mobile Ad-hoc NETworks*) [2], nombre del que derivan y con el que están relacionados otros también conocidos como VANET (*Vehicular Ad-hoc NETworks*) y FANET (*Flying Ad-hoc NETworks*).

No obstante las ventajas de este tipo de entornos, son varias también sus limitaciones. Por una parte, por restricciones usuales relacionadas con el tiempo de vida de la batería, la capacidad de almacenamiento y la potencia de cómputo de los nodos. Por otro lado, y no menos importante que lo anterior, por los enormes riesgos de seguridad inherentes a este tipo de redes y sistemas [3]. Especialmente motivados por su naturaleza abierta (inalámbrica), además de la potencial inexistencia de una infraestructura de control y gestión centralizados, son varios los tipos de amenazas existentes [4]. Por mencionar algunos, sírvase citar, entre otros, ataques de *dropping*, en los que un nodo malicioso elimina paquetes en su ruta (multi-salto) hacia un destino dado; ataques de *jamming*, donde un nodo genera interferencias y evita el acceso con éxito de otros al canal de comunicaciones; ataques de suplantación de identidad (*spoofing, sybil*), consistentes en la falsificación de la identidad de un nodo; ataques de *route poisoning*, donde se falsifican las tablas de encaminamiento de los nodos a fin de atraer tráfico hacia una cierta zona con fines maliciosos (eliminación, falsificación, acceso no permitido).

Si bien son conocidas las medidas preventivas de adopción aconsejada para evitar la ocurrencia de actuaciones maliciosas como las antes referidas, como sucede en cualquier otro entorno de comunicaciones, su despliegue no garantiza en modo alguno la no aparición de las mismas. En consecuencia, ante la potencial superación de las barreras de seguridad preventiva dispuestas (generalmente basadas en el empleo de esquemas criptográficos), se precisa complementar éstas con otras orientadas a la detección de eventos indeseados. En este caso, sobre la base de la monitorización de la actividad habida en el entorno, el objetivo es determinar la ocurrencia de comportamientos maliciosos contra la seguridad del sistema. En respuesta a estos eventos debieran ser adoptadas las medidas oportunas para su resolución y, en suma, la recuperación del sistema. Adicionalmente, es recomendable la realimentación de todo el proceso a fin de permitir la adaptación dinámica del entorno (véase Figura 1) [5].

En la literatura se encuentran desarrollados numerosos esquemas de prevención, detección y respuesta (menos de los terceros que de los dos primeros), pero se evidencia una alta carencia de propuestas orientadas a la inter-operación de estos módulos. De esta manera, las soluciones de seguridad habitualmente disponibles son parciales por cuanto que sólo se enfocan en uno de los tres aspectos citados y, sobre todo, porque se desarrollan obviando la necesidad de disponer de procedimientos efectivos de comunicación entre los distintos

Figura 1: Líneas de defensa tradicionales ante incidentes de seguridad.

ISBN: 978-84-9717-323-0

módulos. Esto es especialmente cierto y crítico para entornos de red ad-hoc [6]. En este caso, y frente a otros mecanismos existentes en la actualidad como es el simple envío de un correo electrónico al administrador del sistema, debe habilitarse algún procedimiento que permita la constatación de este hecho por parte del resto de la red para la subsiguiente ejecución de esquemas de respuesta aislados y/o distribuidos globalmente coherentes.

El presente trabajo aborda el diseño y uso de un protocolo de notificación y alerta de eventos de seguridad en la línea antes apuntada. Para ello, el resto del documento se organiza como sigue. En la Sección II se discuten algunas propuestas en la línea aquí planteada existentes en la bibliografía especializada. Tras ello, y habida cuenta de la baja idoneidad de las mismas para entornos ad-hoc, en la Sección III se presenta nuestra propuesta concreta y se discute su uso con varios fines relacionados. Seguidamente, la Sección IV se dedica a un breve análisis de prestaciones del protocolo introducido desde el punto de vista del impacto que tiene su uso sobre las comunicaciones del entorno. Finalmente, en la Sección V se concluye con los aspectos más relevantes de la propuesta realizada y se apuntan brevemente algunas actuaciones de futuro.

II. Trabajo relacionado

Podemos encontrar algunas propuestas de esquemas de notificación de incidentes de seguridad en la literatura. En concreto, es de reseñar el protocol IDXP [7] y el formato de mensajes asociado IDMEF [8] desarrollados por la IETF (http://www.ietf.org). Ambos están centrados exclusivamente en el manejo de información propia de un IDS (*Intrusion Detection System*), no siendo adecuados para datos relacionados con respuesta a incidentes en un contexto más general [9].

Otra propuesta de notificación es IODEF [10]. De tipo XML, IODEF no ha sido adoptado de forma masiva debido a los requerimientos en cuanto a las herramientas necesarias para soportarlo. Frente a este formato, es de mencionar la disponiblidad de otros protocolos y formatos de mensaje tales como X-ARF [11] y XMPP [12], [13], [14].

Sea como fuere, la escasa generalización alcanzada por las propuestas mencionadas hace que las recomendaciones acerca de soluciones de gestión de información de incidentes de seguridad tiendan hacia el uso de ficheros de tipo texto, aconsejándose el empleo de formatos ligeros como CSV (*Comma Separated Value*).

Al margen de las propuestas específicas para incidentes de seguridad antes comentadas, otra posibilidad para el manejo de información relacionada con una red es *syslog* [15]. Desarrollado en la década de 1980 como parte del proyecto Sendmail para tracear los eventos de un sistema, *syslog* permite la separación del software que genera los mensajes del sistema que los almacena y del software que los analiza. Los mensajes *syslog* están etiquetados con un código indicativo del tipo de software que los generó (ftp, mail, etc.) y un grado de severidad (desde *Emergency*, el más alto, hasta *Debug*, el más bajo). Aunque *syslog* puede utilizarse para la gestión de eventos de seguridad, su complejidad (derivada de su amplia versatilidad) hace que este estándar no resulte el mejor candidato para el fin que aquí perseguimos. En especial para redes ad-hoc, donde, según lo ya apuntado en la Sección I, interesaría la adopción de soluciones específicas y, en consecuencia, ligeras desde el punto de vista del coste y carga implicados.

Seguidamente se describe la propuesta de notificación y alerta en nuestro caso adoptada. Ésta, frente a las anteriores, está específicamente diseñada para su uso en entornos ad-hoc, de manera que resulte los menos costosa posible desde el punto de vista de los recursos requeridos.

III. Protocolo de notificación y alerta de eventos de seguridad

Como ya se ha comentado anteriormente, no existen reportadas en la literatura soluciones adecuadas para la notificación de eventos de seguridad en redes ad-hoc. Ideada tomando como base el protocolo de *routing* AODV [17] para este tipo de redes, la propuesta particular que en este apartado se desarrolla presenta las siguientes características principales:

- Versátil, al implementarse sobre la capa de aplicación (concretamente sobre el puerto 703, actualmente sin asignación).
- Rápido y eficiente, definiéndose sobre UDP para reducir retardos y consumo de recursos.
- Flexible, ya que posibilita su uso con diversos fines, contemplándose en la versión actual dos principales:
  - notificación de eventos de seguridad una vez que se haya detectado la ocurrencia de incidentes reseñables, e
  - intercambio de información orientada a la potencial detección colaborativa de tales eventos o a la respuesta ante los mismos.
- El envío de estos mensajes se prevé en tres variantes: *unicast*, *broadcast* a toda la red y *broadcast* a los vecinos, es decir a un salto (TTL=1), dependiendo del tipo de mensaje concreto de que se trate.

Es evidente la necesidad de definir los mensajes específicos que darán soporte a las funcionalidades mencionadas, así como los aspectos relacionados con el envío de los mismos. Seguidamente se discute en detalle todo ello.

III-A. Usos y tipos de mensajes

Como se ha comentado desde el principio, el protocolo está inicialmente pensado para llevar a cabo la notificación de alertas de seguridad ante la constatación de ciertos incidentes en el entorno ad-hoc monitorizado. Esta comunicación permitirá, en su caso, el despliegue posterior de medidas de respuesta orientadas a dar solución a los incidentes reportados. No obstante este fin principal, también es posible la adopción del protocolo para otros objetivos no menos interesantes en el contexto de la seguridad que nos ocupa. Para ello se propone un diseño flexible a través de la especificación de diversos tipos de mensajes. En concreto, en este punto se plantea un segundo uso del protocolo: intercambio de información

de seguridad entre los nodos del entorno para, por ejemplo, posibilitar una detección de eventos maliciosos de forma colaborativa o una respuesta coordinada frente a los mismos.

III-A1. Notificación de alertas: Como ya se ha indicado con anterioridad, es manifiesta la ausencia de procedimientos de alerta de eventos de seguridad en entornos de red; en particular, para redes ad-hoc. Tomando como base los desarrollos IDS realizados por los autores [18], [19], al tiempo que la experiencia en esquemas de respuesta [20], [21], se plantea un procedimiento de notificación de alertas de seguridad para la comunicación de la siguiente información una vez determinada la ocurrencia de un evento intrusivo malicioso:

- *Tipo de mensaje*: necesario para diferenciar entre los distintos usos ya apuntados para el protocolo pretendido.
- *Tipo de evento detectado*: teniendo presentes las distintas tipologías existentes (*dropping*, *sinkhole*, etc. [4]), parece evidente que los posibles mecanismos de respuesta a desplegar dependerán de la tipología concreta del ataque.
- *Severidad del evento*: para indicar el grado de afectación de éste. Por ejemplo, no es lo mismo un ataque de *dropping* donde se descarte un 20 % de los paquetes a retransmitir que uno donde se descarten todos ellos.
- *Confiabilidad de la detección*: para indicar el grado de certeza con el que se concluye el proceso de detección. Asi, por ejemplo, no es comparable la detección de un ataque fundamentada en la observación de un patrón conocido (basada en firmas o *misuse*) que una derivada de la desviación del comportamiento del sistema analizado (detección basada en anomalías). Es evidente que en el primer caso la confiabilidad será del 100 %, mientras que en el segundo será función (previsiblemente) del grado de desviación observado [22].
- *Identidad del nodo malicioso*: necesaria para la adopción de ciertos mecanismos de respuesta específicos (p.e., el aislamiento del nodo en cuestión). Esta identidad se refiere típicamente a la dirección IP del nodo atacante.
- *Identidad del nodo detector*: similar a la anterior, ésta identifica el nodo que detectó el incidente reportado y que corresponde con el nodo emisor del mensaje de notificación.
- *Instante de detección*: identificativo del momento temporal en el que se produjo la observación del incidente de seguridad reportado. Esta información puede resultar útil de cara a la correlación de eventos.

Adicionalmente a la información principal anterior, centrada en el evento de seguridad específico detectado, otra información oportuna a considerar en los mensajes es:

- *Identificador del mensaje*: como es habitual en numerosos protocolos de comunicaciones, este valor se refiere a un número monótonamente creciente identificativo del mensaje para, entre otros fines, robustecer el protocolo ante ataques de repetición.
- *Longitud total*: debido principalmente al campo que sigue abajo, es preciso la indicación expresa de la longitud total (en palabras de 32 bits) del mensaje.

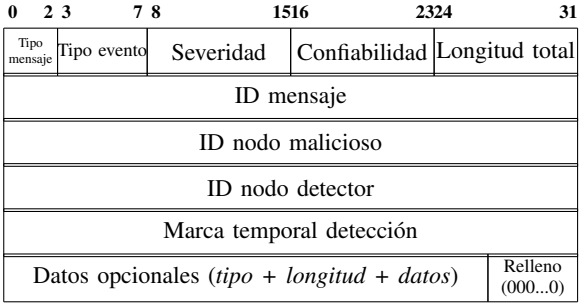

Figura 2: Formato de mensajes de notificación de alertas.

- *Datos (opcional)*: aunque en la versión actual no está definido, sería interesante la inclusión de otra posible información útil varia. Por ejemplo, la localización exacta del nodo malicioso para solucionar ataques de *jamming*. Sean cuales fueren estos posibles usos futuros, el formato de este campo debe ser:
  $< tipo\_datos > \ < longitud\_octetos\_datos > \ < datos >$
  Gracias al campo de *longitud total* previo referido, resulta posible el uso secuenciado de información extra diversa. También es de señalar la necesidad de, con objeto de que el mensaje sea múltiplo de 32 bits, contemplar un campo de *relleno* (*padding*) consistente en todo ceros, localizado (en su caso) al final del campo de información opcional.

De acuerdo con todo lo anterior, el formato de los mensajes de notificación de alertas de incidentes de seguridad propuesto es el mostrado en la Figura 2. En ella se indican los campos anteriormente referidos, junto con los bits asignados a cada uno ellos. Es de significar que algunos de los campos se proponen con una longitud superior a la estrictamente necesaria en este punto para posibilitar la expansión futura del protocolo.

III-A2. Intercambio de información de seguridad: Más allá de la indudable utilidad de los mensajes de alerta descritos, es manifiesto el posible uso del protocolo de notificación ideado para otros fines. Es el caso del potencial intercambio de información de seguridad entre nodos. Esta aplicación, al margen de la evidente similitud con esquemas como IDMEF o *syslog*, surge principalmente de los trabajos [18], [19], donde se plantean esquemas IDS colaborativos fundamentados en el intercambio de información entre nodos (principalmente vecinos). Éstos, frente a los de naturaleza aislada, donde cada nodo implementa su propio IDS a partir de información adquirida exclusivamente de forma local, persiguen la adopción de decisiones de detección más globales y, como tales, más robustas y fiables. Huelga decir que la aplicabilidad del citado intercambio incluye también IDS centralizados donde se precisa la adquisición de información de toda la red por parte de un solo nodo central. En uno y otro caso, centralizado y distribuido, el esquema de intercambio es totalmente análogo: existe un nodo (que implementa un IDS) que solicita información de otro cierto nodo (por ejemplo, porque el IDS local del solicitante ha disparado una alarma para él) a otros nodos de la red (todos, su vecindad, etc.), en respuesta a lo cual se proporciona la información específica solicitada para

facilitar la posterior decisión de detección.

Habida cuenta que los esquemas IDS propuestos por los autores son multi-capa (acceso al canal, capa de red, etc.), la información requerida se va a identificar en los mensajes intercambiados organizada en base a los procedimientos/protocolos específicos a los que aquélla se refiere. En la Figura 3 se muestra el formato específico de los mensajes involucrados en el intercambio de información. Por lo que respecta a los de solicitud (subfigura 3(a)), los campos involucrados son:

- *Tipo de mensaje*: a través del cual se indica la semántica del paquete. Solicitud de información de seguridad en este caso, frente a la notificación de eventos descrita en III-A1 o la respuesta a la solicitud descrita más adelante.
- *Número de entradas*: relativo a la cantidad de variables cuyo valor se solicita. Como se indica más adelante, cada variable se especifica a través de 32 bits.
- *Longitud total*: con el cual se especifica la longitud total (en octetos) del mensaje enviado.
- *ID mensaje*: como en los mensajes de notificación de alertas, si bien en este caso también se utilizará este campo para hacer corresponder solicitudes con respuestas.
- *ID nodo solicitado*: para identificar unívocamente el nodo del que se solicita la información.
- *ID nodo solicitante*: para identificar unívocamente el nodo que solicita la información y que, en definitiva, se prevé llevará a cabo el proceso de detección posterior.
- *Variable 1...n*: campos sucesivos de 32 bits de longitud a través de los cuales se identifica cada una de las *n* variables indicadas en el campo *número de entradas* de las que se pide información para el nodo solicitado. Como hemos mencionado anteriormente, cada variable queda definida (como se hace, por ejemplo, en las MIB de gestión) a partir de dos campos: *protocolo/procedimiento* al que hace referencia (por ejemplo, IP, ICMP, 802.11, etc.) e *identificador* dentro del mismo.

Por lo que respecta a los mensajes de respuesta a los de solicitud anteriores, su formato es el especificado en la Figura 3(b):

- *Tipo de mensaje*: respuesta a solicitud de información.
- *Número de entradas*: cantidad de variables cuyo valor se indica en el mensaje. Como se indica más adelante, cada variable implica el uso de 64 bits, 32 para su identificación y 32 para su valor.
- *Longitud total*: con el cual se especifica la longitud total (en octetos) del mensaje enviado.
- *ID mensaje*: para hacer corresponder solicitudes con respuestas.
- *ID nodo informado*: para identificar unívocamente el nodo del que se comunica la información.
- *ID nodo emisor*: para identificar unívocamente el nodo que envía la información.
- *Variable 1...n*: campos sucesivos de 64 bits de longitud a través de los cuales se identifica e informa de cada una de las *n* variables indicadas en el campo *número de entradas* de las que se requirió información para el *nodo solicitado* en el mensaje de petición (=*nodo informado*). Tras ser identificada cada variable (con 32 bits como se ha establecido antes, 8 de los cuales son para indicar el protocolo/procedimiento al que se refiere), seguidamente se especificará su valor mediante un campo de 32 bits.

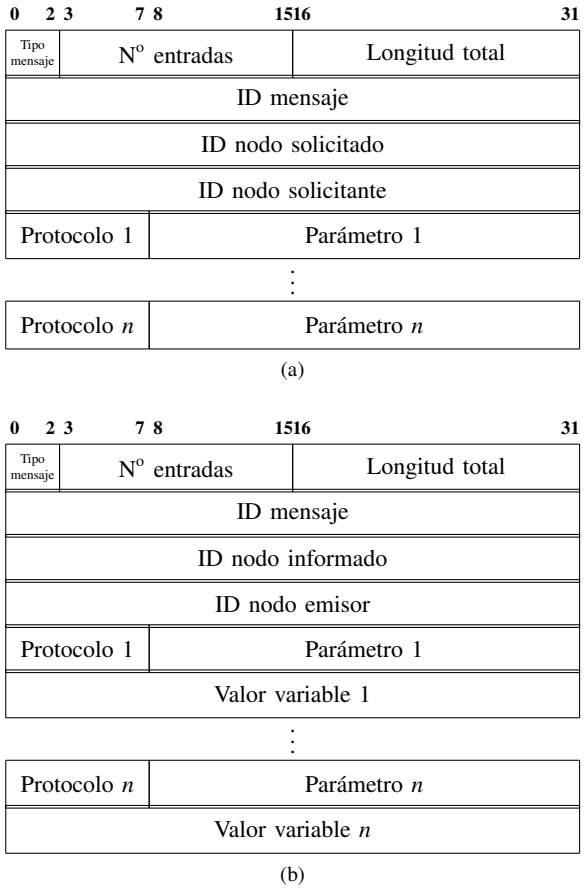

Figura 3: Mensajes de solicitud (a) y respuesta (b) de información.

Aunque la funcionalidad de intercambio de información objeto de estudio no se ha desarrollado completamente en la práctica, en la Tabla I se indican algunas de las variables consideradas y que son utilizadas en los IDS desplegados hasta la fecha por los autores, además de ser de amplio uso para este fin en la literatura. Así, el protocolo propuesto proporciona una gran flexibilidad, posibilitando la extensión del mismo mediante la definición e inclusión de nuevas variables.

No queremos concluir la exposición de los posibles usos y tipos de mensajes asociados al protocolo de notificación desarrollado sin reseñar de nuevo la versatilidad pretendida para el mismo. Así, por ejemplo, se podría definir un nuevo tipo de mensaje de *intercambio de información asíncrona* donde no se precise una solicitud previa. Para ello, por ejemplo, podríamos utilizar el mismo formato de la Figura 3(b) con los siguientes matices:

- *Tipo de mensaje*: fijado a un valor diferente de los tres previos ya descritos.
- *ID mensaje*: identificativo del paquete en sí y no para

Tabla I: Ejemplo de variables para intercambio de información.

Protocolo/ Procedimiento	Parámetro	Notas
Miscelánea	Período muestreo	En s
Topología	Velocidad	En m/s
	Aceleración	En m/s^2
	Localización	Posición GPS
Física	RSSI	De 0 a -80 dBm
MAC 802.11	$\#\mathrm{P}_{\mathrm{RTS}}$	Paquetes RTS / CTS enviados y recibidos
	$\#\mathrm{P}_{\mathrm{CTS}}$	
AODV	$\#\mathrm{P}_{\mathrm{HELLO}}$	Paquetes HELLO / RREQ / RREP enviados, recibidos, retransmitidos y descartados
	$\#\mathrm{P}_{\mathrm{RREQ}}$	
	$\#\mathrm{P}_{\mathrm{RREP}}$	
	NumSeq	Número de secuencia
	HopCount	Número de saltos
Aplicación	$\#\mathrm{P}_{\mathrm{datos}}$	Paquetes de datos enviados, recibidos y perdidos
	#Sesiones	Número de sesiones

hacer corresponder solicitudes con respuestas.

III-B. Distribución de mensajes

Un aspecto importante en el diseño de todo procedimiento de notificación de alertas es el esquema a emplear para la transmisión o envío de la información correspondiente, pues el objetivo es que los recursos implicados, y con ello el impacto sobre las comunicaciones globales, sean los menores posibles. Distintas posibilidades son contempladas para ello en la bibliografía: inundaciones, encaminamiento selectivo, agrupamiento, publicación/suscripción [16]. En nuestro caso, vamos a considerar las siguientes posibilidades en función de la aplicación y tipo de mensaje:

- *Broadcast* a toda la red para la notificación de alertas ante la detección de incidentes. Los nodos que reciban dichos mensajes podrán, a su vez, retransmitir la eventualidad reportada para su distribución a toda la red.
- *Broadcast* a los vecinos para los mensajes de solicitud de información. Para ello, estos paquetes serán enviados sobre la red con el campo TTL del paquete IP sobre el que se encapsulan a valor 1. Es de significar que este tipo de transmisión es más eficiente que el anterior por cuanto que permitiría la inclusión de inteligencia en las retransmisiones de los nodos para evitar informaciones duplicadas.
  También podría considerarse el envío *unicast*, dependiendo del deseo del nodo emisor en cuanto a información pretendida y procedencia de la misma.
- *Unicast* para los mensajes de respuesta hacia el nodo solicitante.

Todas estas cuestiones, así como la propia especificación de los mensajes, tiene un impacto directo sobre las prestaciones de la comunicaciones del entorno monitorizado. Ello es estudiado brevemente en el siguiente apartado.

IV. Análisis de prestaciones

En esta sección se realizará un breve análisis de prestaciones del protocolo propuesto. Para ello, se obtendrá el ancho de banda AB (en bits/s) consumido por la transmisión de los mensajes previamente especificados.

Consideremos una red MANET compuesta de L nodos legítimos $\{N_1, ..., N_L\}$ con un rango de cobertura de r metros, y que se encuentran distribuidos uniformemente en un área de $a \times b$ m^2, con $a, b \gg r$. Asumiendo la existencia de movilidad, cada nodo N_i tendrá su propio conjunto de vecinos V_i. En este escenario general, consideramos adicionalmente la existencia de M nodos maliciosos. Dichos nodos serán excluidos de los cálculos, pues es de suponer que éstos no participarán en actuaciones que tienen como objetivo su detección o aislamiento de la red.

Para el cálculo del ancho de banda consumido será necesario definir una serie de cantidades de interés, así como sus notaciones.

- $\boldsymbol{f_{i,j}^{a/s}}$: representa la frecuencia (en transmisiones por segundo) con la que el nodo N_i envía mensajes (de alerta o de solicitud de información de seguridad) acerca de un nodo N_j. Dicha frecuencia de transmisión vendrá determinada por el procedimiento de detección subyacente implementado.
- $\boldsymbol{P^{a/s/r}}$: representa el tamaño de los paquetes transmitidos (alerta, solicitud o respuesta de información). Dicho tamaño depende de la existencia de datos adicionales en el caso de los mensajes de alerta o del número de parámetros solicitados/respondidos en el caso de los mensajes de intercambio de información.
- $\boldsymbol{E[V_i]}$: denota el número esperado de vecinos del nodo N_i. Dada L/ab la densidad de nodos en el área total, y $(L/ab)\pi r^2$ el número de nodos en el área de cobertura de N_i, es evidente que, restando el propio nodo:

$$E[V_i] = \frac{(L-1)\pi r^2}{ab} \tag{1}$$

- $\boldsymbol{p(I_{v,j})}$: representa la probabilidad de que un nodo N_v dado conozca la información solicitada relativa al nodo N_j y, en consecuencia, pueda responder con un mensaje (*unicast*) a la solicitud recibida.

Una vez definida la notación se ha de distinguir la aplicación concreta para la que se está empleando el protocolo, pues tanto el número como el tamaño de paquetes intercambiados (y con ello el ancho de banda) será dependiente del uso.

IV-A. Notificación de alertas

Para calcular el ancho de banda consumido por la notificación de alertas debemos considerar el peor escenario, es decir, aquel en el que todos los nodos de la red tienen conectividad con al menos otro de los nodos. Puesto que la idea es notificar a todos los nodos la existencia del nodo malicioso, este proceso será *broadcast* a toda la red, donde cada nodo retransmitirá el mensaje de alerta recibido. En esta situación, el número de paquetes de alerta propagados por la red para la notificación iniciada por el nodo N_i relativa al nodo malicioso N_j será de L paquetes (siendo L el número de nodos legítimos en la red).

En consecuencia, el valor esperado del ancho de banda para las situaciones de alerta iniciadas por el nodo N_i respecto a N_j, $AB_{i,j}^{alert}$, será:

$$E[AB_{i,j}^{alert}] = f_{i,j}^{a} \cdot P^{a} \cdot L \text{ bits/s} \quad (2)$$

IV-B. Intercambio de información de seguridad con vecinos

Con respecto a la segunda aplicación aquí prevista, el intercambio de información se producirá cada vez que un nodo N_i precise conseguir información de seguridad acerca de un nodo N_j para, por ejemplo, determinar su comportamiento. Dicho flujo se inicia con un mensaje de solicitud *broadcast* a los vecinos, que será respondido únicamente por aquellos que conozcan la información solicitada por el iniciante. Dichas respuestas serán enviadas en mensajes de respuesta *unicast* (véase Sección III-B).

Así, el valor esperado del ancho de banda consumido ante las posibles peticiones de información de un nodo N_i a sus vecinos respecto del nodo N_j, $AB_{i,j}^{inf}$, será:

$$E[AB_{i,j}^{inf}] = f_{i,j}^{s} \cdot \left(P^{s} + P^{r} \cdot E[V_i] \cdot p(I_{v,j}) \right) \text{ bits/s} \quad (3)$$

Una vez que completemos la implementación efectiva del protocolo propuesto, estos estudios teóricos deberán concretarse sobre escenarios prácticos a fin de ser conscientes de los requisitos reales involucrados.

V. Conclusión

En este trabajo se propone un protocolo de notificación y alerta de eventos de seguridad ideado para la comunicación de actividades maliciosas contra la seguridad de un entorno de red. Por una parte, el procedimiento permite proporcionar diversa información útil, de cara a la adopción de medidas reactivas subsiguientes. Por otro lado, la notificación realizada es distribuida a fin de permitir su uso en entornos no centralizados como son las redes ad-hoc. Por último, el protocolo puede ser usado también como mecanismo de intercambio de información de seguridad entre nodos en este tipo de entornos, con el objeto de posiblitar una detección colaborativa.

Si bien las bondades de la propuesta han sido evidenciadas a nivel teórico en el documento, es objetivo inmediato de los autores la implementación efectiva del protocolo y evaluación de prestaciones del mismo en escenarios experimentales de simulación. Este desarrollo prevé incorporarse al *framework* NETA (*NETwork Attack*) [23], creado por el grupo de investigación NESG (”Network Engineering & Security Group”; http://nesg.ugr.es) y consistente en un entorno basado en OMNET++ para el despliegue, estudio y evaluación de ataques en redes MANET.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el MICINN a través del proyecto TEC2011-22579 y por el MECD a través de la beca del programa de “Formación de Profesorado Universitario” (FPU, Ref.: AP2009-2926).

Referencias

[1] J. He, Mr. Ji, Y. Li, Y. Pan, “Wireless ad-hoc and Sensor Networks: Management, Performance, and Applications,” Boca Raton, FL: CRC Press, 2014.
[2] K.I. Lakhtaria (Ed.), “Technological Advancements and Applications in Mobile Ad-Hoc Networks: Reseach Trends,” Hershey, PA: IGI Global, 2012.
[3] R. Beyah, J. McNair, C. Corbett “Security in Ad-hoc and Sensor Networks,” Hackensack, NJ: World Scientific, 2010.
[4] P. García-Teodoro, L. Sánchez-Casado, G. Maciá-Fernández, “Taxonomy and Holistic Detection of Security Attacks in MANETs,” capítulo del libro “Security for Multihop Wireless Networks”(S. Khan, J. LLoret, Eds.), CRC Press, 2014.
[5] H. Bidgoli (Ed.), “Book of Information Security. Threats, Vulnerabilities, Prevention, Detection, and Management. Volume 3,” John Wiley & Sons, 2006.
[6] A. Nadeem, M.P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks,” en *IEEE Communications Surveys & Tutorials*, Vol. 15, N. 4, 2013, pp. 2027–2045.
[7] B. Feinstein,G. Matthews, “The Intrusion Detection Exchange Protocol (IDXP),” RFC 4767, 2007.
[8] H. Debar, D. Curry, B. Feinstein, “The Intrusion Detection Message Exchange Format (IDMEF),” RFC 4765, 2007.
[9] K. Gorzelak, T. Grudziecki, P. Jacewicz, P. Jaroszewski, L. Juszczyk, P. Kijewski, “Proactive Detection of Network Security Incidents,” ENISA report (A. Belasovs, Ed.), 2011.
[10] R. Danyliw, J. Meijer, Y. Demchenko, “The Incident Object Description Exchange Format,” RFC 5070, 2007.
[11] X-ARF, “Network Abuse Reporting” http://www.x-arf.org, 2014.
[12] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Core,” RFC 6120, 2011.
[13] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence,” RFC 6121, 2011.
[14] P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Address Format,” RFC 6122, 2011.
[15] R. Gerhards, “The Syslog Protocol,” RFC 5424, 2009.
[16] J. Li, S. Khan, Q. Li “An Efficient Event Delivery Scheme in Mobile Ad-hoc Communities,” en *International Journal of Communication Networks and Distributed Systems*, Vol. 10, N. 1, 2013, pp. 25-39.
[17] C. Perkins,E. Belding-Royer, S. Das, “Ad-hoc On-demand Distance Vector (AODV) Routing,” RFC 3561, 2003.
[18] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, “An Efficient Cross-Layer Approach for Malicious Packet Dropping Detection in MANETs,” en *11th. IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications (TrustComm)*, Liverpool (UK), junio 2012, pp. 231-238.
[19] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, N. Aschenbruck, “A Novel Collaborative Approach for Sinkhole Detection in MANETs,” en *Workshop on Security on ad-hoc Networks (SecAN)*, Benidorm (España), junio 2014, pp. 1-14.
[20] R. Magán-Carrión, F. Pulido-Pulido, J. Camacho-Páez, P. García-Teodoro, “Tampered Data Recovery in WSNs through Dynamic PCA and Variable Routing Strategies,” en *3rd. Int. Conference on Communications and Network Security (ICCNS)*, Londres (UK), noviembre 2013. Publicado en *Journal of Communications*, Vol. 8, N. 11, 2013, pp. 738-750.
[21] R. Magán-Carrión, J. Camacho-Páez, P. García-Teodoro, “A Multiagent Self-healing System against Security Incidents in MANETs,” en *Workshop on Active Security through Multi-Agent Systems (WASMAS)*, Salamanca (España), junio 2014, pp. 1-12.
[22] P. García, J.E. Díaz-Verdejo, G. Maciá, E. Vázquez, “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” en *Computers & Security*, Vol. 28, 2009, pp. 18-28.
[23] L. Sánchez-Casado, R.A. Rodríguez-Gómez, R. Magán-Carrión, G. Maciá-Fernández, “NETA: Evaluating the Effects of NETwork Attacks. MANETs as a Case Study,” en *Advances in Security of Information and Communication Networks*, ser. Communications in Computer and Information Science, Vol. 381, (A. Awad, A. Hassanien, K. Baba, Eds.), Springer Berlin Heidelberg, 2013, pp. 1-10.