Análisis de riesgos y contramedidas en REDES MANET

Por Javier Areitio Bertolín

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería y Director del Grupo de Investigación Redes y Sistemas de la Universidad de Deusto. E.Mail: jareitio@deusto.es

Este artículo se enmarca en las actividades desarrolladas dentro de LEFIS-Thematic Network.

En el presente artículo se abordan las redes MANET desde la perspectiva urgente y crítica de su seguridad y su privacidad. Las MANET se están convirtiendo en una forma dominante de red y se espera que desempeñen un papel fundamental en la infraestructura de comunicaciones del futuro. El mundo en que vivimos tiende cada día, más y más, a lo inalámbrico y los servicios de usuario se van haciendo cada vez más móviles, así mismo, se observa un elevado crecimiento en el número de gadgets del tipo smartphone, tablet, etc. y APPs (por ejemplo en App Store y Android Market).

Introducción.

Una MANET (Mobile Ad-hoc NETwork) es una red, del estilo WMN (Wireless Mesh Network), auto-configurable, de enlaces inalámbricos RF, formada por dispositivos (o lo que es lo mismo, nodos) móviles (computadores móviles con capacidades de comunicación inalámbrica como smartphones, tablets/iPad2, PDAs, iPhones, iPad/iPods, móviles inteligentes tipo reloj de pulsera, PCs/Mac portátiles, etc.). Las MANET son redes autónomas, de topología dinámica, enlaces ad-hoc P2P, de fácil y rápido despliegue, que no necesitan infraestructura (como puntos de acceso WiFi y torres de estaciones base celulares con antenas 2G/2,5G, 3G/3,5G, 4G). Una MANET pura carece de infraestructura, esto implica que los mecanismos de seguridad-privacidad están descentralizados y distribuidos. Los dispositivos en una MANET pueden moverse independientemente o como grupos en diferentes direcciones. Por tanto la topología de red y sus enlaces entre dispositivos cambian con frecuencia. Cada dispositivo puede funcionar como retransmisor, reenviando tráfico destinado a otros dispositivos. Las rutas entre nodos pueden contener potencialmente múltiples saltos. La movilidad puede causar cambios de rutas. Las MANET pueden ser redes autónomas o pueden conectarse a otras redes externas con infraestructura (Internet, redes corporativas-Intranets, extranets (o intranets interconectadas a través de Internet), redes celulares como GSM/GPRS/HSDPA/WCDMA, etc.). Según un estudio de Cisco Systems el 90% de los responsables de Tecnologías de Información opinan que el gadget tablet se generalizará en los próximos dos años, así mismo señala que en Alemania la presencia del tablet en el área comercial es del 31% frente al 21% de la media global y el 19% registrado en España.

Principales propiedades. Limitaciones de los dispositivos.

Las principales características de las MANET son la autonomía, la movilidad, la comunicación inalámbrica RF, el multi-salto y la no dependencia de infraestructuras fijas. Pueden ser autónomas o estar conectadas a Internet/Intranet (para acceder a más servicios y recursos). Debido a que los nodos que se comunican pueden llegar a estar fuera de rango, deben poder retransmitir tráfico. Todos los nodos en las redes MANET suelen utilizar el mismo espectro de frecuencia o canal físico. Consecuentemente el nivel MAC (Media Access Control) desempeña una parte clave en la sincronización del acceso al canal entre nodos. Una MANET es auto-formante, es decir, los dispositivos desplegados toman un enfoque P2P (Peer-to-Peer) en la formación de su propia infraestructura de routing de red. Los dispositivos que se encuentran dentro del rango de otros, establecen asociación de red, sin necesidad de intervención humana. El continuo movimiento conduce a variar la conectividad entre los dispositivos, dando lugar a cambios de la topología de red. Una MANET se auto-repara, es decir, se reorganiza automáticamente cuando los dispositivos se unen o abandonan la red sin impactar en el funcionamiento de los otros dispositivos que participan. Una MANET se auto-protege, es decir, los dispositivos salvaguardan la información que fluye a través de la red, defendiéndose contra accesos no autorizados, suplantaciones, denegación de servicios por inhibidores de RF, etc. de acuerdo con la política de seguridad global. La auto-protección es compleja teniendo en cuenta que los dispositivos móviles carecen de seguridad física y la existencia de vulnerabilidades del medio de transmisión con escuchas clandestinas, MITM e interferencias-jaming. Cada dispositivo debe poder transmitir, recibir y encaminar mensajes en nombre de otros dispositivos (función proxy). Los dispositivos MANET presentan limitaciones en cuanto a capacidad y recursos tales como rango de transmisión, duración y potencia de la batería, disponibilidad de memoria y potencia de CPU (computación). Debido a su gran flexibilidad y resiliciencia-resistencia frente a fallos, las MANET posibilitan desarrollar un creciente número de aplicaciones. Se utilizan en el área comercial, en logística, en operaciones de emergencia para búsquedas, rescates y recuperación de desastres (terremotos/maremotos, desprendimiento de tierras, inundaciones, tornados/huracanes, fugas químicas y nucleares, etc.), en operaciones de bomberos, militares (soldados, tanques, helicópteros) y policiales (contra guerrillas urbanas), en despliegues sanitarios, e-commerce/e-business, tráfico vehicular y guía contra accidentes, comunicaciones ad-hoc, conferencias, juegos multi-usuario, artefactos robotizados, detección biológica, espacio de trabajo móvil, infraestructuras críticas como smart-energy, smart-buildings, smart-transport, redes de área personal, entornos civiles (redes de taxis, salas de reuniones, macro-discotecas, estadios olímpicos, aviones, trasatlánticos, estudiantes en campus universitarios, conferencias, redes de sensores, etc.).

Categorias de redes MANET.

Los principales tipos de redes MANET son:

VANET (Vehicular Ad-hoc NETwork).

Son redes utilizadas para comunicarse entre vehículos y/o entre vehículos e infraestructura al borde de la carretera (estaciones base) para compartir

información de tráfico, estado de las carreteras, condiciones medioambientales y posibles accidentes-obras. En este entorno, la resistencia de los usuarios a la trazabilidad es una característica natural ya que como es posible el seguimiento de vehículos, la tecnología debe poner los medios, que los hay, para proteger la privacidad de las personas manteniendo sin degradar la seguridad. Las VANET están siendo estandarizadas por el ISO (Internacional Standards Organization) dentro del estándar DSRC (Dedicated Short Range Communications). Algunos fabricantes de automóviles ya comienzan ha instalar el equipamiento necesario y las tecnologías en sus vehículos para cumplir con DSRC.

WSN (Wireless Sensor Network) móvil no estacionaria.

Una WSN consta de un conjunto de sensores autónomos (dispositivos pequeños), distribuidos espacialmente, conectados vía una infraestructura de comunicaciones inalámbrica (o Ad hoc) con el objetivo de monitorizar, registrar, procesar y almacenar, de forma cooperativa, condiciones físicas del entorno y medioambientales como temperatura, grado de deformación, sonido, vibración, radiación, presión, humedad, nivel de contaminación, movimiento, etc. Se pueden identificar tres áreas conceptuales:
(i) Sensores urbanos, personales, móviles. Se caracterizan por ser móviles, pueden estar operados por personas, su autonomía de energía puede ser de pocos días.
(ii) Sensores autónomos remotos. Normalmente no son móviles, su autonomía de energía puede ser de años. Por ejemplo medir parámetros físicos en la cima de una montaña de poca accesibilidad.
(iii) Sensores embebidos en infraestructuras y edificios/puentes. No suelen ser móviles y no los operan las personas.

Las WSN pueden ser estacionarias/fijas o móviles. Un ejemplo de las segundas del tipo multisensor es el caso de permitir que los smartphones se utilicen como sensores, que capturen muy diversas condiciones, por ejemplo medioambientales (contaminantes como monóxido de carbono, nivel de ruido, datos de IoT). En un futuro próximo nos encontraremos con sensores móviles en entornos de business, sanitarios, civiles, militares, en operaciones de búsqueda y rescate, guerra urbana, etc.

La propiedad física a ser monitorizada determina el tipo de sensor:
(i) Sensor de temperatura: termistores basados en semiconductores, termopares, por lectura de radiación infrarroja.
(ii) Presión: manómetro, barómetro, medidor de ionización.
(iii) Ópticos: fotodiodos, fototransistores, sensores infrarrojos, sensores CCD.
(iv) Acústicos: micrófonos, resonadores piezoeléctricos, sonómetros.
(v) Mecánicos: sensores táctiles, diafragmas capacitivos, células piezoeléctricas, medidor de presión-tensión, galgas extensiométricos.
(vi) Vibración y movimiento: acelerómetros, sensores de flujo de masa de aire.
(vii) Posición: GPS, giróscopos, sensores basados en ultrasonidos, sensores basados en infrarrojos.
(viii) Electromagnéticos: magnetómetros, sensores de efecto Hall.
(ix) Químicos: sensores de pH, sensores electroquímicos, sensores de gas por infrarrojos, sensores de gas Sarin.
(x) Humedad: higrómetros, sensores capacitivos y resistivos, sensores de humedad basados en MEMS.
(xi) Radiación: detectores de ionización, contadores Geiger- Mueller, medidores de V/m.
(xii) Biológicos: detectores de virus ántrax, VIH, etc.

Algunas URLs sobre portales de sensores (hacia la Web de las cosas, IoT):
http://pachube.com
http://openenergymonitor.org/emon/;
http://sourceforge.net/projects/gsn/ (global sensor network)
http://atom.research.microsoft.com/sensewebv3/sensormap/ (mapa de sensores Microsoft)
http://sensorpedia.com (sensorpedia).

MANET Geo-sociales.

Las Redes Sociales online van creciendo en los últimos años. La siguiente innovación en Redes Sociales es anticiparse a trabajar sobre dispositivos móviles utilizando información de localización. Existen diversas aplicaciones de Red Social móviles basadas en localización como Foursquare, Google.com/Latitude, Brightkite. Así mismo, varias de las principales plataformas de Redes Sociales han empezado a utilizar información de localización en sus versiones móviles. Actualmente la mayor parte de estas aplicaciones de Redes Sociales se soportan en infraestructura de red celular, sin embargo esto cambiará pronto. La empresa sueca TerraNet AB presentó una red en malla de teléfonos móviles que permite realizar llamadas y transmitir datos encaminando entre los equipos de los participantes sin sitios celulares. En el futuro este modo ad-hoc de funcionamiento aumentará y se adoptará para cubrir áreas sin conectividad o para reducir la carga en infraestructuras de red celulares UMTS/HSDPA/GPRS/GSM/WCDMA, etc. Otro dominio de aplicación son los juegos geo-sociales multi-usuario interactivos como por ejemplo TurfWars.

MANET para entornos de misión crítica, militares y para cuerpos de seguridad (policía, bomberos, etc.).

Son redes compuestas por dispositivos que no necesitan infraestructura, utilizados en entornos militares/guerra urbana, especialmente en el campo de batalla, por ejemplo dispositivos portátiles (con normal MIL) o implantados como prótesis (para facilitar su adaptación con la persona) utilizados por los soldados-policías de a pie, dispositivos de comunicación en vehículos y aeronaves así como otros tipos de personal y equipamiento. El proteger la seguridad y privacidad en estas redes es crucial debido a la hostilidad del entorno donde se utilizan. Si el adversario puede detectar los movimientos de los nodos, podrá inferir los tipos de nodos, así por ejemplo un nodo que se mueva 95 Km. en 10 minutos probablemente sea una aeronave (por ejemplo un helicóptero), si se mueve sólo 6 Km. en el mismo período de tiempo posiblemente sea un vehículo. Otras actividades de los adversarios es el seguimiento de nodos específicos, por ejemplo averiguar quien es el comandante o el centro de operaciones para destruirlo. Los ataques a los dispositivos en dichas redes son reales y se realizan siempre que el atacante encuentre un punto de debilidad. Además existe un elevado riesgo de que los adversarios capturen dispositivos y traten de extraer información secreta de dentro, una posible defensa es que los microprocesadores y chips de estos dispositivos incluyan en hardware tecnología del tipo Intel AT (Anti-Theft) para destruir su contenido si caen en manos no deseadas.

Aspectos de seguridad-privacidad y retos en MANET.

Los aspectos de seguridad-privacidad más difíciles en MANETs son:
(1) Las cuestiones de gestión de identidades (nombres, direccionamiento).
(2) La autenticación mutua de usuarios y dispositivos.
(3) El proceso de routing y el descubrimiento de servicios.
(4) El acceso y entrada a la red.
(5) Los sistemas de detección y prevención de intrusiones. (
6) La gestión de información confiable.

Algunos de los desafíos que plantean las MANETs son:
(1) Rango de transmisión inalámbrico limitado.
(2) Naturaleza de difusión del medio inalámbrico.
(3) Pérdida de paquetes debido a errores de transmisión, por causas naturales y maliciosas.
(4) Cambios de ruta inducidos por la movilidad.
(5) Pérdida de paquetes inducida por la movilidad.
(6) Restricciones de las baterías de los dispositivos móviles que se comunican.
(7) Posibles particiones de red frecuentes.
(8) Facilidad para las escuchas clandestinas de las transmisiones inalámbricas si no están cifradas y/o ocultas por esteganografía. Así como de suplantaciones MITM si no existen mecanismos de firma digital.

Clases de atacantes y modelos de ataques MANET.

Los atacantes (o adversarios) pueden clasificarse atendiendo a muy diferentes criterios en:

(1) Externos.

Son adversarios que no pertenecen a la red o al grupo que se comunican de forma autorizada. Dichos adversarios no poseen claves criptográficas utilizadas para proteger la red. Estos adversarios son más fáciles de detectar. En los ataques de adversarios externos el atacante causa congestión del tráfico o trastorna los nodos-dispositivos mediante la denegación de servicios, para ello puede utilizar técnicas como:
(i) Alterar el número de secuencia situado en el campo control del mensaje, los nodos maliciosos pueden causar ataques DoS o redirección del tráfico.
(ii) El ataque DoS puede también lanzarse alterando las rutas de la fuente en las cabeceras de los paquetes.
(iii) La propagación de la información de routing (o encaminamiento) puede bloquearse atacando a los protocolos de routing.
(iv) Para perturbar la transmisión del paquete a lo largo del camino predefinido, el atacante ataca el reenvío del paquete.
(v) Para perturbar una ruta operativa, el atacante puede generar un falso error de ruta o crear la impresión incorrecta en otros, lo que puede ocultar el error.
(vi) Un nodo puede representar su identidad incorrecta y ataca por spoofing lo que se denomina suplantación.
(vii) Obtener el control sobre los propios nodos por medio de técnicas no honradas y utilizar los nodos comprometidos para realizar acciones maliciosas-perversas.

(2) Internos.

Estos adversarios pertenecen a la red o al grupo que se comunica de forma autorizada. Dichos adversarios poseen claves criptográficas utilizadas para proteger el funcionamiento de la red. Estos adversarios son más difíciles de detectar y de defenderse contra ellos y sus resultados suelen ser muy dañinos. En los ataques procedentes de atacantes internos, el adversario desea obtener acceso a la red tomando parte en las actividades de la red. Utiliza el nodo corriente como base para realizar sus comportamientos maliciosos.

(3) Fijos o móviles.

Según se encuentren estacionarios o en movimiento.

(4) Sigilosos y no sigilosos.

Según se mantenga oculto o se pueda percibir algo su existencia.

(5) Activos y pasivos.

Según el tipo de ataque que realicen.

(6) En solitario o en grupo.

Múltiples atacantes pueden coexistir en el mismo sistema y pueden unir sus fuerzas trabajando de forma cooperativa (dando lugar a un ataque de confabulación). Esto posibilita realizar ataques más complejos.

Cada tipo de adversario puede lanzar dos tipos de ataques:

(1) Ataques pasivos.

No causan daño directo a un sistema sino que se dedican a capturar información. Se utilizan técnicas como:
(i) Escuchas clandestinas de las comunicaciones con antenas. La RF (Radio Frecuencia) es un medio ubicuo, potencialmente toda entidad puede escuchar transmisiones no protegidas y protegidas si se conoce el protocolo, incluso desde mucha distancia, el caso límite es el uso de satélites. El ataque de escucha clandestina obtiene cierta información confidencial como la clave pública, la clave privada o las contraseñas.
(ii) Análisis de tráfico. Analizando el tráfico (quien es el emisor, quien es el receptor, cual es el número y longitud de los mensajes intercambiados, a qué hora se envían, desde donde se envían vía IP y geo-localización, etc.) puede inferirse información útil como la topología de la red y el rol del nodo-dispositivo. Pueden observarse diferentes niveles. Normalmente se utilizan como puntos de arranque para realizar ataques dirigidos a elementos clave, por ejemplo un ataque de Denegación de Servicios (DoS) alrededor del objetivo. El atacante no interfiere con el funcionamiento del protocolo y normalmente trata de mantenerse sigilosos para que no se le detecte.

(2) Ataques activos.

Causan daño directo y perturban el funcionamiento normal del sistema. Obtienen acceso (o toman el control físico) de una parte del enlace de comunicaciones (o de un nodo de un extremo) para insertar, modificar y/o capturar transmisiones y mensajes. Dichos ataques se lanzan fácilmente a una MANET debido a la naturaleza inalámbrica de los enlaces de difusión y el acceso no restringido. Son ataques más fáciles de detectar que los pasivos. Los ataques más comunes son:

(i) Ataque físico. Los nodos pueden estar fácilmente accesibles a los atacantes físicos. Dos posibles técnicas son: (a) Destrucción. Uno o varios nodos se destruyen y se eliminan de la red. (b) Alteración. Los nodos son analizados y/o alterados de diferentes formas: volcado del firmware, reprogramación del nodo, nodos clonados y volcado de las claves criptográficas.

(ii) Ataques de camuflaje, de repetición, de modificación de mensajes y ataques sybil: (a) En el ataque de camuflaje un nodo pretende ser otro; se suplantan nodos. La identificación no siempre se utiliza o es fácil de atacar.

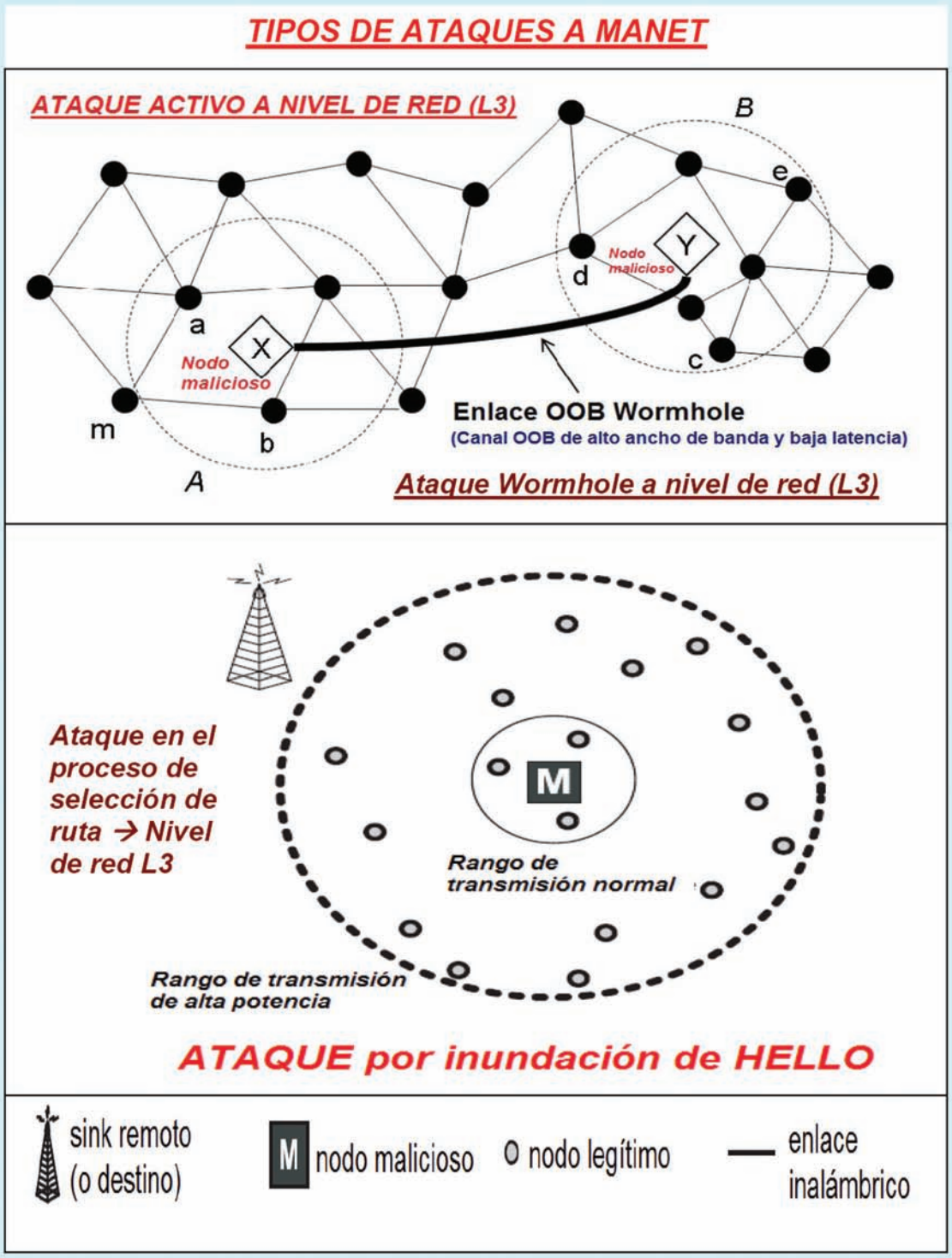


Fig. 1.- Ataques a MANET en el nivel de red.

Los protocolos reactivos (opuestos a los protocolos basados en routing) pueden atacarse fácilmente. (b) En un ataque de repetición los nodos camuflados con éxito pueden repetir el mismo mensaje de forma indefinida (es el caso del logging-in sin nombre de usuario y contraseña). (c) En un ataque de modificación del mensaje el mensaje puede modificarse antes de ser repetido o reenviado (por ejemplo la temperatura esta dentro de los valores normales). (d) En un ataque sybil un nodo se relaciona con el resto de la red utilizando múltiples identidades diferentes. Los datos acumulados pueden alterarse y el camino de routing puede invalidarse. El nodo atacante dice tener muchas identidades o localizaciones.

(iii) Ataques de denegación de servicios (DoS). Los ataques DoS socavan la disponibilidad del servicio proporcionado por el sistema. Los ataques DoS pueden realizarse en diferentes niveles,

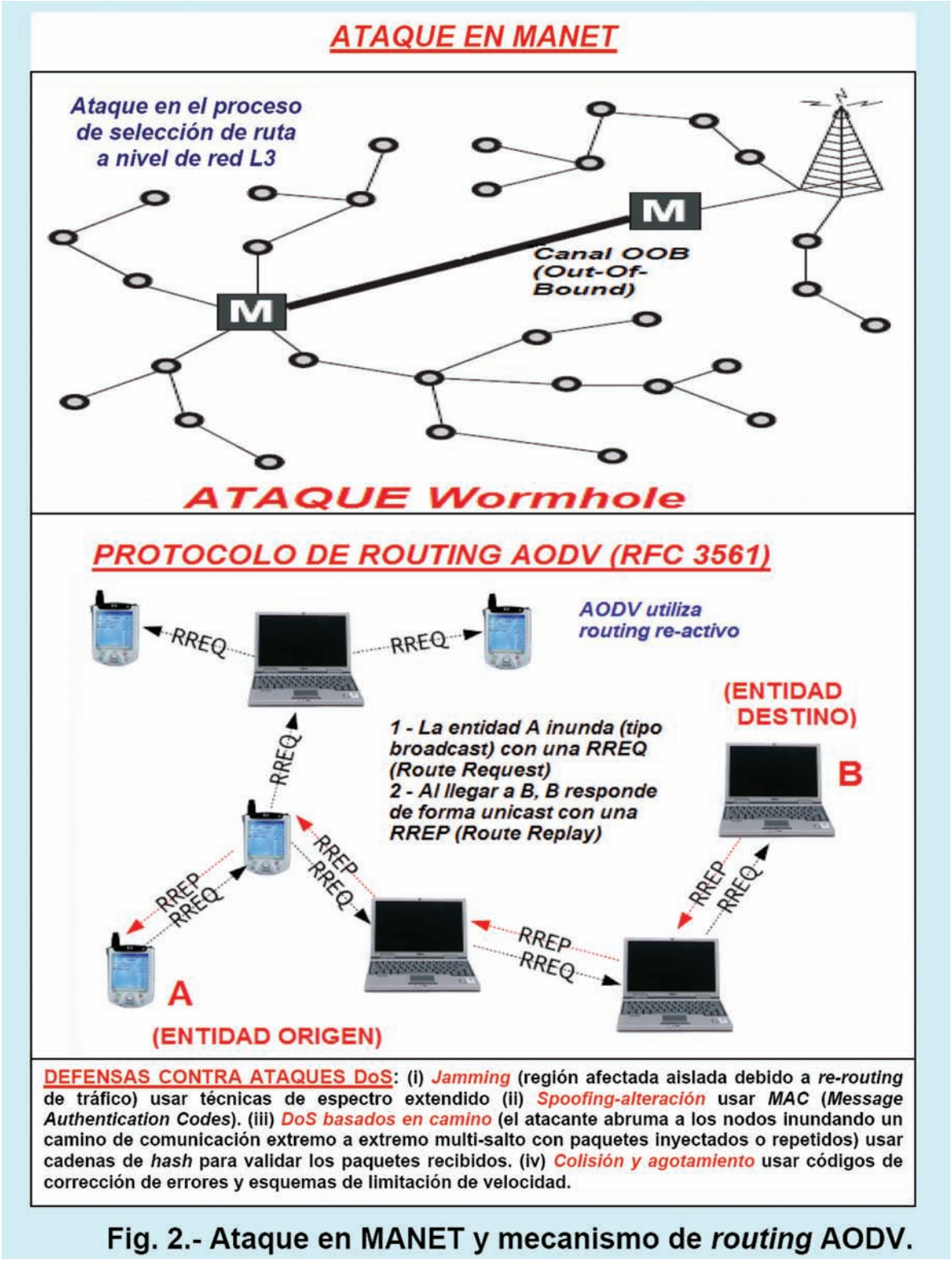


Fig. 2.- Ataque en MANET y mecanismo de *routing* AODV.

sin embargo, se suelen solapar diferentes tipos de DoS:

(a) DoS a nivel físico (L1). Diversas técnicas son: (1) El jamming. La señal de RF puede ser perturbada utilizando señales que se solapan, que pueden reducir el cociente S/N (potencia de señal partido por potencia del ruido) por debajo del umbral aceptable. El jamming puede realizase de forma remota y selectivamente. (2) Destrucción y alteración. Estos dos ataques se pueden realizar para causar DoS dentro del sistema.

(b) DoS a nivel MAC y enlace de datos (L2). Estos ataques explotan información específica del protocolo. Son: la colisión intencionada (mediante el envío de paquetes CTS (Clear-To-Send) que chocan cuando se recibe un paquete RTS (Request To Send); mediante jamming de períodos activos; mediante falsificación de transmisiones largas) y el agotamiento de recursos (los nodos normalmente tienen una cantidad limitada de ener-

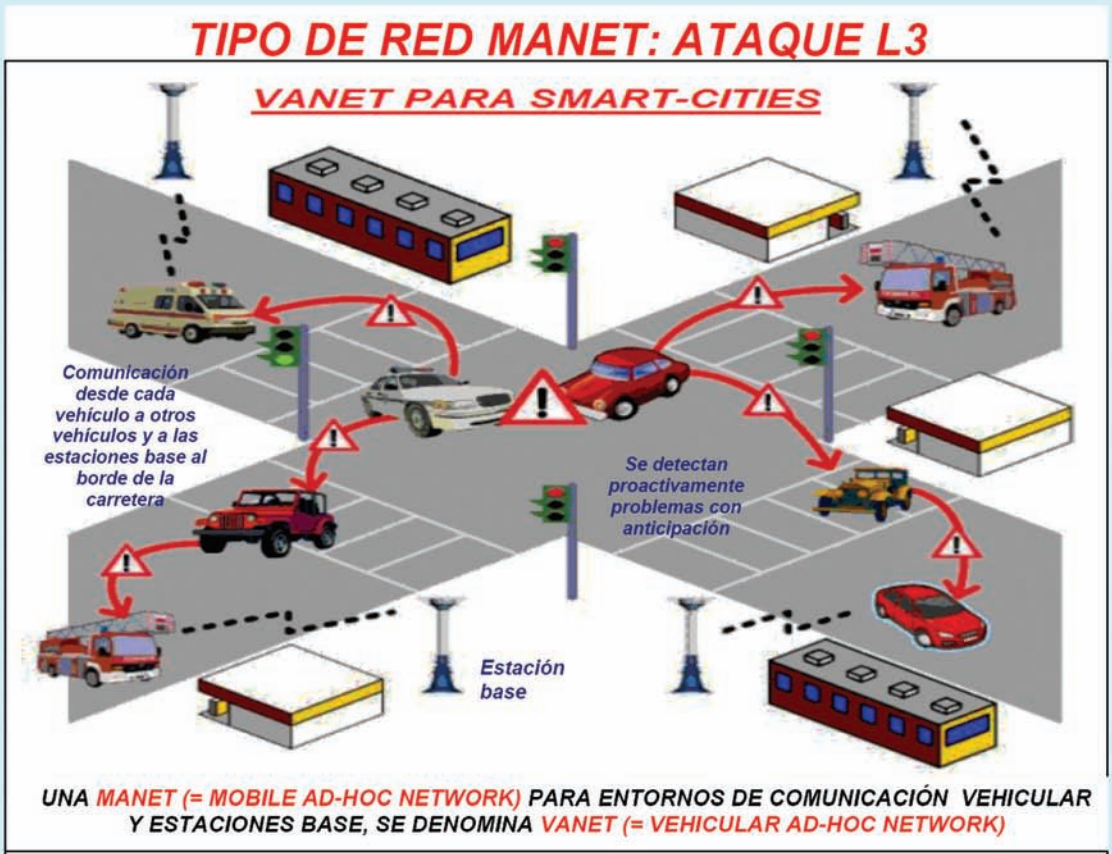


Fig. 3.- Un tipo de MANET y una clase de ataque L3.

gía, una batería. Mediante ataques de colisiones intencionados prolongados se puede producir una disminución de energía más rápida; mediante la eliminación permanente de los nodos atacados de la red).

(c) DoS a nivel de red (L3). El objetivo de estos ataques es perturbar la entrega normal de paquetes del nivel de red o causar agotamiento de recursos mediante el envío de datos falsificados. Algunas técnicas utilizadas son: (1) Inundación de 'hello' (se utilizan señales potentes para difundir paquetes hello donde el atacante pretende ser un vecino de todos los demás nodos. Los mensajes enviados al atacante no alcanzarán su destino). (2) Los desvíos (se puede forzar rutas sub-óptimas, por ejemplo, añadiendo nodos virtuales, de modo que se utiliza más energía para retransmitir los paquetes. Además se pueden crear lazos). (3) Los ataques sinkhole (un nodo malicioso

MECANISMO DE FIRMA DIGITAL UMBRAL (t = 3, N = 18) BASADA EN ECC DE TIPO DISTRIBUIDO PARA MANET

- **OBJETIVO**: *Permite distribuir un conjunto de fragmentos de clave privada a un grupo N de posibles firmantes, de modo que al reunirse t o más posibles firmantes puedan reconstruir la clave privada y firmar un mensaje. Si se reúnen menos de t posibles firmantes no podrán recuperar la clave privada de firma, y firmar. Se utiliza el mecanismo umbral de secreto compartido Shamir (t = 3, N = 18).*
- **DESCRIPCIÓN DEL MECANISMO**: **(1) PROCESO INICIAL**: Se elige una curva elíptica sobre GF(p) donde p es un número primo grande p, por ejemplo: p = 23 → $y^2 = (x^3 + 2.x + 17) \bmod 23$ de 19 puntos, donde 18 puntos son de orden 19. Se elige un punto P de orden 19, es decir: 19.P = O, por ejemplo P = (3, 2). En este caso L = 19. Se elige un valor secreto a, por ejemplo a = 11, y se calcula el punto Q = a.P. En este caso Q = 11.P = (10, 18). Se hacen públicos P y Q. Todos los posibles firmantes comparten dos secretos a y k utilizando un esquema umbral tipo *secreto compartido Shamir* (t, N). Sea por ejemplo k = 13 y sea (t = 3, N = 18). Sean los polinomios: $a_i = (7.i^2 + 5.i + a) \bmod L$; $k_i = (7.i^2 + 5.i + k) \bmod L$; Tres posibles fragmentos de a son: $a_1 = 4$, $a_2 = 11$, $a_3 = 13$. Tres posibles fragmentos de k son: $k_1 = 6$, $k_2 = 13$, $k_3 = 15$. Se reparte a las N = 18 posibles firmantes un fragmento de k y otro de a, por ejemplo: $k_1 = 6$, $k_2 = 13$, $k_3 = 15$ y $a_1 = 4$, $a_2 = 11$, $a_3 = 13$. Si se juntan tres o más recuperan k y a.

(2) PROCESO DE FIRMA DIGITAL: Sea el mensaje a firmar M = 2. Un grupo autorizado de t = 3 o más entidades se reúnen y calculan k. Determinan R = k.P. En este caso: R = 13.P = (15, 15). A partir del punto R se obtiene el valor de la abscisa que se llama: r = (x de R) = 15. Se calcula: el hash de M concatenado con r, es decir: e = H(M | r). Supongamos por ejemplo que: e = H(M | r) = (M + r) mod L. En este caso e = 2 + 15 = 17 mod 19. Con los valores (a_i, k_i) que poseen los posibles firmantes si son tres o más los llevan a la expresión $s_i = (k_i . e - a_i) \bmod L$ y determinan utilizando el polinomio $s_i = (\alpha.i^2 + \beta.i + s) \bmod L$ → las incógnitas (s, α, β). En este caso: $s_1 = 3$, $s_2 = 1$, $s_3 = 14$. Con tres o más valores se recupera s = 1, $\alpha = 17$, $\beta = 4$. La *firma digital es: (M, r, e, s)*. En este caso: (M = 2, r = 15, e = 17, s = 1).

(3) PROCESO DE VERIFICACIÓN: Se comprueba si e' = H(M | r) = e; en este caso: H(2, 15) = 17 = e. Se calcula P' = (s.P + Q) mod p. En este caso: P' = 1.P + Q = (11, 6). Se obtiene un punto X de la curva con abscisa r = 15 → X = (15, ± y mod 23) → X = (15, 8) o (15, 15). La firma es válida si: ± P ' = e.X. Aquí: e.X = 17.(15, 15) = (11, 6) ; e.X = 17.(15, 8) = (11, 17) = – (11, 3) mod 23 →OK !

O	(2,11)	(2,12)	(3,2)	(3,21)	(7,11)	(7,12)	(8,4)	(8,19)	(10,5)	(10,18)	(11,6)	(11,17)	(13,3)	(13,20)	(14,11)	(14,12)	(15,8)	(15,15)
(2,11)	(8,4)	O	(7,11)	(3,2)	(14,12)	(3,21)	(15,8)	(2,12)	(13,3)	(15,15)	(14,11)	(13,20)	(11,6)	(10,18)	(7,12)	(11,17)	(10,5)	(8,19)
(2,12)	O	(8,19)	(3,21)	(7,12)	(3,2)	(14,11)	(2,11)	(15,15)	(15,8)	(13,20)	(13,3)	(14,12)	(10,5)	(11,17)	(11,6)	(7,11)	(8,4)	(10,18)
(3,2)	(7,11)	(3,21)	(2,11)	O	(8,4)	(2,12)	(14,12)	(7,12)	(13,20)	(11,6)	(15,15)	(10,5)	(10,18)	(13,3)	(8,19)	(15,8)	(11,17)	(14,11)
(3,21)	(3,2)	(7,12)	O	(2,12)	(2,11)	(8,19)	(7,11)	(14,11)	(11,17)	(13,3)	(10,18)	(15,8)	(13,20)	(10,5)	(15,15)	(8,4)	(14,12)	(11,6)
(7,11)	(14,12)	(3,2)	(8,4)	(2,11)	(15,8)	O	(11,17)	(3,21)	(10,18)	(14,11)	(8,19)	(13,3)	(15,15)	(11,6)	(2,12)	(10,5)	(13,20)	(7,12)
(7,12)	(3,21)	(14,11)	(2,12)	(8,19)	O	(15,15)	(3,2)	(11,6)	(14,12)	(10,5)	(13,20)	(8,4)	(11,17)	(15,8)	(10,18)	(2,11)	(7,11)	(13,3)
(8,4)	(15,8)	(2,11)	(14,12)	(7,11)	(11,17)	(3,2)	(10,5)	O	(11,6)	(8,19)	(7,12)	(10,18)	(14,11)	(15,15)	(3,21)	(13,20)	(13,3)	(2,12)
(8,19)	(2,12)	(15,15)	(7,12)	(14,11)	(3,21)	(11,6)	O	(10,18)	(8,4)	(11,17)	(10,5)	(7,11)	(15,8)	(14,12)	(13,3)	(3,2)	(2,11)	(13,20)
(10,5)	(13,3)	(15,8)	(13,20)	(11,17)	(10,18)	(14,12)	(11,6)	(8,4)	(7,12)	O	(3,2)	(8,19)	(3,21)	(2,12)	(7,11)	(15,15)	(14,11)	(2,11)
(10,18)	(15,15)	(13,20)	(11,6)	(13,3)	(14,11)	(10,5)	(8,19)	(11,17)	O	(7,11)	(8,4)	(3,21)	(2,11)	(3,2)	(15,8)	(7,12)	(2,12)	(14,12)
(11,6)	(14,11)	(13,3)	(15,15)	(10,18)	(8,19)	(13,20)	(7,12)	(10,5)	(3,2)	(8,4)	(14,12)	O	(7,11)	(2,11)	(11,17)	(2,12)	(3,21)	(15,8)
(11,17)	(13,20)	(14,12)	(10,5)	(15,8)	(13,3)	(8,4)	(10,18)	(7,11)	(8,19)	(3,21)	O	(14,11)	(2,12)	(7,12)	(2,11)	(11,6)	(15,15)	(3,2)
(13,3)	(11,6)	(10,5)	(10,18)	(13,20)	(15,15)	(11,17)	(14,11)	(15,8)	(3,21)	(2,11)	(7,11)	(2,12)	(3,2)	O	(14,12)	(8,19)	(7,12)	(8,4)
(13,20)	(10,18)	(11,17)	(13,3)	(10,5)	(11,6)	(15,8)	(15,15)	(14,12)	(2,12)	(3,2)	(2,11)	(7,12)	O	(3,21)	(8,4)	(14,11)	(8,19)	(7,11)
(14,11)	(7,12)	(11,6)	(8,19)	(15,15)	(2,12)	(10,18)	(3,21)	(13,3)	(7,11)	(15,8)	(11,17)	(2,11)	(14,12)	(8,4)	(13,20)	O	(3,2)	(10,5)
(14,12)	(11,17)	(7,11)	(15,8)	(8,4)	(10,5)	(2,11)	(13,20)	(3,2)	(15,15)	(7,12)	(2,12)	(11,6)	(8,19)	(14,11)	O	(13,3)	(10,18)	(3,21)
(15,8)	(10,5)	(8,4)	(11,17)	(14,12)	(13,20)	(7,11)	(13,3)	(2,11)	(14,11)	(2,12)	(3,21)	(15,15)	(7,12)	(8,19)	(3,2)	(10,18)	(11,6)	O
(15,15)	(8,19)	(10,18)	(14,11)	(11,6)	(7,12)	(13,3)	(2,12)	(13,20)	(2,11)	(14,12)	(15,8)	(3,2)	(8,4)	(7,11)	(10,5)	(3,21)	O	(11,17)

Fig. 4.- Mecanismo firma digital umbral (3, 18) ECC para MANET.

se presenta como una buena elección de routing y se convierte en un hub para los mensajes que van a la estación base. Estos mensajes pueden entonces desecharse o utilizarse para ataques adicionales). (4) El ataque blackhole (un nodo empieza a desechar todo el tráfico que recibe. Si el nodo es también un sumidero, el ataque es mucho más efectivo). (5) El reenvío selectivo o ataque greyhole (sólo un tipo concreto de paquetes se desecha por el nodo bien para su propia ventaja o para evitar la detección). (6) El ataque wormhole dos nodos maliciosos pueden confabularse para reenviar mensajes de uno a otro utilizando un canal de baja latencia y alto ancho de banda OOB (Out-Of-Bound), atrae muchos flujos de los nodos legítimos. Las tablas de vecinos son invalidadas y los paquetes regulares se desechan al alcanzar su TTL). (7) El ataque rushing. Explota las técnicas de descubrimiento

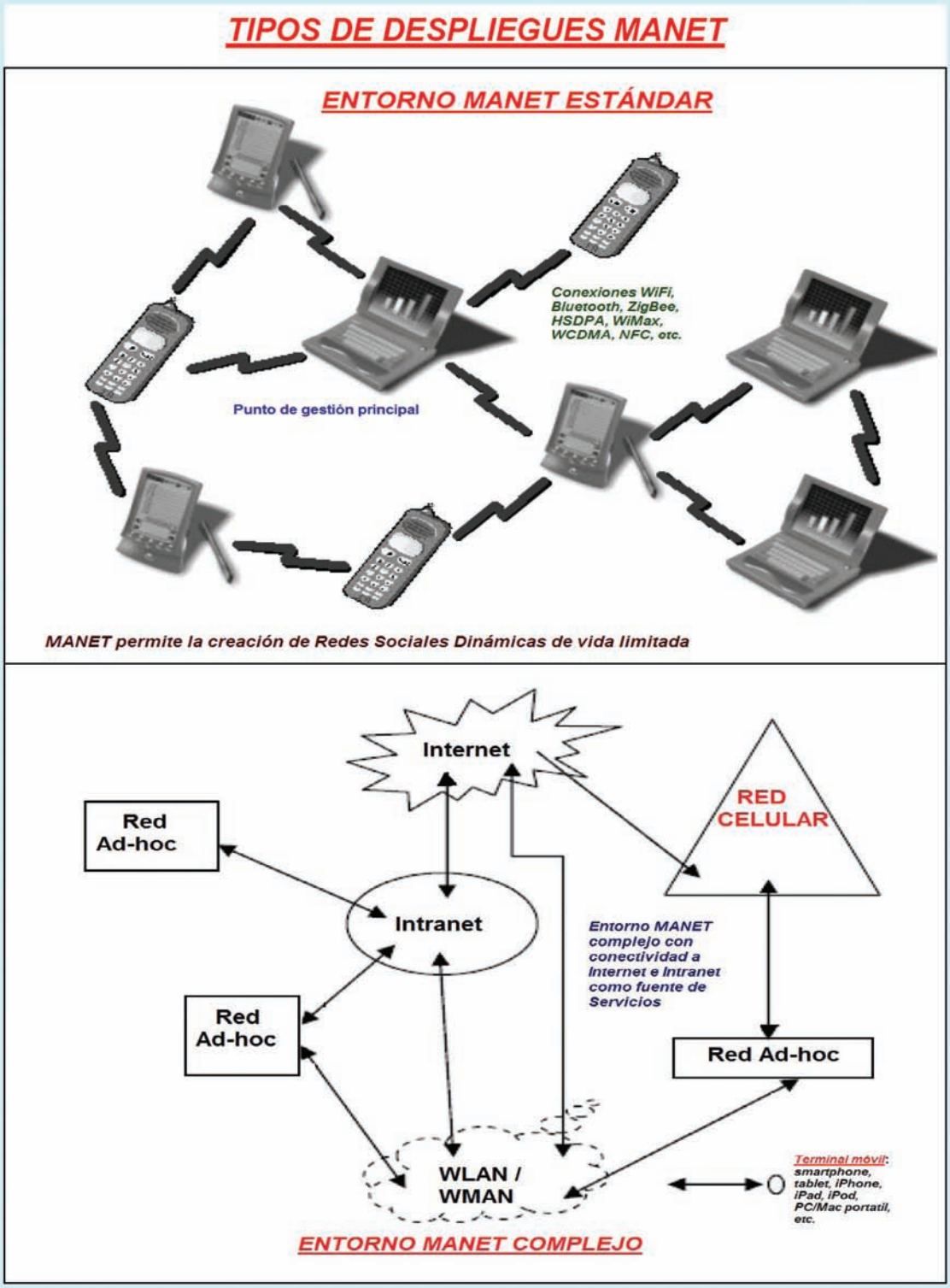


Fig. 5.- Tipos de despliegues MANET.

de ruta de los protocolos de routing del tipo bajo demanda. Los paquetes de petición de ruta se envían con rapidez hacia el destino aumentando la probabilidad del nodo malicioso de estar en la ruta seleccionada.

(d) DoS a nivel de transporte (L4). Dos técnicas utilizadas son: (1) SYN flooding. Un nodo envía múltiples paquetes SYN a otros nodos con una dirección de retorno falsa, de modo que no se completa el 3WHS (3 Way HandShaking), que es la fase uno de tres del protocolo orientado a la conexión TCP de la capa de transporte. Esto causa que las víctimas almacenen cantidades elevadas de conexiones medio-abiertas, de modo que eventualmente no puedan aceptar nuevas conexiones legítimas. Este ataque puede mitigarse aumentando el número de slots para conectarse (backlog queue) y mediante syn cookies. (2) El ataque black hole. Un atacante reemplaza la víctima después del establecimiento de

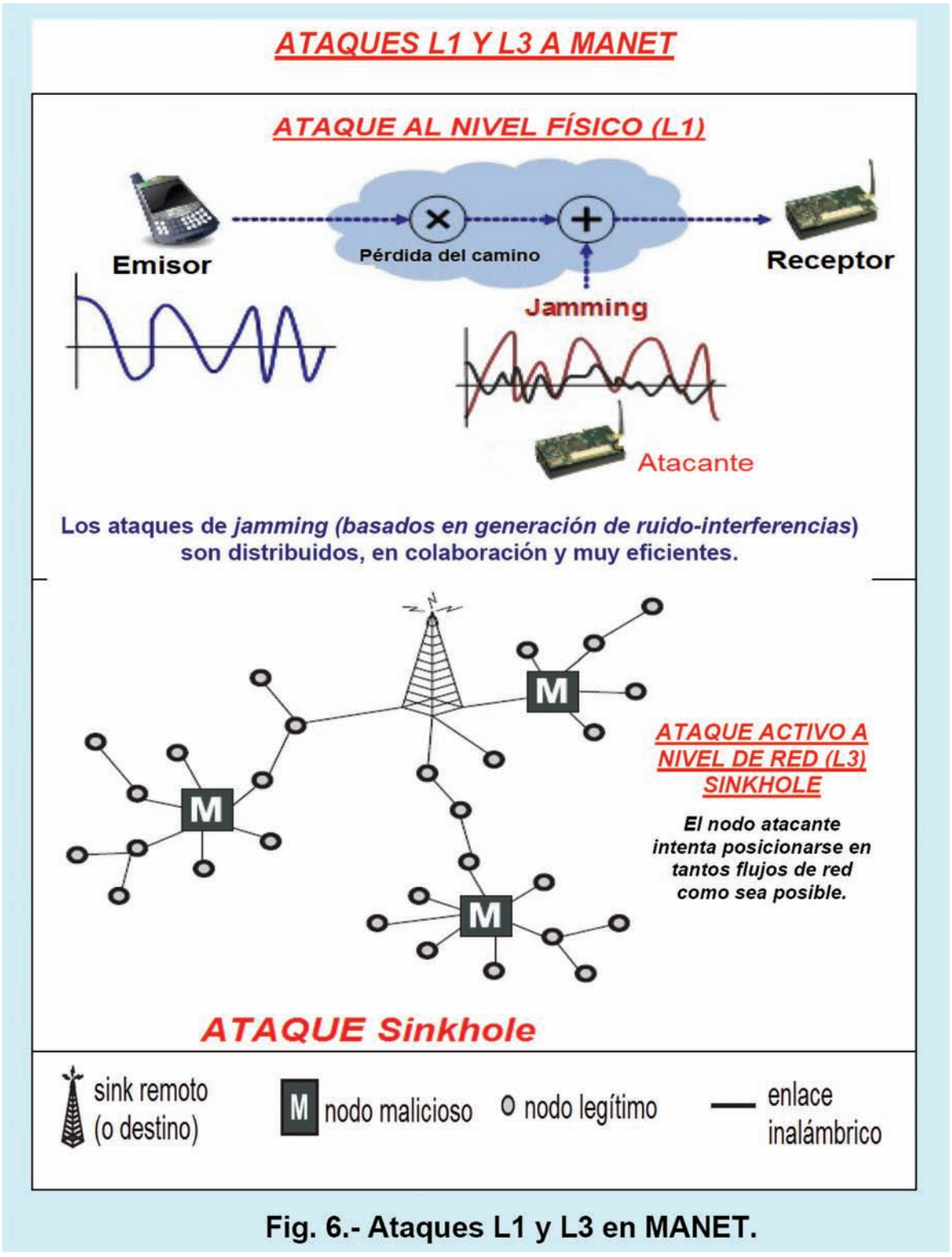


Fig. 6.- Ataques L1 y L3 en MANET.

la sesión (cuando las credenciales se han intercambiado) y continúa la comunicación no detectándose nada por parte del otro nodo. (3) Ataque MITM.

(iv) Ataques criptográficos. La criptografía normalmente se utiliza como elemento de securización y se utilizan primitivas criptográficas como: (a) Generadores de números pseudo-aleatorios (PRNGs). Los números pseudoaleatorios se emplean para muchas tareas como nonces (valores criptográficos efímeros de un solo uso), IVs (vectores de inicialización para mecanismos de cifrado). Sin embargo, se diseñan normalmente para propósitos estadísticos y la semilla puede obtenerse si se observan suficientes números. Sólo los PRNGs robustos deberían ser utilizados para propósitos de seguridad en MANET. (b) Firmas digitales. Los esquemas criptográficos utilizan firmas digitales para autenticar mensajes y proteger su integridad. Se usan RSA-CRT y ECC debido al uso de CPUs débiles.

Dependiendo del tipo de esquema, los mensajes firmados conocidos pueden repetirse, las firmas antiguas pueden añadirse a mensajes falsificados. (c) Gestión de claves criptográficas. Las claves criptográficas pueden ser manejadas de forma no segura durante su generación, compartición, almacenamiento, etc. Los ataques destinados a obtener las claves puede realizarse en estas fases (en una MANET no suele haber una autoridad central de confianza).

Mecanismos y contramedidas seguridad-privacidad para MANET

Para implantar seguridad en MANET se deben utilizar estrategias y tecnologías bien gestionadas: (1) Debe existir algún mecanismo para descubrir la ruta correcta. (2) La topología de red debería ser confidencial. (3) Ser capaz de detectar nodos maliciosos. (4) Utilizar cripto-sistemas simétricos y asimétricos (de bajo peso como ECC, RSA basado en CRT, etc.) y mantener la clave pública en secreto. (5) Implantar la gestión de claves criptográficas mediante criptografía umbral (tipo Shamir), sistema de grupo basado en contraseñas y gestión de claves públicas auto-organizadas. (6) Proteger la privacidad mediante una estructura basada en un continuo cambio de pseudónimos y PET. (7) Determinar el punto de ruptura en una red utilizando técnicas de localización de fallos y senseo de QoS. (8) Recoger medidas extremo a extremo de los caminos más largos analizando las medidas de pérdidas y retardo. (9) Reenviando paquetes seguros en los que cada nodo tiene la función de mantener en observación a sus vecinos. (10) Utilizar dispositivos de confianza en vez de una infraestructura de pre-distribución de claves criptográficas del propietario. (11) Aplicar la cooperación basada en token en la que se exija los tokens para poder participar en la red.

Patrones de movimiento en redes AD-HOC.

Se pueden identificar entre otros los siguientes modelos de movilidad para redes MANET: (1) RPG (Referente Point Group). Se basa en grupos de dispositivos que se comportan de forma similar. En este caso, los dispositivos se dividen en grupos de igual tamaño (o a veces distinto). Cada grupo tiene un centro lógico que define los patrones de movimiento para todo el grupo, es decir su velocidad, aceleración y dirección. Cada miembro del grupo se coloca de forma aleatoria en la vecindad de su punto de referencia, relativa al centro del grupo. Esto permite que las posiciones relativas de los dispositivos dentro del grupo cambien con el tiempo. El centro del grupo selecciona de forma aleatoria destinos dentro del área de operación y se mueva hacia dichos destinos. Todos los dispositivos del grupo siguen el movimiento del centro y añaden desplazamientos aleatorios a su punto de referencia dentro del grupo. (2) RW (Random Walk). Se basa en entidades o dispositivos que se comportan de forma independiente. En este caso, un dispositivo elige un destino aleatorio dentro del área de operación y se mueve hacia ella. Una vez que el dispositivo llega a su destino, de forma aleatoria elige un nuevo destino y comienza a moverse hace él. Un ejemplo de este tipo de patrón de movimiento puede ser la movilidad en el campo de batalla de los militares. (3) TVU (Time-Varying User). Se basa en grupos de dispositivos que se comportan de forma similar. Se basa en el comportamiento que se da en las redes inalámbricas de las redes de campus universitarios, se observan dos tendencias: la preferencia de visitar una localización y la re-aparición periódica. Se caracteriza por definir zonas frecuentemente visitadas. Cada dispositivo se asigna de forma aleatoria a una zona. Se definen dos períodos de tiempo: el período de movimiento normal y el de concentración, en este último un dispositivo visita su zona con mucha probabilidad. Cada dispositivo tiene dos modos de movimiento: local y de itinerancia. En el local la movilidad del dispositivo se centra dentro de su zona. En el de itinerancia, un dispositivo puede moverse libremente dentro de toda el área de operaciones. Cada dispositivo cambia el modo de movimiento de forma aleatoria.

Categorías de protocolos de routing para MANET.

Los protocolos de routing para MANET pueden clasificarse en las siguientes categorías: (1) Protocolos proactivos (o conducidos por tabla). Determinan las rutas de forma independiente del patrón de tráfico. Los protocolos tradicionales de routing de estado del enlace y de vector distancia son proactivos. Este tipo de protocolos, mantienen la ruta constantemente actualizada. Frecuentemente mantienen listas de destinos y rutas distribuyendo todas las tablas de routing por la red. Las rutas se establecen en base al tráfico de control continuo y siempre están disponibles. Las principales deficiencias son la baja reacción a la hora de la reestructuración y malfuncionamiento y el costo-gasto (ancho de banda, tiempo) creado por el tráfico de control. Ejemplos de estos protocolos son DSDV (Destination Sequenced Distance Vector), OLSR (Optimized Link State Routing-IETF-RFC3626), FSR (Fisheye State Routing) y TBRPF (Topology Broadcast based on Reversed Path Forwarding). (2) Protocolos reactivos (o bajo demanda). Son los más populares. Mantienen las rutas sólo si es necesario. Este tipo de protocolos reacciona bajo demanda inundando con una query. Determina la ruta siempre y cuando se necesita. La fuente inicia el proceso de encontrar la ruta. Consecuentemente el costo del routing es menor pero el retardo del descubrimiento de la ruta es mayor. Excesivas inundaciones pueden causar que la red se atasque. No obstante se ha demostrado que para algunas MANET es un protocolo eficiente. Ejemplos de dichos protocolos de routing son: AODV (Ad-hoc On-demand Distance Vector-IETF-RCF3561), LMR (Lightweight Mobile Routing), TORA (Temporally Over Routing Algorithm) y ABR (Associativity Based Routing). En los protocolos de routing bajo demanda las rutas se mantienen sólo entre los nodos que necesitan comunicarse. Las RREQ (Route Request) se envían por inundación a través de la red. Cuando un nodo re-difunde RREQ establece un camino inverso señalando hacia la fuente. Cuando el destino recibe un RREQ responde enviando un RREP (Route Replay). El RREP viaja por el camino inverso establecido cuando el RREQ se reenvió. (3) Protocolos que utilizan información de localización geográfica. Suponen que cada nodo esta equipado con uno o varios mecanismos de localización-posicionamiento como GPS (Global Positioning System), GALILEO (Europeo), GLONASS (Rusia), QZSS (Japón). Ejemplos de dichos protocolos de routing son: LAR (Location Aided Routing), DREAM (Distance Routing Effect Algorithm for Mobility), GPSR

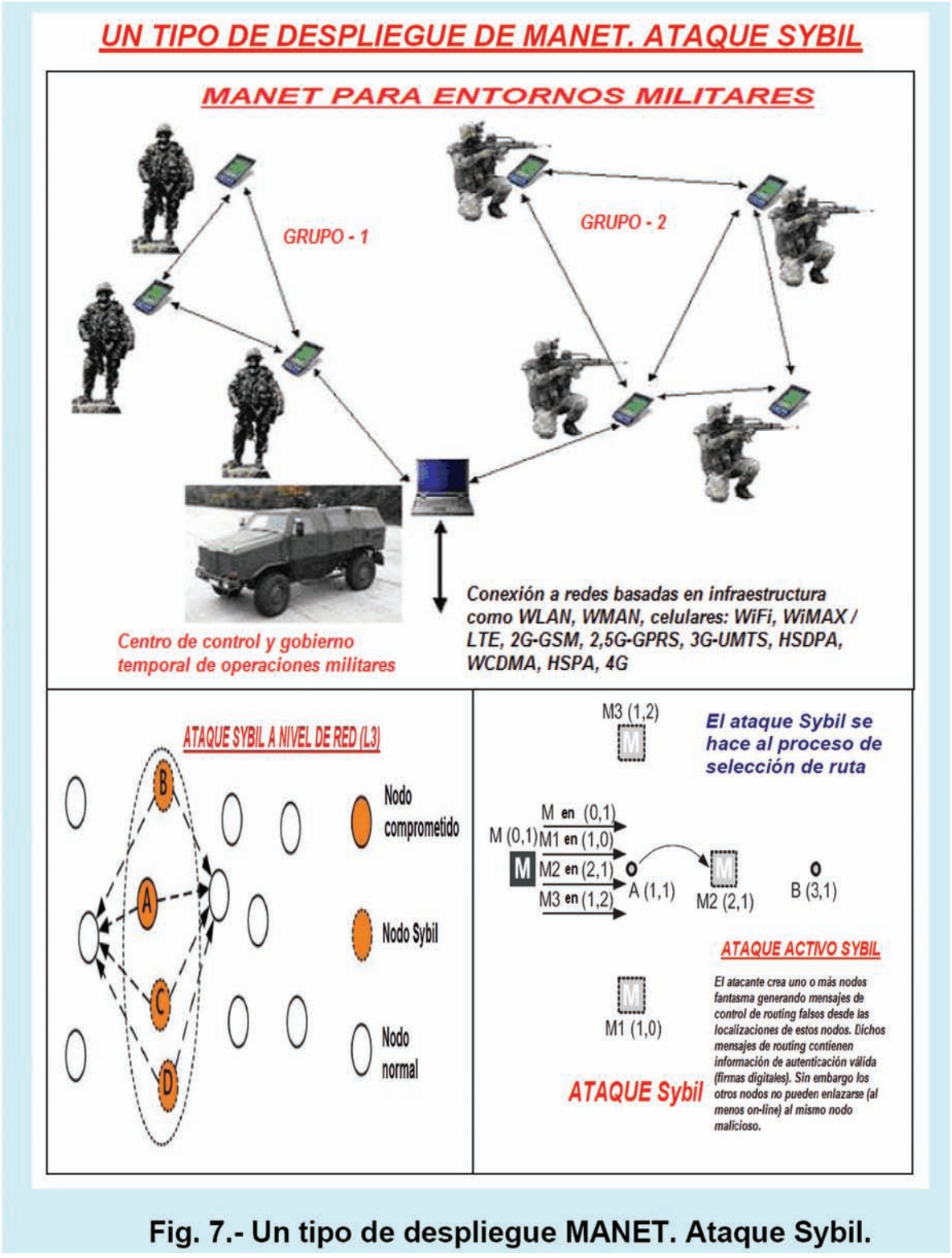


Fig. 7.- Un tipo de despliegue MANET. Ataque Sybil.

(Greedy Perimeter Stateless Routing) y GeoCast (Geographic addressing and routing). (4) Protocolos híbridos. Es una combinación de ciertas características de los protocolos anteriores. Un ejemplo es ZRP (Zone Routing Protocol) que mezcla aspectos de protocolos reactivos y proactivos. Los protocolos bajo demanda son susceptibles a ataques como Sybil, Wormhole, Sink hole, inundación Hello, rushing, inundación RREQ e información de routing falsa. Los protocolos conducidos por tabla son bastante inmunes a los ataques rushing e inundación RREQ. Ver: http://www.ietf.org/html.charters/manet-charter.html

Consideraciones finales.

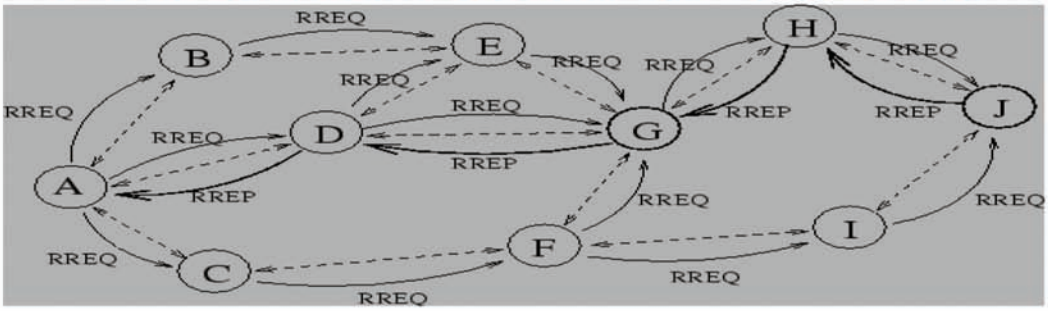
Nuestro grupo de investigación lleva trabajado más de quince años sintetizando, analizando, desarrollando y evaluando entornos de red MANET protegidos desde la seguridad y priva-

MECANISMO DE FIRMA DIGITAL NO NEGABLE PARA MANET

- Una *firma digital no negable* es aquella que sólo puede ser verificada por B con el consentimiento expreso del firmante A. Previene que B pueda verificar la validez de una firma de A a menos que el firmante A lo desee.

- **GENERACIÓN DE CLAVES PÚBLICA-PRIVADA DE LA ENTIDAD QUE FIRMA A:**
  - La entidad A selecciona y los hace públicos un número primo grande p escogido de forma aleatoria y un *generador* o elemento primitivo g de GF(p). Sean por ejemplo p = 13 y g = 3.
  - La entidad A selecciona un *clave privada* x y obtiene la *clave pública* $K = g^x \bmod p$. Sean por ejemplo x = 5 y $K = 3^5 \bmod 13 = 1$.
- **PROCESO DE GENERACIÓN DE LA FIRMA EN LA ENTIDAD A SOBRE EL MENSAJE M:**
  - Sea M el mensaje/documento a firmar. Por ejemplo M = 2. La entidad A calcula la *firma*: $z = M^x \bmod p$. En este caso: $z = 2^5 \bmod 13 = 6$.
- **PROCESO DE VERIFICACIÓN. COLABORAN LAS DOS ENTIDADES: LA ENTIDAD B VERIFICADORA Y LA ENTIDAD FIRMANTE A:**
  - La entidad B selecciona dos valores aleatorios secretos a, b pertenecientes a GF(p) y envía a la entidad A el valor: $c = z^a (g^x)^b \bmod p$. Sean por ejemplo: a = 2, b = 3, entonces: $c = 6^2 (3^5)^3 \bmod 13 = 10$.
  - La entidad A calcula primero: $t = x^{-1} \bmod (p - 1)$ luego: $d = c^t \bmod p$ y le envía a la entidad B el valor d. En este caso: $t = 5^{-1} \bmod 12 = 5$; $d = 5^5 \bmod 13 = 4$.
  - La entidad B verifica la firma y la da como válida si se cumple la siguiente igualdad: el valor d recibido debe ser igual a: $(M^a . g^b) \bmod p$. En este caso: $d = (M^a . g^b) \bmod p$ ya que: d = 4 y $(2^2 . 3^3) \bmod 13 = 108 = 4$, luego: 4 = 4.

PROTOCOLO DE ROUTING AODV - RFC3561



Un posible camino para una RREP si la estación A desea encontrar una ruta con el dispositivo J.

Fig. 8.- Mecanismo de firma digital no negable para MANET y ruta AODV.

cidad. Los smatphones y tablets son ya elementos de computación-comunicación claves y de utilización masiva en empresas donde se demanda un acceso móvil seguro para las aplicaciones y recursos de negocio críticos independientemente donde se encuentren sus empleados y de la hora que operen. La seguridad en redes móviles ad-hoc se ha hecho extremadamente importante. Es urgente mitigar los posibles ataques y abordar profesionalmente cuestiones de seguridad críticas como detección de nodos maliciosos, el control de acceso, la autenticación mutua multifactor (de seis factores: saber-contraseña, reconocer-fotos, tener-tarjeta, fisiológicos-biometría, de comportamiento-biometría, de geolocalización-lugar, temporales-fecha-hora), sensores de detección-prevención de intrusiones, privacidad-anonimato, verificación de la localización-posicionamiento, etc.

Bibliografia

-Areitio, J. "Seguridad de la Información: Redes, Informática y Sistemas de Información". Cengage Learning - Paraninfo. 2012.

-Areitio, J. "Identificación, análisis y evaluación de la seguridad en las comunicaciones con tecnología ZigBee". REE. Nº 682. Septiembre 2011.

-Areitio, J. "Análisis en torno a las tecnologías de privacidad en redes. Anonimato en transmisión de datos". REE Nº 660. Noviembre 2009.

-Areitio, J. "Test de penetración y gestión de vulnerabilidades, estrategia clave para evaluar la seguridad de red". REE Nº 653. Abril 2009.

-Paar, C., Westhoff, D., Claude, C. and Hartenstein, H. "Security in Ad-Hoc and Sensor Networks". Springer. 2005.

-Xiao, Y., Shen, X. and Du, D-Z. "Wireless Network Security". Springer. 2010.

-Cayirci, E. and Rong, C. "Security in Wireless Ad Hoc and Sensor Networks". Wiley. 2009.

-Beyah, R., Mcnair, J. and Corbett, C. "Security in Ad Hoc and Sensor Networks". World Scientific Publishing Company. 2009.

-Pathan, A-S. K. "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET". Auerbach Publications. 2010.

-Anjum, F. and Mouchtaris, P. "Security for Wireless Ad Hoc Networks". Wiley-Interscience. 2007.

-Makki, S.K., Reiher, P., Makki, K., Pissiou, N. and Makki, S. "Mobile and Wireless Network Security and Privacy". Springer. 2010.

-Zheng, J., Simplot-Ryl, D. and Leung, V.C.M. "Ad Hoc Networks". Springer. 2011.