UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

MODALIDAD ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

SERVICIOS DE AUTENTICACIÓN Y MODELO DE SEGURIDAD EN REDES MÓVILES AD HOC

Trabajo de Tesis previo a la obtención
del título de Ingeniero en Informática

Autor:

Jaramillo Falconí Sebastián Mateo

Director :

Ing. Torres Tandazo Rommel Vicente

SAN RAFAEL

2010

Ing.
Rommel Torres
DIRECTOR DE TESIS

CERTIFICA:

Que la Sr. Sebastián Mateo Jaramillo Falconí, autor de la tesis "**SERVICIOS DE AUTENTICACIÓN Y MODELO DE SEGURIDAD EN REDES MÓVILES AD HOC**", ha cumplido con los requisitos estipulados en el Reglamento General de la Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo desde su inicio hasta la culminación, por lo cual autorizo su presentación.

Loja, 30 de Agosto del 2010

- - - - - - - - - - - - - - -
Ing. Rommel Torres
DIRECTOR DE TESIS

CESIÓN DE DERECHOS

Yo, **Sebastián Mateo Jaramillo Falconí,** declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja, que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad".

_____

Sebastián Mateo Jaramillo F.

AUTORÍA

Las ideas, opiniones, conclusiones, recomendaciones y más contenidos expuestos en el presente informe de tesis son de absoluta responsabilidad de los autores.

_____

Sebastián Mateo Jaramillo F.

AGRADECIMIENTO

Agradezco a la Energía Suprema Universal el haber dirigido las acciones que derivaron en este trabajo.

A mis padres por su constante apoyo y cariño en todo momento y lugar.

A mi familia y amigos por su entusiasmo.

A mis directores de tesis sin los cuales este proyecto no se habría cristalizado.

A la Universidad Técnica Particular de Loja por su calidad y prestigio académico.

ABSTRACT

Una red Ad Hoc Móvil es una red auto organizada sin infraestructura fija y de múltiples saltos. La naturaleza de este tipo de redes constituye un gran desafío al momento de diseñar una infraestructura de seguridad que brinde los recursos necesarios que generen un nivel de confianza dentro de las limitaciones existentes. En los últimos años los temas de seguridad han atraído la atención de los investigadores, sin embargo; los esfuerzos de investigación se han enfocado en soluciones aisladas o exclusivas de una capa. Las propuestas de arquitecturas en varias capas son mínimos y poco difundidos, sin embargo confiamos que un modelo de seguridad debe aplicarse a varios niveles, es por ello que proponemos un modelo de seguridad por capas desde el nivel de enlace de datos hasta el nivel de aplicación, orientado a redes militares y civiles con considerables niveles de amenaza implícitos.

TABLA DE CONTENIDO

CAPITULO I

1. Redes MANET (Mobile Ad Hoc Networks) y aplicaciones

1.1. Introducción

Una red MANET (Mobile Ad Hoc Network), algunas veces llamada red de malla o mesh network, es una red auto configurable de dispositivos móviles conectados por enlaces inalámbricos [1]. Cada dispositivo es libre de moverse independientemente en cualquier dirección, de esta manera cambia sus enlaces hacia otros dispositivos de manera frecuente. Cada dispositivo deberá funcionar como enrutador reenviando el tráfico no relacionado con su propio uso. El reto principal al construir una red de estas características, es dotar a cada dispositivo para que continuamente mantenga la información de enrutamiento requerida para que contribuya con el manejo del tráfico de manera apropiada. Las principales características de este tipo de redes son topología dinámica, enlaces de ancho de banda limitado y de capacidad variable, limitaciones de energía, capacidad de procesamiento y características de seguridad limitadas. Algunas aplicaciones de la tecnología MANET, incluyen aplicaciones comerciales e industriales con intercambio cooperativo de datos móvil. Adicionalmente, las redes móviles basadas en malla pueden operar como una alternativa económica y robusta o como mejoramiento a infraestructuras móviles basadas en celdas. Existen requerimientos de robustez, compatibilidad IP para servicios de datos en redes militares, servicios de emergencia, control de tráfico, asistencia remota, etc. En este tipo de redes donde no se tiene una infraestructura fija disponible, es necesario reforzar los mecanismos de autenticación utilizando estrategias diferentes que se ajusten a las necesidades y características de este tipo de red y de este modo contribuir a la seguridad de la red y la confianza en los usuarios.

Publicaciones derivadas de la presente investigación SERVICIOS DE AUTENTICACIÓN Y MODELO DE SEGURIDAD EN REDES MÓVILES AD HOC, enviada el 3 de Mayo del 2010 al III Congreso de Redes CITIC que tuvo lugar en la ciudad de Quito los días 7, 8 y 9 de Julio de 2010. El documento enviado estuvo entre las ponencias aceptadas. Revisar ANEXOS.

1.2. Ejemplos de aplicación

1.2.1. Despliegue Temporal de Redes

En escenarios donde no es factible montar una infraestructura de red por limitaciones en costos o por condiciones del ambiente. Por ejemplo en conferencias o eventos temporales o labores de investigación de campo es donde estas redes tienen aplicación directa.

1.2.2. Operaciones de Asistencia en Desastres

La capacidad de despliegue rápido y oportuno en situaciones de crisis, como desastres naturales, convierte a las redes Ad Hoc en la tecnología ideal en el manejo y asistencia de desastres.

1.2.3. Aplicaciones Militares

Por las características de movilidad y autoconfiguración estas redes pueden aplicarse en escenarios de combate, actividades de reconocimiento e inteligencia, sin embargo las características de seguridad actuales limitan la puesta en operación efectiva en estos escenarios.

1.3. Enrutamiento en Redes MANET

1.3.1. Enrutamiento Proactivo (manejado por tablas)

Este tipo de protocolos [2] mantienen listas actualizadas de destinos y sus rutas a través de la distribución periódica de tablas de enrutamiento a través de la red. Las principales desventajas de tales algoritmos son:

1. La correspondiente cantidad de datos para mantenimiento.
2. Reacción lenta en reestructuración y fallas.

Algunos ejemplos de este tipo de protocolos son los siguientes.

- AWDS (Ad Hoc Wireless Distribution Service).

- DSDV (Highly Dynamic Destination-Sequenced Distance Vector Routing Protocol).
- MMRP (Mobile Mesh Routing Protocol).
- OLSR (Optimized Link State Routing Protocol).
- TBRPF (Topology Dissemination based on Reverse-Path Forwarding routing Protocol).
- WRP (Wireless Routing Protocol).

1.3.2. Enrutamiento Reactivo (Bajo Demanda)

Este tipo de protocolos encuentran una ruta bajo demanda inundando la red con paquetes de búsqueda de rutas. Las principales desventajas de tales algoritmos son:

1. Tiempo de latencia alto en la búsqueda de rutas.
2. Una inundación excesiva puede llevar a la obstrucción de la red.

Ejemplos de estos algoritmos son los siguientes:

- AODV (Ad Hoc On Demand Distance Vector routing protocol).
- DSR (Dynamic Source Routing).
- DYMO (Dynamic Manet On-Demand Routing).

1.4. Desafíos de seguridad

1.4.1. Introducción

El tema de seguridad en redes de este tipo constituye un gran desafío, ya que involucra la aplicación y el estudio de nuevos modelos que sustenten la vulnerabilidad al acceso en redes dinámicas de este tipo. Esta característica propia de estas redes, provoca un problema de seguridad fundamental que es la red abierta para el libre ingreso de los nodos que pasan a formar parte de la infraestructura. Es por ello fundamental la implementación de algoritmos de

autenticación y sistemas de cifrado para proteger la confidencialidad de los datos del usuario que atraviesan por los diversos medios y tecnologías que constituyen una red de estas características.

Los requisitos de seguridad en una red móvil Ad Hoc son los mismos que los existentes en redes cableadas tradicionales, y son: confidencialidad, integridad, autenticación, no repudiación y disponibilidad. Sin embargo, las características generales de una MANET hacen que el cumplimiento de los requisitos anteriores sea un problema mucho más complejo de abordar, mostrando la dificultad de diseñar una solución general en términos de seguridad sobre un escenario móvil Ad Hoc [3].

Los principales desafíos de seguridad que enfrentan las redes MANET, incluyen los siguientes:

- Compromiso de los nodos colaboradores en la red, y pueden darse por robo, secuestro, destrucción de los nodos que se suman y colaboran con las funciones de enrutamiento de la red.
- Ataques activos y pasivos hacia los nodos, los mismos que provocan problemas generales a toda la red.
- Nodos con comportamiento indeseable por falta de cooperación, los mismos que constituyen ataques internos.

1.5. Ataques en contra de la Seguridad

1.5.1. Introducción

Los ataques de seguridad ante los cuales están expuestos los protocolos de enrutamiento en una red Ad Hoc, son de dos tipos. *Ataques activos a través de los cuales los nodos con mal comportamiento (misbehaving nodes) tienen que cargar con algunos costos energéticos con el fin de realizar alguna operación dañina. Los ataques pasivos por otro lado, consisten principalmente en falta de cooperación con el propósito de ahorrar energía.* Los nodos que realizan ataques activos con el objetivo de causar daño a otros nodos son considerados como *maliciosos* mientras que los nodos que realizan ataques pasivos se los considera como *egoístas (selfish).* Los

nodos maliciosos pueden interrumpir el normal funcionamiento de los protocolos de enrutamiento, modificando la información de rutas, fabricando información falsa o suplantando a otros nodos. Como se observa en la figura 1.5.1.1 se ha hecho una clasificación de los ataques más comunes, resumen realizado a través del análisis de varios autores, este esquema está basado en el modelo de referencia OSI aplicado a redes MANET.

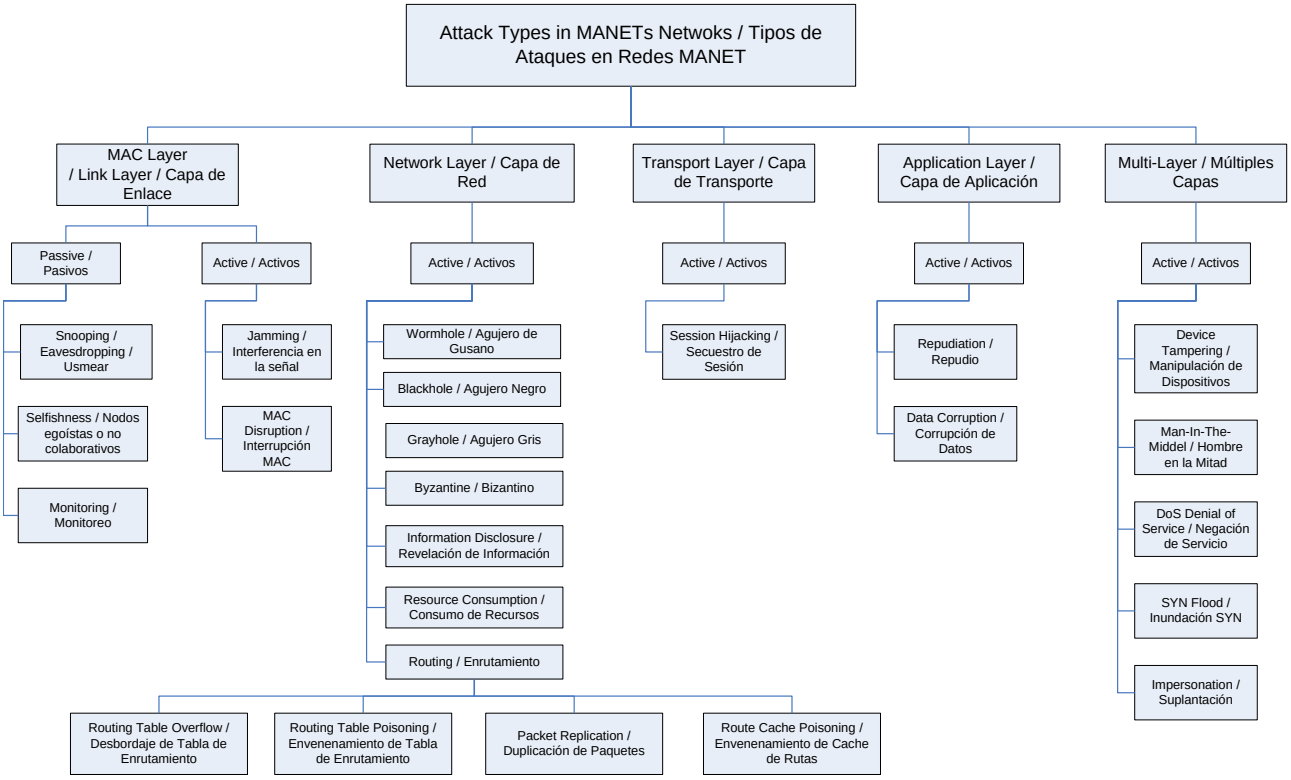

Figura 1.5.1.1 Tipos de Ataques en Redes MANET

1.5.2. Ataques Activos

En [14] se analizan varios tipos de ataques y se realiza una clasificación de los mismos. A continuación se revisan cada uno de ellos.

1.5.2.1. Ataques que Utilizan Modificación

Los ataques que utilizan modificación, tienen como objetivo la alteración de la información de enrutamiento, como por ejemplo, la modificación de mensajes

de actualización de ruta. A continuación se mencionan una serie de ataques a los cuales están expuestos los protocolos AODV y DSR, ya que estos dos protocolos se han propuesto como estándar por la IETF, sin embargo tiene serias deficiencias de seguridad.

1.5.2.2. Redirección modificando los Números de Secuencia de Ruta

Los protocolos tales como AODV asignan cierto valor a las rutas hacia las rutas de un destino específico para decidir la prioridad. Una ruta con un valor mayor es preferida, por lo tanto un nodo puede cambiar el tráfico sobre sí mismo anunciando una ruta hacia un nodo con un valor mayor.

1.5.2.3. Redirección con Conteo de Saltos Modificado

Sin contar con otra métrica, AODV usa el campo de conteo de saltos para determinar el camino más corto. Un nodo malicioso puede reiniciar el campo de conteo de saltos del mensaje RREQ a cero, lo que incrementas las oportunidades de que sea incluido en la ruta de reciente creación. De manera similar los nodos maliciosos pueden evitar ser incluidos dentro de las rutas creadas estableciendo el valor de conteo de saltos del mensaje RREQ hacia el infinito.

1.5.2.4. Negación de servicio con Rutas Fuente Modificadas

DSR utiliza rutas fuente iniciando estas en paquetes de datos. Estas rutas carecen de revisión de integridad. Por lo tanto los ataques de negación de servicio son posibles y pueden alterar las rutas fuente en los encabezados de los paquetes los que evita que el paquete sea enviado hacia su destino.

1.5.2.5. Ataques que utilizan Suplantación

Cuando un nodo tergiversa su identidad en red, ya sea a través de una alteración en su dirección MAC o IP en los paquetes salientes, la suplantación puede tener lugar. Este puede modificar el enraizamiento de algunos nodos lo que puede provocar bucles en la red lo que incrementara en gran medida el consumo de energía.

1.5.2.6. *Ataques que utilizan Fabricación de errores*

Este tipo de ataques generan falsos mensajes de enrutamiento los cuales pueden ser difíciles de distinguir construcciones inválidas. En los ataques de tipo fabricación, un intruso genera falsos mensajes de enrutamiento, tales como actualizaciones de enrutamiento, con el fin de perturbar la operación de la red o consumir los recursos de otros nodos.

1.5.2.7. *Falsificando Errores de ruta en AODV y DSR.*

En AODV y DSR, si un nodo destino o un nodo intermedio que se encuentra a lo largo del camino se mueve, el nodo ascendente rompe la difusión de mensajes de error hacia todos los vecinos. Este mensaje causa que la correspondiente ruta sea inválida. Un ataque de negación de servicio puede tener lugar enviando mensajes de error que indiquen un enlace roto evitando de este modo la comunicación entre la fuente y el destino.

1.5.2.8. *Envenenamiento de Cache en DSR*

Un nodo a la escucha puede añadir información de enrutamiento contenida en el encabezado del paquete hacia su propio cache de rutas. Un atacante puede explotar este método de aprendizaje de modificación de caches de ruta, transmitiendo paquetes que contienen rutas inválidas en sus encabezados.

1.5.2.9. *Ataque de consumo de recursos*

En este ataque, un nodo malicioso deliberadamente intenta consumir los recursos de otros nodos, tales como, batería, ancho de banda, etc. Los ataques pueden ser en la forma de mensajes de control de petición de ruta innecesarios, muy frecuente generación de paquetes beacon, o reenvío de información caduca a los nodos.

1.5.2.10. *Ataque al Apuro (Rushing Attack)*

Los protocolos de enrutamiento bajo demanda como AODV son vulnerables a este tipo de ataques. Un nodo atacante que recibe un RREQ desde el nodo

fuente, inunda con este paquete rápidamente a la red, antes de que otros nodos que reciben la misma petición puedan reaccionar. Los nodos que reciben el legítimo RREQ asumen que esos paquetes son duplicaciones del paquete previamente recibido por el atacante y por lo tanto son eliminados. Cualquier ruta descubierta posteriormente por el nodo fuente contendrá al nodo atacante como uno de los nodos intermedios. Por lo tanto el nodo fuente no será capaz de encontrar rutas seguras.

1.5.2.11. Ataque de Agujero Negro (Black Hole Attack)

En este tipo de ataques, un nodo malicioso publica falsamente un buen camino hacia el destino durante el proceso de búsqueda de caminos. La intención de los nodos maliciosos podría ser la obstaculización en el proceso de búsqueda o la interrupción de que los paquetes de datos sean enviados hacia el nodo interesado.

1.5.2.12. Ataque de Agujero Gris (Grey Hole Attack)

El ataque Grey Hole tiene dos fases. En la primera fase, un nodo malicioso explota al protocolo AODV para publicarse el mismo como poseedor de una ruta valida hacia el destino, con la intención de interceptar paquetes, a pesar de que la ruta sea falsa. En la segunda fase, el nodo echa los paquetes interceptados con una cierta probabilidad. Este ataque es más difícil de detectar que el de agujero negro, donde el nodo malicioso echa los paquetes recibidos con total certeza. Este ataque puede exhibir su comportamiento malicioso de maneras diferentes. Este puede echar los paquetes que vienen de o están destinados hacia cierto nodo específico en la red mientras reenvía los paquetes de otros nodos. Otro tipo de Grey Hole puede comportarse maliciosamente por cierto periodo de tiempo, echando paquetes y luego cambiar su comportamiento a normal. Un ataque Grey Hole puede también exhibir un comportamiento que es una combinación de los otros dos lo que lo vuelve aún más difícil de detectar.

1.5.2.13. *Ataque de Agujero de Gusano (Wormhole Attack)*

En un ataque de agujero de gusano, un atacante recibe paquetes en un punto de la red, luego ejecuta una construcción de un túnel enviando estos paquetes hacia otro punto en la red, y luego los vuelve a poner en la red desde ese punto. Para unas distancias de túnel mayores que las de la transmisión inalámbrica normal de un salto simple, es sencillo para el atacante hacer que el paquete del túnel llegue con mejor métrica que en la métrica de la ruta multisalto, por ejemplo se puede usar un enlace inalámbrico de alto rango o un enlace cableado directo hacia otro atacante cómplice del primero. También existe la posibilidad de que el atacante reenvíe cada bit a través del agujero de gusano de manera directa, sin tener que recibir el paquete completo antes de enviar los bits del paquete por el túnel, evitando de este modo el retardo producido por el agujero de gusano. Debido a la naturaleza de la transmisión inalámbrica, el atacante puede crear un agujero de gusano incluso para paquetes no direccionados hacia el mismo. Si el atacante realiza su túnel honesta y confiablemente, ningún daño es causado, el atacante en realidad provee un servicio muy útil y más eficiente a la conexión de la red. Sin embargo, el agujero de gusano pone al atacante en una posición muy ventajosa en relación a los otros nodos de la red, el atacante puede utilizar esta ventaja en una gran variedad de formas. El ataque puede ser perpetrado incluso si la comunicación de la red provee confidencialidad y autenticidad, incluso si el atacante no posee claves criptográficas. [4]El atacante es invisible en las capas superiores, a diferencia de lo que sucede con un nodo malicioso en protocolo de enrutamiento, el cual puede ser a menudo fácilmente identificado, la presencia del agujero de gusano y los dos atacantes cómplices en cualquier punto final del agujero de gusano no son visibles en la ruta.

Para realizar una clasificación más acorde a la realidad, vamos a considerar la infraestructura por capas fundamentada en el modelo de referencia OSI y en el modelo TCP/IP, así analizamos las amenazas a las que está expuesta la red MANET en varios niveles.

En la tabla 1.5.2.1 se muestran los ataques por capas. Tomado de [5].

OSI	TCP/IP	MANET	Ataques MANET por capa	Ataques MANET multicapa
Capa 7 Aplicación	Aplicación Telnet, FTP, NFS, NIS	Aplicación	Repudiation Data Corruption	Device Tampering Man-in-The-Middle DoS SYN Flood Impersonation Wormhole
Capa 6 Presentación	Sesión RPC			
Capa 5 Sesión	Transporte Sockets/streams – TLI, TCP, UDP			
Capa 4 Transporte		Transporte	Session Hijaking	
Capa 3 Red	Red IP + ARP RARP ICMP	Red	Black Hole Grey Hole Byzantine Information Disclosure Resource Consumption Routing Overflow, Route Table Poisoning Packet Replication Cache Poisoning Selfishness	
Capa 2 Enlace de Datos	Protocolo físico Ethernet TR FDDI PPP	Enlace de datos	Pasivos: Eavesdropping, Selfishness, Monitoring Activos: Signal Jamming, MAC Disruption	
Capa 1 Física	Medio de Transmisión Coax, Fibra, 10 baseT	Física		

1.5.3. Ataques Pasivos

En [6] el autor pone como ejemplo los dos tipos de ataques que se describen brevemente a continuación.

1.5.3.1. Espionaje (Eavesdropping)

Los datos clasificados en líneas de comunicación pueden ser escuchados y en las redes inalámbricas el llevar a cabo esta intervención es más fácil de realizar. Por lo tanto, estas redes son más susceptibles a este tipo de ataques. De manera particular cuando la información es transferida de manera plana sin utilizar mecanismos de encriptación.

1.5.3.2. Análisis de Tráfico

Al igual que en el contenido de paquetes de datos, el patrón de tráfico puede ser también el objetivo de los adversarios. La detección de la estación base, a la cual los nodos se conectan o a las cabezas de clúster cuando se utilizan esos esquemas distribuidos, puede resultar extremadamente útil para que los adversarios realicen un ataque de negación de servicio o realizar un espionaje de los paquetes que atraviesan la red.

1.6. Estrategias Generales de Seguridad

1.6.1. Enrutamiento y Reenvío Seguros

Muchos protocolos de enrutamiento para redes Ad Hoc, tienen vulnerabilidades de seguridad, que los expone fácilmente a una serie de ataques. En este apartado nos enfocaremos en dos de los protocolos que están siendo considerados como estándar por la IETF [13]: AODV [7] y DSR [8].

Los protocolos de enrutamiento seguros actuales propuestos toman en cuenta los ataques externos activos, sin embargo los ataques pasivos internos, y el problema con los nodos egoístas no ha sido tratado. Las propuestas futuras tendrán como prerrequisito fundamental un entorno administrado y caracterizado por alguna infraestructura de seguridad que deberá ser

establecida antes de la ejecución de protocolos de enrutamiento seguros. Las propuestas más significativas para enrutamiento seguro en redes Ad Hoc se muestran a continuación.

1.6.1.1. Ariadne

Los primeros estudios serios de seguridad inician con el protocolo Ariadne propuesto por Hu y otros, el cual es la versión segura del protocolo DSR [9]. Según los autores este protocolo resiste el compromiso de los nodos y cuenta con un esquema altamente eficiente de criptografía simétrica. Además este protocolo no requiere de hardware especial de alta confiabilidad ni de potentes procesadores. Ariadne garantiza que el nodo destino en el proceso de descubrimiento de ruta, puede autenticar al iniciador, también garantiza que el iniciador puede autenticar cualquier nodo intermedio en su camino hacia el destino, el cual está presente en el mensaje RREP, además ningún nodo intermedio puede remover al nodo previo incluido en la lista de los mensajes RREQ o RREP. Al igual que el protocolo SRP, el cual se trata a continuación, Ariadne necesita de algún esquema de autenticación para iniciar. Los esquemas de autenticación empleados por Ariadne son tres: claves secretas compartidas entre todos los pares de nodos, claves secretas compartidas entre los nodos en comunicación combinada con autenticación de broadcast, o a través de firmas digitales. El primero de los tres esquemas es el más eficiente sin embargo requiere de secretos compartidos entre los nodos, lo cual no siempre es posible de establecer [13]. La segunda opción para Ariadne es el esquema de autenticación de TESLA [10], el cual está basado en encriptación asimétrica, lo que requiere una autoridad de certificación o de claves previamente desplegadas. Ariadne hace frente a los ataques realizados por nodos maliciosos que modifican y fabrican información de enrutamiento, es también efectivo frente a ataques de suplantación, y en una versión avanzada hace frente al ataque de agujero de gusano (wormhole attack). Los nodos egoístas no están tomados en cuenta, lo que lo vuelve susceptible a estos ataques. En Ariadne, el mecanismo básico de RREQ es ampliado con ocho campos adicionales

utilizados para proveer autenticación e integridad al protocolo de enrutamiento. Con el propósito de prevenir la inyección de errores de ruta inválidos fabricados dentro de la red por cualquier otro nodo diferente al nodo emisor, que se encuentra especificado en el mensaje de error, cada nodo que encuentra un enlace roto añade información de autenticación TESLA al mensaje de error de ruta. Ariadne también es protegido contra una inundación de paquetes RREQ que pueden llevar hacia el ataque de envenenamiento de cache. Los nodos benignos pueden filtrar los paquetes RREQ falsificados o excesivos utilizando cadenas de descubrimiento de ruta (Route Discovery Chains), un mecanismo para la autenticación el descubrimiento de ruta, que permite a cada nodo tasar el límite de descubrimientos iniciados por cualquier nodo. Ariadne es inmune al wormhole attack solo en su versión avanzada, la que utiliza una extensión llamada TIK (TESLA with Instant Key disclosure) [11] que requiere una sincronización de reloj muy ajustada entre los nodos, es posible detectar anomalías en discrepancias de tiempo causadas por un ataque de este tipo.

1.6.1.2. Secure Routing Protocol (SRP)

Este protocolo propuesto por Papadimitratos y otros [12] fue diseñado como una extensión compatible con una variedad de protocolos de enrutamiento reactivos existentes. SRP combate los ataques que interrumpen el proceso de descubrimiento de ruta y garantiza la adquisición de información topológica correcta. SRP permite al iniciador del descubrimiento de ruta detectar y eliminar réplicas de información falsa. SRP confía en la disponibilidad de una asociación segura SA (Security Association) entre el nodo fuente (S) y el nodo destino (T). La SA puede establecerse mediante un esquema de distribución de claves hibrida basado en claves públicas de las partes en comunicación. S y T pueden intercambiar una clave secreta simétrica ($K_{S,T}$) utilizando las claves públicas de cualquiera de ellos para establecer un canal seguro. S y T pueden después autenticarse mutuamente y autenticar los mensajes de enrutamiento. SRP hace frente a nodos maliciosos no cooperativos capaces de modificar, reenviar y fabricar paquetes de enrutamiento. En el caso puntual del protocolo

DSR, SRP requiere incluir un encabezado de 6 palabras, el cual contiene identificadores únicos los cuales etiquetan el proceso de descubrimiento y el *Message Authentication Code (MAC)* calculado a través del algoritmo de hash acuñado. Con el fin de iniciar una petición de ruta (route request) RREQ, el nodo origen tiene que generar el MAC de todo el encabezado IP, el paquete del protocolo básico RREQ y la clave compartida $K_{S,T.}$ Los nodos intermedios que reenvían el RREQ hacia el destino mide la frecuencia de peticiones recibidas desde sus vecinos, con el fin de regular el proceso de propagación cada nodo mantiene un rango de prioridad que es inversamente proporcional a la tasa de búsquedas. Un nodo que maliciosamente contamina el tráfico de red con mensajes RREQ no solicitados, será servido al último o ignorado, debido a su bajo rango de prioridad. A la recepción de un RREQ, el nodo destino verifica la integridad y autenticidad del RREQ calculando el hash acuñado de los campos solicitados y comparándolos con el MAC contenido en el encabezado de SRP. Si el RREQ es válido, el destino inicia una respuesta de ruta (route reply) RREP usando el encabezado de SRP, de la misma forma en cómo lo hizo el origen en el momento de iniciar la petición. El nodo origen desecha respuestas que no coincidan con los esperados identificadores de consulta y revisa la integridad usando el MAC generado por el destino. La primera versión de SRP es propensa al ataque de envenenamiento de cache de rutas (route cache poisoning). Los autores proponen dos alternativas de diseño de SRP que usa un nodo token de réplica intermedio (Intermediate Node Reply Token) INRT. INRT permite a los nodos intermedios que pertenecen al mismo grupo que comparte una clave común (K_G) para validar el RREQ y proveer de mensajes RREP válidos. SRP también sufre de falta de un mecanismo de validación para el mantenimiento de mensajes de ruta, los paquetes de error en ruta no son verificados. Un nodo malicioso puede dañar solamente las rutas a las cuales pertenece, según los autores este protocolo es inmune a ataques de IP spoofing. SRP es susceptible a ataques de agujero de gusano (wormhole attack) [14].

1.6.1.3. *ARAN (A Secure Routing Protocol for Ad Hoc Wireless Networks)*

El protocolo de enrutamiento seguro propuesto por Sanzgiri y otros [13] fue concebido como un protocolo de enrutamiento bajo demanda o reactivo, el cual detecta y protege contra acciones maliciosas llevadas a cabo por terceras partes en el entorno Ad Hoc, ARAN introduce el manejo de la autenticación, integridad y no repudio como parte de una política mínima para redes Ad Hoc y consiste en un proceso de certificación preliminar, paso obligatorio en la etapa de autenticación y una segunda etapa opcional que provee rutas seguras más cortas. ARAN requiere el uso de un servidor de certificados confiable llamado T. Antes de entrar a la red, cada nodo debe solicitar un certificado firmado por el nodo T. El certificado contiene la dirección IP del nodo, su clave pública, un sello de tiempo (timestamp) de cuando el certificado fue creado y el tiempo en que este expira junto con la firma del nodo T. Todos los nodos se supone deben mantener certificados frescos con el servidor confiable y deben conocer la clave pública de este. La meta de esta primera etapa del protocolo ARAN es para que la fuente verifique que el destino esperado fue alcanzado. En esta etapa, la fuente confía en el destino a elegir el camino de retorno. La fuente inicia el proceso de descubrimiento de ruta difundiendo un paquete RDP (Route Discovery Process) hacia sus vecinos. La segunda etapa del protocolo ARAN garantiza de manera segura que el camino recibido por una fuente que inicia un proceso de descubrimiento de ruta es el más corto. De manera similar a la primera etapa, la fuente difunde un mensaje SPC (Shortest Path Confirmation) hacia sus vecinos. El mensaje SPC es diferente del mensaje RDP solamente en dos campos adicionales que le proveen el certificado al destino y la encriptación al mensaje completo con la clave pública del destino, lo que es una operación costosa. El firmado de los mensajes combinado con la encriptación de los datos previene que los nodos del medio cambien la longitud del camino, porque hacer esto rompería la integridad del paquete SPC. La fase de mantenimiento de ruta del protocolo ARAN es asegurada firmando digitalmente los paquetes de error generados. Sin embargo es extremadamente complicado detectar cuando los mensajes de error son fabricados por los enlaces que están

verdaderamente activos y no se han roto. No obstante como estos mensajes son firmados, los nodos maliciosos no pueden generar mensajes de error de otros nodos. El no repudio provisto por los mensajes de error firmados permite que un nodo sea verificado como la fuente de los mensajes de error que envía. Como en todo sistema basado en certificados criptográficos, el tema de revocación de claves debe tratarse, para asegurar que los certificados expirados o revocados no le permitan a su titular acceder a la red. En ARAN cuando se necesita revocar un certificado, el servidor de certificados confiable T envía un mensaje de broadcast que anuncia la revocación al grupo Ad Hoc. Cualquier nodo que recibe este mensaje lo retransmite hacia sus vecinos. Las notificaciones de revocación necesitan ser almacenadas hasta que el certificado revocado expire normalmente. Cualquier vecino del nodo con el certificado revocado necesita reformar su enrutamiento como sea necesario, con el fin de evitar la transmisión a través del nodo no confiable. Este método no es a prueba de fallos. En algunos casos, el nodo no confiable quien está obteniendo una revocación de su certificado puede ser la única conexión entre dos partes de la red Ad Hoc. En este caso, el nodo no confiable podría no reenviar la notificación de revocación de su propio certificado, resultando en la partición de la red, como los nodos que han recibido la notificación de revocación no reenviarán mensajes a través del nodo malicioso, mientras que todos los otros nodos dependientes de este para encontrar al resto de la red se quedarían incomunicados. Esto dura hasta que el certificado del nodo malicioso pueda ser nuevamente válido, o hasta que este nodo deje de ser la única conexión entre las dos particiones. Al momento en el que el certificado revocado deba haber expirado, el nodo no confiable no será capaz de renovar su certificado, y todo el enrutamiento a través de este nodo termina. Para acelerar la propagación de notificaciones de revocación, cuando un nodo conoce un nuevo vecino, este puede intercambiar un resumen de sus notificaciones con este vecino; si estos resúmenes no coinciden, las verdaderas notificaciones pueden ser reenviadas y retransmitidas para iniciar la propagación de la notificación. El protocolo ARAN protege contra amenazas que utilizan modificación, fabricación y

suplantación, pero el uso de criptografía asimétrica lo vuelve muy costoso en términos de CPU y uso de energía. Además "ARAN no es inmune al ataque de agujero de gusano (wormhole attack)" [14].

1.6.1.4. SEAD (Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks)

Hu y otros [15] presentaron un protocolo de enrutamiento seguro proactivo basado en el Destination-Sequenced Distance Vector protocol (DSDV) [16]. En los protocolos proactivos de este tipo, los nodos periódicamente intercambian información de enrutamiento entre sí con la intención de que cada uno de los nodos conozca siempre la ruta actual hacia todos los destinos. Específicamente SEAD está inspirado en la versión DSDV-SQ del protocolo DSDV. Esta versión se ha demostrado que supera otras versiones e DSDV simulaciones previas de redes Ad Hoc [17] [18]. El principal objetivo de SEAD es evitar que cualquier nodo malicioso publique mejores rutas falsas o manipule el número de secuencia recibido por la fuente. En SEAD se implementa básicamente características para proteger modificaciones en la información de enrutamiento, tales como, la métrica, número de secuencia y ruta fuente. Este protocolo utiliza cadenas de hash de una vía y utiliza elementos en grupos de m (siendo m el diámetro de la red) para cada número de secuencia. Cada nodo usa un simple siguiente elemento específico de su cadena de hash en cada actualización de ruta que este envía sobre el mismo. El límite superior de la red se denota con (m-1). Una entrada es autenticada usando el número de secuencia en esa entrada para determinar un grupo contiguo de m elementos de la cadena de hash del nodo destino, elemento que debe ser usado para autenticar esa actualización de ruta. La naturaleza de las cadenas de hash de una vía previene que cualquier nodo anuncie una ruta con un número de secuencia mayor que el número de secuencia de la fuente. Para evitar bucles de enrutamiento, la fuente de cada mensaje de actualización de ruta debe ser autenticada. Este protocolo requiere de claves de secreto compartido por pares (pairwise shared secret keys) o de autenticación de difusión tales como, TESLA [10] O TIK [11] para

autenticar a los vecinos. SEAD no hace frente a los ataques de agujero de gusano (wormhole attack) aunque los autores proponen, como en el protocolo de ARIADNE, la utilización del protocolo TIK para detectar la amenaza. Se puede concluir que este protocolo ya ha tenido suficiente investigación y desarrollo sin embargo el utilizar como base al protocolo DSDV, ya es una desventaja debido a que los protocolos de mayor interés para los investigadores en la actualidad son AODV y DSR. Por lo tanto si vamos a realizar esfuerzos de investigación, estos deberán estar en consonancia a las tendencias actuales, las cuales generalmente han sido puestas bajo mayor observación debido a los resultados que han dado a las simulaciones.

1.6.2. Prevención, Detección y Reacción

El egoísmo es un nuevo tipo de comportamiento no deseado en los nodos de las redes Ad Hoc, y la obligación a la cooperación vendría a ser su contramedida ante este mal comportamiento. Un nodo egoísta es aquel que se rehúsa a cooperar en el enrutamiento de paquetes con el fin de ahorrar energía para destinarla a su propio uso. El egoísmo puede causar serios problemas en el rendimiento total de la red, ya que siendo una red autocooperativa y autoconfigurable, la cual depende de la contribución que cada nodo realice en la red, un comportamiento de este tipo no es aceptable ya que el resultado final puede ser la terminación de la comunicación. El egoísmo de los nodos ha sido tratado recientemente por la comunidad científica, y solo se han propuesto pocas medidas para combatir esta situación. Las propuestas actuales de obligación a la cooperación para redes MANET caen en dos categorías: soluciones basadas en divisas (currency based), por el cual una cierta forma de dinero digital se utiliza como un incentivo para la cooperación, y soluciones basadas en monitoreo, donde se utiliza el principio de observaciones compartidas por la mayoría de nodos legítimos.

1.6.2.1. Nuglets (Divisa Virtual)

En [19] se presentan dos asuntos importantes orientados específicamente al entorno Ad Hoc. En primer lugar, los usuarios finales deben dar algún incentivo para contribuir en la operación de la red (especialmente para transmitir los paquetes que pertenecen a otros nodos), en segundo lugar, los usuarios finales deben ser disuadidos de sobrecargar la red. La solución consiste en una compra de divisas Nuglet utilizadas en cada transacción. Dos modelos diferentes se describen: el modelo de Cartera de paquetes y el modelo de Comercio de Paquetes. En el modelo de cartera de paquetes cada paquete es cargado con nuglets para su servicio de reenvío. La ventaja de este enfoque es que disuade a los usuarios de sobrecargar la red, pero con el inconveniente de que la fuente necesita saber cuántos nuglets necesita incluir en el paquete que envía. En el modelo de comercio de paquetes, cada paquete se negocia por nuglets por los nodos intermedios, cada nodo intermedio compra el paquete del nodo antecesor en la ruta. Por lo tanto el destino debe pagar por el paquete. La principal ventaja de este enfoque, es que la fuente no necesita saber exactamente cuántos nuglets debe cargar al paquete que envía. Sin embargo como la generación de paquetes no está cargada, puede darse una sobrecarga maliciosa en la red la cual no se puede prevenir.

1.6.2.2. CONFIDANT

En [20] los autores proponen la técnica CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks), como una extensión del protocolo DSR, el cual tiene por objetivo la detección de nodos maliciosos a través de monitoreo y generación de reportes combinados y estableciendo rutas evitando los nodos con mal comportamiento. Los componentes en cada nodo incluyen un monitor de red, registros de reputación de primera mano y por otro lado observaciones confiables acerca del comportamiento del enrutamiento y reenvío de los otros nodos, registros de confianza para controlar la confianza dada a las advertencias recibidas, y un administrador de rutas para adaptar el comportamiento del nodo local de acuerdo a su reputación y para tomar

acciones contra los nodos maliciosos. Las limitaciones de CONFIDANT se encuentran en los supuestos de los sistemas basados en detección de reputación. Los eventos deben ser observables y clasificables para la detección, y la reputación solo puede ser significativa si la identidad de cada nodo es persistente, de otro modo será vulnerable frente a ataques de suplantación.

1.6.2.3. CORE

En el esquema propuesto por Molva [21], se estimula la cooperación de los nodos por una técnica de monitoreo colaborativo y un mecanismo de reputación. Cada nodo de la red monitorea el comportamiento de sus vecinos con respecto a una función buscada y reúne observaciones acerca de la ejecución de esa función. En base a las observaciones recolectadas, cada nodo calcula un valor de reputación de cada vecino utilizando un sofisticado mecanismo que diferencia entre reputación subjetiva (observaciones), reputación indirecta (reportes positivos de otros), y reputación funcional (comportamiento frente a una tarea específica), los cuales son pesados para un valor de reputación combinado. La fórmula utilizada para el efecto evita falsas detecciones a través del uso de un factor de envejecimiento el cual da más relevancia a observaciones pasadas, las variaciones del comportamiento de un nodo son filtradas. Además, si la función que está siendo monitoreada provee un mensaje de asentimiento, la información de reputación puede también obtenerse de los nodos que no se encuentran en el rango de radio del nodo monitoreado. En este caso, solamente las calificaciones positivas son asignadas a los nodos que participaron en la ejecución de la función en su totalidad. El mecanismo CORE resiste ataques realizados usando su propio mecanismo de seguridad, ninguna calificación negativa es desplegada entre los nodos, por lo tanto es imposible que un nodo reduzca de manera maliciosa la reputación de otro nodo. El mecanismo de reputación permite a los nodos de la MANET aislar gradualmente a los nodos egoístas, cuando la reputación asignada a un nodo vecino se reduce por debajo al umbral predefinido, la provisión del servicio hacia el nodo con mal comportamiento se interrumpe. Al igual que otros

mecanismos basados en reputación, el mecanismo CORE sufre contra un ataque de suplantación, a los nodos con mal comportamiento no se les impide cambiar su identidad en la red, permitiendo al atacante eludir el sistema de reputación.

Khin Sandar Win [22] hace un análisis de las soluciones y contramedidas frente a los ataques de agujero de gusano y presenta tres estrategias de solución.

1.6.2.4. Correas de Paquetes (Packet Leashes)

Este es un mecanismo para detectar los ataques de agujero de gusano y defenderse de ellos. Existen dos propuestas para utilizar este mecanismo: Correas Geográficas (Geographical Leashes) y Correas Temporales (Temporal Leashes). En las correas geográficas, cada nodo conoce la posición precisa y todos los nodos tienen un reloj que se sincroniza libremente. Antes de iniciar la transmisión de un paquete cada nodo adjunta su actual posición y tiempo de transmisión al mismo, el nodo que recibe el paquete calcula la distancia hacia el emisor y el tiempo que le toma al paquete atravesar la ruta. El receptor puede utilizar su información de distancia en cualquier momento y verificar si el paquete atravesó o no por un agujero de gusano. En las correas temporales, todos los nodos deben mantener una ajustada sincronización de reloj pero no confían en la información del GPS. Cuando se utilizan correas temporales el nodo emisor adjunta el tiempo de transmisión a cada paquete enviado **ts** en la correa de paquetes, y el nodo receptor utiliza su propio tiempo de recepción de paquetes **tr** para verificación. El nodo emisor calcula un tiempo de expiración **te** luego del cual este paquete no debería ser aceptado, y pone esta información en la correa. Para prevenir que un paquete atraviese más allá de la distancia **L**, el tiempo de expiración se establece en $\mathbf{te= ts+ (L/c)-\Delta}$, donde **c** es la velocidad de la luz y $\mathbf{\Delta}$ es el máximo error de sincronización de reloj. Todo nodo emisor adjunta el tiempo de transmisión a cada paquete enviado. El receptor compara el tiempo con su tiempo mantenido localmente, asumiendo que la velocidad de propagación es igual a la velocidad de la luz, y calcula la distancia hacia el emisor. El receptor puede entonces detectar si el paquete ha viajado por un número de saltos adicional antes de alcanzar al receptor. Tanto las Correas

Geográficas como las Correas Temporales requieren que todos los nodos puedan obtener claves simétricas autenticadas de todos los otros nodos de la red. Esto permite que el receptor pueda autenticar la ubicación e información del tiempo del paquete recibido.

1.6.2.5. Tiempo de Vuelo

Otro conjunto de técnicas de prevención frente a este tipo de ataque, que trabaja de manera similar a las correas temporales, se fundamenta en el tiempo de vuelo de los paquetes individuales. Una posibilidad para prevenir este tipo de ataques, tal como lo mencionan [23] en su trabajo, se trata de la medición del tiempo de viaje round-trip del mensaje y su asentimiento, después se estima la distancia entre los nodos con este tiempo de vuelo y se determina de este modo si la distancia calculada se encuentra entre el máximo rango de comunicación posible. La base de todos estos enfoques se sustenta en el RTT (Round Trip Travel Time) del mensaje en el medio inalámbrico, el cual puede relacionarse con la distancia entre los nodos, asumiendo para esto que la señal inalámbrica viaja a la velocidad de la luz. El uso de RTT elimina la necesidad de una estrecha sincronización de relojes como sucede con las correas temporales. El nodo solamente utiliza su propio nodo para medir el tiempo.

1.6.2.6. Técnicas Especializadas

Existen otras técnicas especializadas para redes específicas sin embargo son poco prácticas al momento de asegurar redes MANET generales. A continuación se muestra una tabla donde se analizan las diversas técnicas para detectar y controlar este tipo de ataques. Esta tabla fue propuesta por [22].

Método	Requerimientos	Comentario
Correas de Paquetes Geográficas	Coordenadas de GPS, con poca sincronización de relojes (ms)	Robusto, solución simple, hereda las limitaciones generales de la tecnología GPS.
Correas de Paquetes Temporales	Relojes estrechamente sincronizados (ns)	No es práctico, requiere sincronización de tiempos, nivel que no se ha alcanzado todavía en redes sensor.
Correas de paquetes de fin a fin	Coordenadas de GPS, con poca sincronización de relojes (ms)	Hereda las limitaciones generales de la tecnología GPS.
Tiempo de Vuelo	Habilitación de hardware con mensaje de un bit, con respuesta inmediata sin involucramiento de CPU.	Poco práctico, requerirá muy probablemente de modificaciones en capa de enlace.
Antenas Direccionales	Antenas Direccionales en todos los nodos o algunos nodos con ambas cosas GPS y antenas direccionales.	Buena solución para redes que confían en antenas direccionales, pero no directamente aplicable en otras redes más generales.
Visualización de la Red	Controlador Centralizado	Parece prometedor, trabaja mejor en redes de alta densidad, no se ha estudiado la movilidad, muchos terrenos no estudiados.
Localización	Conocimiento de la localización, nodos guardianes	Solución para redes sensor, no aplicable para redes móviles.
Análisis Estadístico	No hay requisitos	Trabaja solamente en protocolos bajo demanda multisalto.

Tabla 1.6.2.1 Técnicas de Reenvío Seguro

1.6.3. Administración de Confianza (Trust Management)

Esta estrategia de seguridad es una de las más importantes y tiene relación directa con esta investigación, además de que es uno de los puntos neurálgicos en la seguridad integral de una red MANET. La administración efectiva de los esquemas de autenticación y manejo de claves reviste especial importancia en una red de esta naturaleza, ya que es la única forma de garantizar que las otras estrategias de seguridad puedan llevarse a cabo efectivamente, ya que si no garantizamos un canal e transmisión seguro, las demás amenazas que las otras estrategias no pueden resolver pueden tener lugar y comprometer al sistema de otros modos, que actúan en capas diferentes a las cuales, se han propuesto soluciones aplicables solo a esos niveles. Por lo tanto, esta es una medida necesaria para la propuesta de una arquitectura integral que opere en toda la pila de protocolos. Esto se reduce a la administración efectiva de claves y a los mecanismos utilizados para lograr mayor seguridad del sistema. En la siguiente sección se detallan los mecanismos existentes para administrar claves y los mecanismos de encriptación utilizados para tal efecto.

CAPITULO II

2. Autenticación en redes MANET

2.1. Introducción

En los capítulos anteriores se trataron los temas de enrutamiento seguro, tema en el cual se han analizado las propuestas de protocolos de enrutamiento seguros, tales como, ARAN, SEAD, ARIADNE. Por otro lado se analizó también la necesidad de mantener un reenvío seguro de paquetes, característica de seguridad necesaria para garantizar un adecuado comportamiento de los nodos que intervienen en el enrutamiento de los paquetes. Finalmente se menciona a breves rasgos el tema de Administración de Confianza. La Administración de Confianza, es el uso adecuado de cualquier esquema de autenticación con el fin de garantizar los requisitos fundamentales de seguridad, como son la confidencialidad, integridad y no repudio de la información transmitida por cualquier medio electrónico. A continuación nos adentramos al estudio de la Autenticación, esquemas criptográficos y esquemas de autenticación propuestos para redes MANET.

2.2. Autenticación

Existen múltiples referencias en la literatura especializada para definir la autenticación una de ellas es la siguiente: "Autenticación es un proceso que involucra a un autenticador el cual se conecta con un peticionario utilizando un protocolo de autenticación para verificar las credenciales presentadas por el peticionario para determinar los privilegios de acceso. Una tercera parte confiable puede estar involucrada como parte de protocolo de autenticación [24]".

Aquí otra definición:

La autenticación es la técnica mediante la cual un proceso verifica que su compañero de comunicación sea quién se supone que debe ser y no un impostor [25].

En seguridad informática la autenticación puede basarse en diferentes métodos. El método más común es utilizar una contraseña, sin embargo la fortaleza de este método es solo tan buena como la complejidad de la contraseña y su extensión. Las contraseñas cortas son más sencillas de romper que aquellas más extensas. La autenticación fuerte se define como la validación de un nodo contra información previamente almacenada utilizando credenciales derivadas criptográficamente.

2.3. Criptografía

2.3.1. Criptografía de Clave Simétrica o Privada

En primer lugar voy a hacer una diferenciación muy rápida y puntual entre la criptografía de clave pública y la criptografía de clave privada. En la criptografía de clave privada la misma clave generada por el criptosistema se utiliza tanto para cifrar como para descifrar la información, el esquema se muestra en las figuras 2.2.1.1 y 2.2.1.2

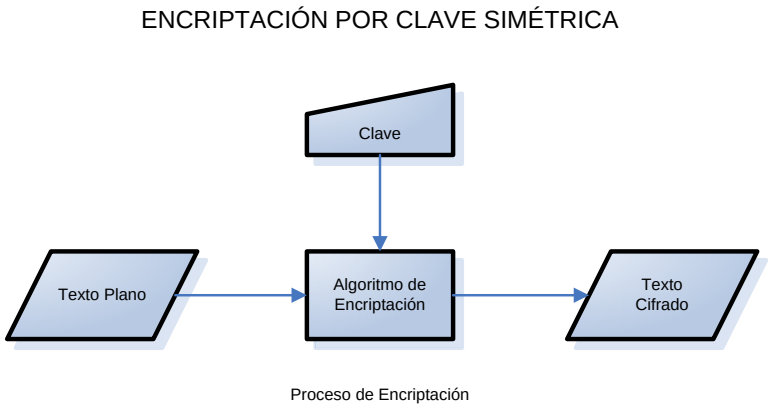

Figura 2.2.1.1 Encriptación por Clave Simétrica - Encriptación

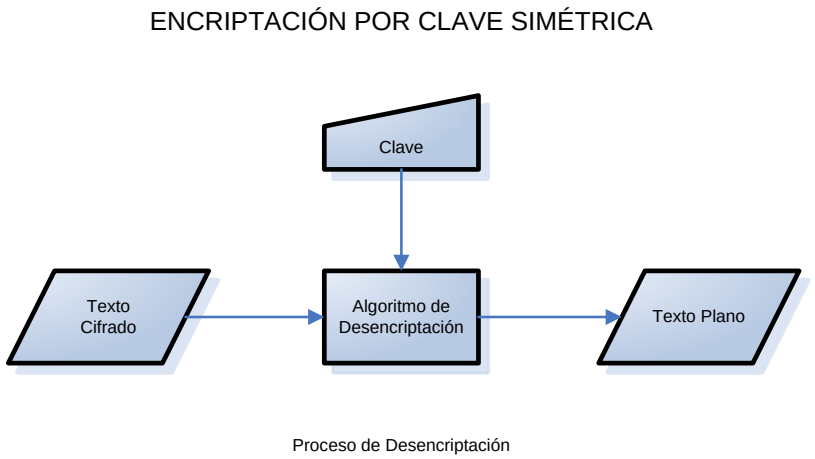

Figura 2.2.1.2 Encriptación por Clave Simétrica - Desencriptación

Como puede observarse, este modelo es muy simple pero tiene como principal inconveniente el compromiso de la clave cuando el mensaje es transmitido a través de una red insegura, como ventaja se puede considerar que los algoritmos de encriptación por clave privada son mucho más rápidos y eficientes que su contraparte de clave pública.

2.3.2. Criptografía de Clave Asimétrica o Pública

La encriptación por clave asimétrica (Clave Pública) utiliza por otro lado un par de claves una pública y otra privada las cuales están relacionadas matemáticamente y son dependientes la una de la otra. El proceso de encriptación por clave pública se muestra en el esquema de las figuras 2.2.2.1 y 2.2.2.2

En las figuras supondremos que la parte A es el emisor y la parte B el receptor.

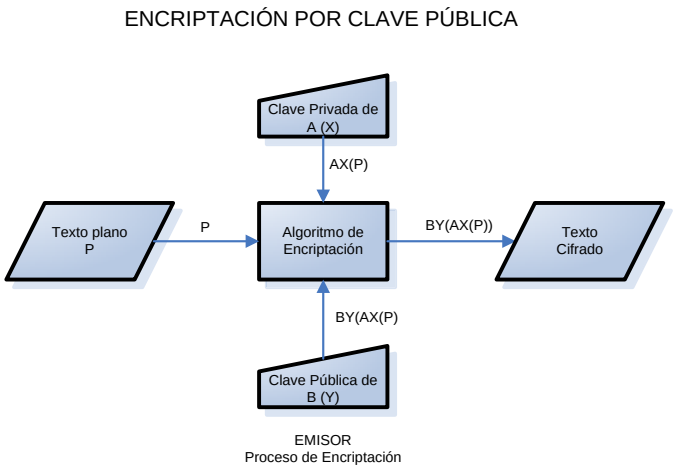

Figura 2.2.2.1 Encriptación por Clave Pública - Encriptación

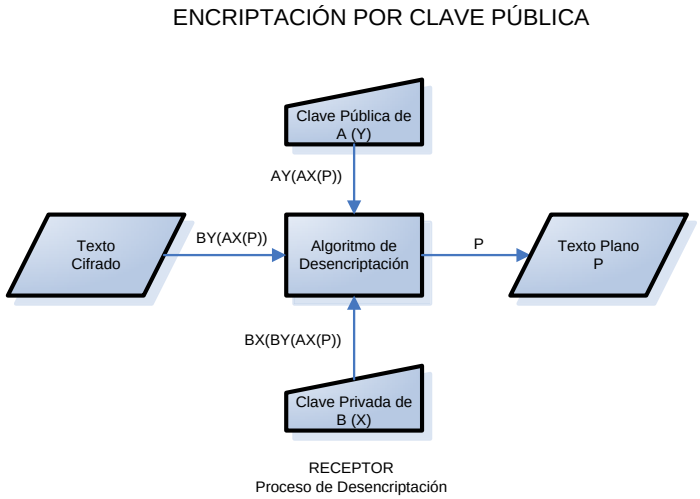

Figura 2.2.2.2 Encriptación por Clave Pública - Desencriptación

Existen varios algoritmos de encriptación de clave pública, sin embargo el que ha prevalecido invulnerable hasta la actualidad es el algoritmo RSA, nombrado de este modo por sus inventores Rivest, Shamir y Adelman, este algoritmo ha sobrevivido a todos los intentos para romperlo por aproximadamente ya 25 años. Es por tanto considerado de los algoritmos de encriptación más robustos que existen, sin embargo para dotar de suficiente fortaleza se requiere que este algoritmo tenga claves de al menos 1024 bits, lo que lo hace demasiado lento para la generación de criptogramas [26]. Es por ello que para realizar la encriptación de la clave privada se utiliza la encriptación por clave simétrica, tales como, Rijndael de Daemen y Rijmen (128

– 256 bits), Triple DES de IBM (168 bits), Twofish de Bruce Schneier (128 – 256 bits), RC5 de Ronald Rivest (128 – 256 bits).

Como puede observarse en este tipo de infraestructura intervienen muchos más elementos que refuerzan la seguridad del criptosistema, sin embargo, la seguridad del sistema depende de cuán segura se mantenga la confidencialidad de la clave privada, puesto que, si ésta es descubierta se comprometería la seguridad de todo el sistema y no serviría de nada.

Por otro lado cuando se utiliza este tipo de infraestructura es de interés del usuario que su clave pública se conozca y de esta forma puede mostrarse que, un individuo el cual posee un certificado digital es confiable.

2.4. Esquemas De Autenticación

2.4.1. Introducción

En esta sección se discutirán los modelos generales de autenticación, se describirán los modelos. La Figura 2.3.1.1 ilustra la clasificación de estos modelos. El esquema se propuso en [27].

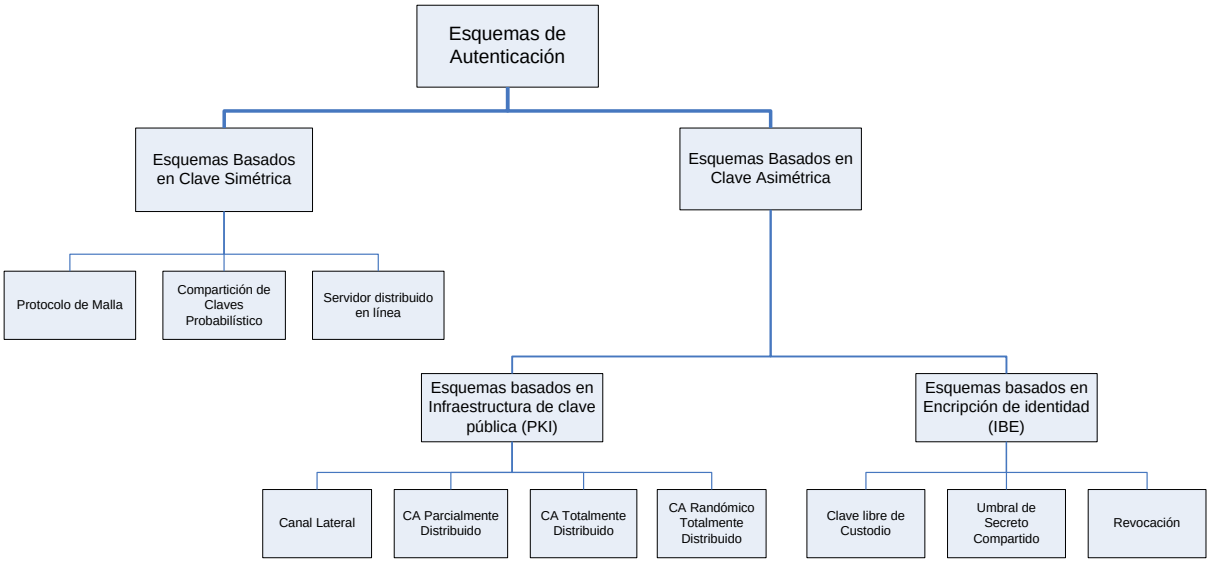

Figura 2.3.1.1 Esquemas de Autenticación [27]

2.4.2. Soluciones Simétricas

Cuando se utiliza encriptación simétrica, se debe compartir una clave entre todos los dispositivos que quieren comunicarse. La compartición de la clave puede alcanzarse transmitiendo la clave a través de un canal confidencial y autentico antes de la ejecución del protocolo de autenticación. Si queremos utilizar la clave común directamente para cifrar la comunicación, las partes que quieren comunicarse necesitan compartir una clave simétrica de un tamaño adecuado. No es recomendable utilizar la misma clave de cifrado por un largo periodo de tiempo. Para evitar esto, una clave de sesión fresca puede derivarse de información común y/o de claves de sesión previas. Se conocen dos estándares actuales y un protocolo para redes Ad Hoc los cuales están basados en esquemas puramente simétricos.

2.4.2.1. Modelo IEEE 802.11b

El estándar fue propuesto para definir la interface sobre el aire entre clientes inalámbricos y una estación base, o entre dos clientes inalámbricos. Originalmente este estándar no estaba pensado para utilizarse en redes Ad Hoc, sino que se diseñó para redes con infraestructura fija. Existen dos modos de autenticación en este protocolo:

1. Sistema Abierto (Open System): La cual es la configuración por defecto y no requiere de ninguna forma de autenticación entre los dispositivos en comunicación.

2. Clave Compartida (Shared Key): La cual requiere que las partes involucradas en la comunicación intercambien una clave secreta a través de un canal seguro, previa la ejecución del protocolo de autenticación.

Por consiguiente el primer modo no provee ninguna autenticación y el segundo utiliza un protocolo de desafío y respuesta simple que verifica si ambas partes poseen la misma llave. El algoritmo WEP se utiliza tanto en el protocolo de autenticación, así como en el algoritmo de cifrado. El algoritmo requiere un manejo externo (un canal seguro). Este requerimiento es el punto

crucial del protocolo debido a que puede ser muy restrictivo en algunas redes Ad Hoc. No se puede asumir la existencia de un canal seguro entre los dispositivos de las aplicaciones Ad Hoc. El protocolo de autenticación implementado es débil y los ataques se presentan, debido a que el tamaño de la clave in el estándar es de apenas 40 bits lo que lo vuelve propenso a los ataques de fuerza bruta. Se ha probado que el algoritmo WEP es débil incluso cuando el tamaño de la clave se incrementa. En Junio de 2004 el estándar WEP fue reemplazado por el algoritmo AES [25], esto se realizó con el fin de mejorar la seguridad.

2.4.2.2. Modelo Bluetooth

El protocolo es estandarizado por IEEE 802.15 [28] para Redes Inalámbricas de Área Personal (WPAN Wireless Personal Area Networks). Este protocolo ya es utilizado por varias aplicaciones a pesar de los inquietantes problemas a la seguridad. Muchos fabricantes implementan Bluetooth de manera muy pobre, lo que permite a terceros acceder a datos de PDAs o teléfonos celulares, ya que en estas implementaciones la autenticación ha sido deshabilitada para permitir un intercambio más ágil de información entre dispositivos móviles. Si la autenticación está habilitada, la clave de 128 bits se deriva de un PIN que fue ingresado en los dispositivos de comunicación. La longitud de esta clave varía entre 8 y 128 bits. Hay que notar que en ocasiones esta clave está configurada en 0 por defecto o es configurada como una clave de corta longitud por los usuarios que no desean ingresar PINes extensos no es muy amigable. Las soluciones Bluetooth no escalan bien debido a que los PINes deben ingresarse manualmente en cada dispositivo, lo que lo vuelve un proceso ineficiente e inseguro.

2.4.3. Soluciones Híbridas

Algunas soluciones Ad Hoc combinan criptosistemas simétricos y asimétricos con el fin de proveer autenticación de la entidad y/o establecimiento de claves. A continuación se presentan modelos de autenticación híbridos.

2.4.3.1. Modelo de Password

Dependiendo del tamaño de memoria disponible y de la forma en que la clave secreta se intercambia, puede ser mejor compartir passwords cortos en lugar de largas claves. Si queremos usar passwords compartidos que deriven en una clave de cifrado fuerte, necesitamos usar un criptosistema asimétrico. Para implementar esta idea, necesitamos de un protocolo de intercambio de clave autenticada por password o (PAKE Password-Authenticated Key Exchange) [29], que resista ataques de diccionario. Debe notarse que estos protocolos proveen autenticación de entidades y establecimiento de una clave de sesión. Debido al uso de criptosistemas asimétricos, los protocolos PAKE requieren de pesados pasos computacionales, por los costos computacionales que estos protocolos implican, es necesario examinar estos protocolos para determinar si son o no adecuados para aplicaciones en redes Ad Hoc. Estos protocolos vienen a ser una combinación de passwords débiles y cifrado asimétrico, lo que da como resultado una clave compartida fuerte. Esto fue propuesto por Bellovin y Merrit [29]. Estos autores sugieren utilizar un password para cifrar una calve pública de corta duración. Una de las variantes introducidas está basada en un cifrado DH de acuerdo de claves. Adicionalmente, el protocolo no requiere de la presencia de una tercera parte confiable como un CA. Desafortunadamente este protocolo requiere gasto computacional excesivo que no se desea en redes Ad Hoc.

2.4.3.2. Modelo de Cadena de Claves

El uso de elementos de cadenas de hash para autenticación fue introducido por Lamport [30] en 1981. En un esquema de cadenas de hash, la función hash

$h( )$ se aplica n veces a un valor aleatorio x. El valor inicial $x_0=x$ y se conoce como ancla y el valor $x_n= h_n(x)$ corresponde al valor final de la cadena de hash. Cada dispositivo se encarga de calcular su propia cadena hash, e intercambia de manera autentica x_n con sus compañeros de comunicación, y mantiene el valor de $x_0$en secreto.

Cuando se requiere la identidad de un dispositivo de la red por un valor de x_i, desde su cadena de hash puede probar su identidad respondiendo con un valor previo de la misma. Solamente al dispositivo que conoce el ancla se le permite calcular la respuesta requerida. Se debe considerar que los esquemas conocidos como cadenas de claves, solamente proveen autenticación unidireccional y no se establece ninguna clave durante la ejecución del protocolo.

El protocolo propuesto por Weimerskirch y Westho [31], el cual no requiere la presencia de una Autoridad de Certificación (CA) o el uso de certificados. Los costos computacionales se basan en valores de hash por lo tanto muy económicos. El ancla x0 de la cadena de claves actúa como la clave privada del dispositivo y el valor xn actúa como clave pública. Desde su introducción este protocolo no contempla ningún canal seguro para el intercambio de claves públicas, por lo tanto estas claves públicas no se pueden intercambiar con autenticidad o al menos no existe la garantía para ello. Como resultado el esquema de autenticación utilizado en este modelo es sumamente pobre, ya que está más orientado hacia los servicios que hacia la seguridad. Esta clave pública está limitada a un servicio y no a una identidad. En un trabajo posterior los mismos autores [32] fortalecieron la autenticación al precio de dos requerimientos:

1. Acceso a Internet permanente o temporal.

2. Dispositivos de red con poder computacional moderado.

En este escenario las claves públicas x_n de los dispositivos son firmadas por una CA. Luego al momento en que el dispositivo recibe la clave pública que

necesita para verificar la firma de la CA. Para cada miembro de la comunicación, cada dispositivo necesita realizar la verificación. Una vez que las claves son verificadas satisfactoriamente, el esquema se vuelve igual al original con requerimientos computacionales mínimos.

2.4.4. Soluciones Asimétricas

A continuación se describirán varios modelos de autenticación para redes Ad Hoc las cuales se basan en sistemas de cifrado asimétricos. Las llaves públicas se utilizan para autenticación de entidades y para establecimiento de sesiones mediante claves. La clave de sesión es luego utilizada en un esquema de cifrado simétrico que provee comunicación confidencial entre los dispositivos autenticados. La falta de una CA central es el principal problema cuando se implementan protocolos asimétricos en redes sin infraestructura fija. Aquí se distinguen cuatro categorías de modelos de autenticación asimétricos:

1. Con una Autoridad de Certificación (CA) y el uso de certificados.
2. Con una CA sin el uso de certificados
3. Sin una CA pero con el uso de certificados
4. Sin una CA y sin el uso de certificados

La primera categoría incluye el modelo de CA distribuida, el segundo modelo corresponde al modelo basado en identidad y clave pública auto distribuida. La tercera categoría contiene modelo de auto organización y subgrupo confiable y la cuarta categoría corresponde a un modelo de clave pública sin certificación.

2.4.4.1. Modelo de CA distribuida

La idea se basa en el hecho que la CA no debería estar representada por un solo nodo, debido a que los nodos proveen una protección física débil la cual puede ser fácilmente comprometida por un adversario. En el 2001, Zhou y Haas introdujeron un protocolo [33], del cual aseguraban se ajustaba a redes sin

infraestructura consistente de anfitriones móviles. La idea era distribuir la potencia de la CA hacia t+1 nodos especiales, también conocidos como nodos servidor, los cuales estarían presentes en la inicialización de la red. Los autores implementaron esta idea a través de un esquema de umbral (t+1, n). Cualquiera de los nodos servidores t+1 en la red pueden conjuntamente expedir certificados. Cada miembro en la red está en posesión de un par de claves pública y privada. Los miembros de la red pueden solicitar copias auténticas de las claves públicas de cualquier miembro de la red, desde cualquier grupo de nodos servidor.

Un nodo A necesita realizar una solicitud para obtener una copia autentica de la calve pública de B. A inicia la búsqueda enviando un broadcast hacia al menos un nodo servidor t+1. Cada uno de estos nodos firma la solicitud de clave pública, con su clave secreta compartida por el sistema. Las firmas parciales de los nodos servidor son entonces enviadas hacia un nodo combinador C, el cual combina todas las firmas parciales y envía la firma completa hacia A. El nodo A verifica la firma en la clave pública del nodo B y la acepta o rechaza. Como se puede apreciar, la carga de trabajo de los nodos servidor y combinador es muy alta, ya que, estos deben responder a todas las búsquedas. En lugar de obtener la firma de los nodos servidor muchas veces, parecería más eficiente si cada nodo solicitara un certificado para su propia clave pública a los nodos servidor y luego devolver este certificado cuando sea requerido por otro nodo, como se propone en [34]. Kong y Zerfos presentaron un protocolo que combina el protocolo RSA, con el esquema de umbral. Los autores extiendes las tareas de la CA, la cual es representada por k nodos, los cuales otorgan, renuevan y revocan certificados, nótese que no existen nodos servidor especiales en esta implementación como se requería en la primera solución. La verificación de certificados requiere menor gasto computacional y de comunicación que el protocolo anterior debido a que no se requiere de otros dispositivos, más que los que desean comunicarse. Ambas soluciones presentadas todavía requieren de mucho poder computacional y deben ser revisados para su implementación en dispositivos móviles de baja potencia.

2.4.4.2. Modelo Basado en Identidad

Estos esquemas introducidos por Shamir en 1984 [35], no requieren ningún intercambio de claves anterior a la autenticación real, debido a que información común es utilizada como clave pública y certificado a la vez. La criptografía basada en identidad se fundamenta en la idea de utilizar identidades humanas únicas, tales como, nombres, direcciones de e-mail, etc., como clave pública. Por lo tanto, las identidades son auto certificables. Existen dos ventajas principales de este acercamiento. En primer lugar, no se requieren certificados de claves públicas, y en segundo lugar, no se requiere de intercambio de claves públicas. La implementación de la revocación de claves públicas es simple en estos sistemas y puede ser alcanzada añadiendo una fecha de expiración. Los esquemas basados en Identidad requieren una CA en primera instancia, para generar y distribuir las claves secretas personales de todos los usuarios. Luego de esta fase la CA se vuelve redundante. El hecho de que la CA conozca las claves secretas de todos los usuarios es considerado generalmente una desventaja en los esquemas basados en Identidad. El canal autentico y confidencial entre cada dispositivo y la CA plantea otra desventaja, se debe notar que en otros esquemas asimétricos que un canal autentico es suficiente, debido a que solamente la información pública es transmitida. Si se desea el poder de la CA podría ser limitado por alguna de las siguientes alternativas:

1. La asignación de una fecha de expiración a la clave secreta del sistema principal.

2. Cifrar todos los mensajes utilizando pares de claves pública/privada adicionales desconocidas por la CA.

3. Distribución del poder implementando un esquema de umbral que requiera k nodos para realizar todas las tareas.

CAPITULO III

3. Definición del Problema

3.1. Análisis y definición del problema

El problema comienza en el momento en que se trabaja por asegurar una sola capa de la pila de protocolos y debido a que la seguridad es un problema que sobrepasa y afecta a varios niveles, en el presente proyecto se ha propuesto la recomendación de un modelo de seguridad que proteja en varios niveles, en donde, las contribuciones de una capa inferior cooperen con las capas superiores. Las propuestas actuales de seguridad se enfocan en algunas de las estrategias de seguridad de enrutamiento seguro, reenvío seguro, o la trilogía prevención, detección y reacción que monitorea el comportamiento no deseado. Al momento la mayoría de estos esfuerzos han sido enfocados una sola capa (generalmente a la capa de red) y de este modo se pretende asegurar a todo el sistema de comunicación Ad Hoc móvil con las consecuentes limitaciones que esto implica, ya que no se puede pretender el logro de una seguridad eficiente a un solo nivel, es por ello que el modelo propuesto pretende eliminar las correspondientes desventajas de estos enfoques y plantear una alternativa de acuerdo a un modelo más estructurado y lógico de administración de seguridad que trascienda varios niveles en donde cada capa sea la responsable de un nivel de seguridad y que cada una de las capas contribuyan a la seguridad total de la red, consiguiendo así mayor eficiencia dentro de redes con requerimientos de seguridad más exigentes en robustez y flexibilidad operativa.

3.2. Hipótesis

El modelo de seguridad propuesto minimizará los riesgos a los que se enfrenta una red Ad Hoc móvil en ambientes de alto riesgo.

3.3. Objetivos

Presentar un modelo de seguridad que contemple las vulnerabilidades en cada capa que conforma una red MANET.

Detallar las estrategias de seguridad llevadas a cabo por cada capa.

Utilizar las propuestas de seguridad existentes cuya probada eficiencia contribuya al reforzamiento de la seguridad de todo el modelo.

3.4. Modelos de Seguridad por Capas Previos

El modelo propuesto por [36] sugiere una arquitectura de seguridad definida en cinco capas en el cual se detallan los requisitos de seguridad a cumplir en cada uno de los niveles. En la capa de seguridad 1 SL1 habla de una Infraestructura de Confianza que es la relación de confianza básica que debe existir entre nodos, ya que se trata de una tarea muy desafiante, establecer un mecanismo de seguridad distribuido a este nivel se espera que los investigadores inviertan sus esfuerzos en desarrollar mecanismos de control ya que de esta capa dependen las otras. En la capa 2 SL2 llamada Capa de Seguridad de Comunicaciones la cual opera al nivel de enlace y la cual debe impedir que las tramas sean víctimas frente a ataques como intercepción, alteración, o la escucha sigilosa desde un nodo no autorizado. En la capa 3 SL3 Capa de Enrutamiento Seguro a este nivel se deben considerar dos aspectos; enrutamiento seguro y reenvío seguro de datos, se deben proteger los paquetes de ser víctimas de eliminación o alteración, esta capa es un componente especialmente importante ya que los nodos deben cooperar para mantener funcional a la red. La capa de Seguridad de Red SL4 describe los mecanismos de seguridad llevados a cabo para operaciones de acceso de fin a fin entre sistemas aquí se ejecutan los servicios de autenticación, seguridad e integridad. En la capa 5 SL5, se ejecutan servicios, tales como, SSL, SSH y cualquier otro servicio específico concerniente al protocolo de seguridad de una aplicación en específico. Se debe tomar en cuenta que los mecanismos de cifrado y manejo de

claves no eliminan la necesidad de detección y reacción frente a intrusos o frente al mal comportamiento de los nodos.

Por otro lado en [37] se presenta un modelo de dos capas que asegura la capa de enlace y la capa de red según el modelo de referencia OSI, en este trabajo se realiza un análisis de las vulnerabilidades y se analizan también las soluciones existentes y su implementación en dos niveles. A nivel de enlace de datos se propone un MAC (Mensaje de Control de Acceso) seguro, con protección reactiva, a través, de la detección y reacción. Se propone además el uso de un protocolo WEP de próxima generación para corregir las fallas de seguridad en este protocolo. A nivel de capa de red se proponen varios mecanismos entre los que se incluye el enrutamiento seguro, a través de los protocolos de seguridad existentes y el reenvío seguro de paquetes, con el uso de técnicas de detección y reacción frente a comportamientos no deseados en los nodos que forman la red.

Podemos concluir por lo tanto, al revisar la descripción de estos modelos que solamente se enfocan en problemas particulares de una capa, sin embargo este enfoque no integra a todas los niveles que intervienen en la comunicación y por lo tanto resultan en soluciones parciales, las mismas que no tienen mayor validez en ambientes de alto riesgo donde la pérdida de información y el compromiso de los nodos intervinientes es una constante amenaza con la que hay que lidiar desde diferentes frentes. En modelo que proponemos a continuación se han tomado en cuenta las amenazas a las que la información está expuesta en varios niveles y se han reforzado los mecanismos de control de manera concurrente para solventar las debilidades presentes a cada nivel del modelo.

CAPITULO IV

4. Modelo Propuesto

4.1. Introducción

La seguridad debe ser una parte integral de dentro del desarrollo de la red, más no un mecanismo añadido posteriormente. Más aún la seguridad no puede ser considerada desde una visión de capas independientes o separadas, en la actualidad contamos con varios mecanismos de seguridad que han sido implementados en diferentes capas basados en modelo de referencia OSI. En una red móvil Ad Hoc de estas características, donde el nodo es autorizado por la red y donde solo a los nodos autorizados se les permite el acceso a los recursos, se deben seguir ciertos pasos para garantizar la seguridad de todo el sistema.

El modelo en términos generales procura un fortalecimiento de la seguridad en varios niveles, comenzando desde el nivel de enlace de datos hasta la capa 4. Este modelo de seguridad opera en dos fases, la primera de ellas comprende la preautenticación, autenticación y revocación de credenciales, la segunda fase por otro lado se encarga de realizar un enrutamiento y reenvío seguros el mismo que asegura a la red a nivel de capa 3.

Los protocolos utilizados en estos niveles son del tipo IBE o Identity Based Encryption (Encriptación Basada en Identidad), en el nivel físico y de enlace, este protocolo utiliza un sistema de clave simétrica para agilizar el proceso de autenticación, el cual es el primer mecanismo de control, que garantizará la seguridad en los otros niveles. Otro protocolo utilizado es el protocolo ARAN [13], el cual opera a nivel de capa 3 y asegura el enrutamiento, otro protocolo que asegura la comunicación en capa 4 es el SSL, el cual encripta la comunicación para evitar ataques de espionaje y robo de información y finalmente a nivel de aplicación se sugiere el uso de un firewall, el cual bloqueará puertos específicos.

En los siguientes apartados se amplía esta información con mayor detalle.

4.2. Requisitos de Seguridad

Los procesos que todo sistema de establecimiento y control de seguridad deben seguir son los siguientes: arranque, preautenticación, establecimiento de credenciales, autenticación, monitoreo de comportamiento y revocación de credenciales. A continuación se detallan cada uno de estos procesos. Existe un protocolo desarrollado para cumplir con esta primera fase y otras posteriores, este protocolo llamado MANET-IDAKE [38] (Identity-Based Authetication and Key Exchange), se compone de 6 algoritmos: Inicio, Extracción, Distribución, Cálculo de Clave Pre-Compartida, Renovación de Claves, y Revocación de Claves, en la figura 4.2.1.1 se muestra el funcionamiento de este protocolo. Debemos considerar que todos los procesos realizados en esta fase se cumplen en la capa de enlace de datos. A continuación necesitamos asegurar los paquetes de datos en la capa de red encargada de efectuar las operaciones de enrutamiento seguro, para esto proponemos el uso del protocolo ARAN [13] desarrollado por Sanzgiri y otros, que cumple con los requisitos de enrutamiento seguro y reenvío seguro. Según los autores este protocolo es lo suficientemente fuerte para combatir los ataques que utilizan fabricación [18], además de ataques de suplantación de identidad y redirección de paquetes, por lo que lo hace un candidato apropiado para utilizar en nuestro modelo de seguridad, además de estas características los autores aseguran que el costo computacional del esquema de clave pública utilizado es similar al esquema de cadenas de hash del TESLA [10] utilizado por Ariadne [9], pero como contraparte ofrece un alto grado de confiabilidad en el aseguramiento del enrutamiento. Los requisitos de para la capa de transporte es la encriptación de la información utilizando alguno de los algoritmos de cifrado, los algoritmos actuales para cifrado como SSL 3 con AES son una gran alternativa a la hora de asegurar la privacidad de la conexión. Para la capa de aplicación se requiere el bloqueo de ciertos puertos o aplicaciones específicas que pueden comprometer la seguridad del nodo o de la red, para evitar estas amenazas se recomienda el uso de un firewall.

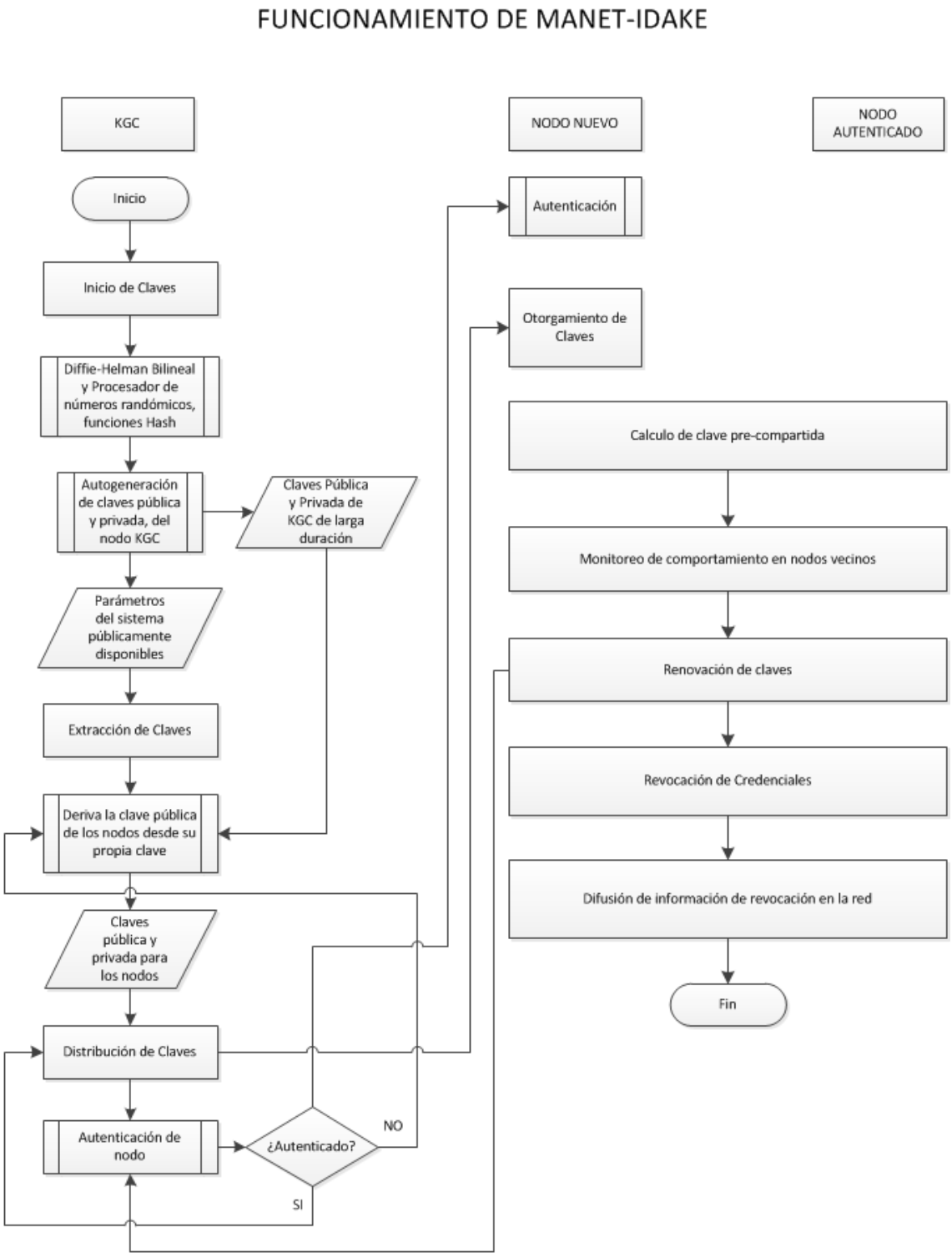

Figura 4.2.1.1 Funcionamiento MANET-IDAKE

4.3. Primera Fase De Seguridad

La primera fase de seguridad de seguridad, se inicia desde la capa física hasta la capa de enlace de datos y se mantiene vigente mientras exista la red, esta fase comprende todos los pasos que se describen a continuación. En esta fase se utiliza un esquema de encriptación por clave pública basado en identidad o IBE. Se recomienda este esquema de autenticación para la fase de arranque y las fases subsiguientes ya que es una forma práctica y no muy demandante en recursos para para implementarse.

4.3.1. Arranque

En esta etapa el nodo que solicita una conexión, presenta una credencial, esta credencial puede ser algo que posee como una clave, algo que conoce como una contraseña, o algo que es, como por ejemplo sus elementos biométricos[1]. La principal característica que debe tener la credencial es que debe ser única y permanecer así por siempre para evitar el repudio.

4.3.2. Preautenticación (Capa de enlace de datos)

En esta etapa el nodo solicitante que ha presentado sus credenciales intenta que el nodo autorizado le entregue la clave para poder acceder a los recursos de la red u ofrecer servicios, el canal empleado para este propósito debe ser un canal seguro con encriptación para la compartición de claves y contraseñas, este canal es establecido en la capa de enlace de datos.

4.3.3. Establecimiento de Credenciales (Capa de enlace de datos)

En esta etapa se le otorgan al nodo solicitante las credenciales, para poder verificar la identidad del mismo y sirve también como una verificación de su estado posterior. La credencial otorgada y entregada al nodo puede ser simétrica o un par de claves pública/privada. Las credenciales otorgadas deben contener una etiqueta con el tiempo de expiración de las mismas, después del

[1]Elementos biométricos son aquellos, elementos únicos de un sistema biológico cuyas características son únicas e irrepetibles, estas pueden ser las huellas digitales, el iris ocular, la voz, etc.

cual el nodo tiene la obligación de renegociar un nuevo certificado para sus credenciales. En nuestro caso se utilizarán claves asimétricas en un esquema de clave pública distribuida, es decir que el otorgamiento de estas claves quedará a cargo de los nodos designados como CA. Para garantizar la fortaleza de este esquema deberá existir al menos un nodo de este tipo que actuará como Autoridad de Certificación (CA), el cual es el encargado de otorgar el par de claves pública/privada que posteriormente se utilizarán para generar los hash necesarios a partir de esta combinación de claves entre el emisor y el receptor. En la Figura 4.3.3.1 se muestra un escenario de aplicación con los nodos principales realizando las tareas de preautenticación, otorgamiento de claves y revocación de claves.

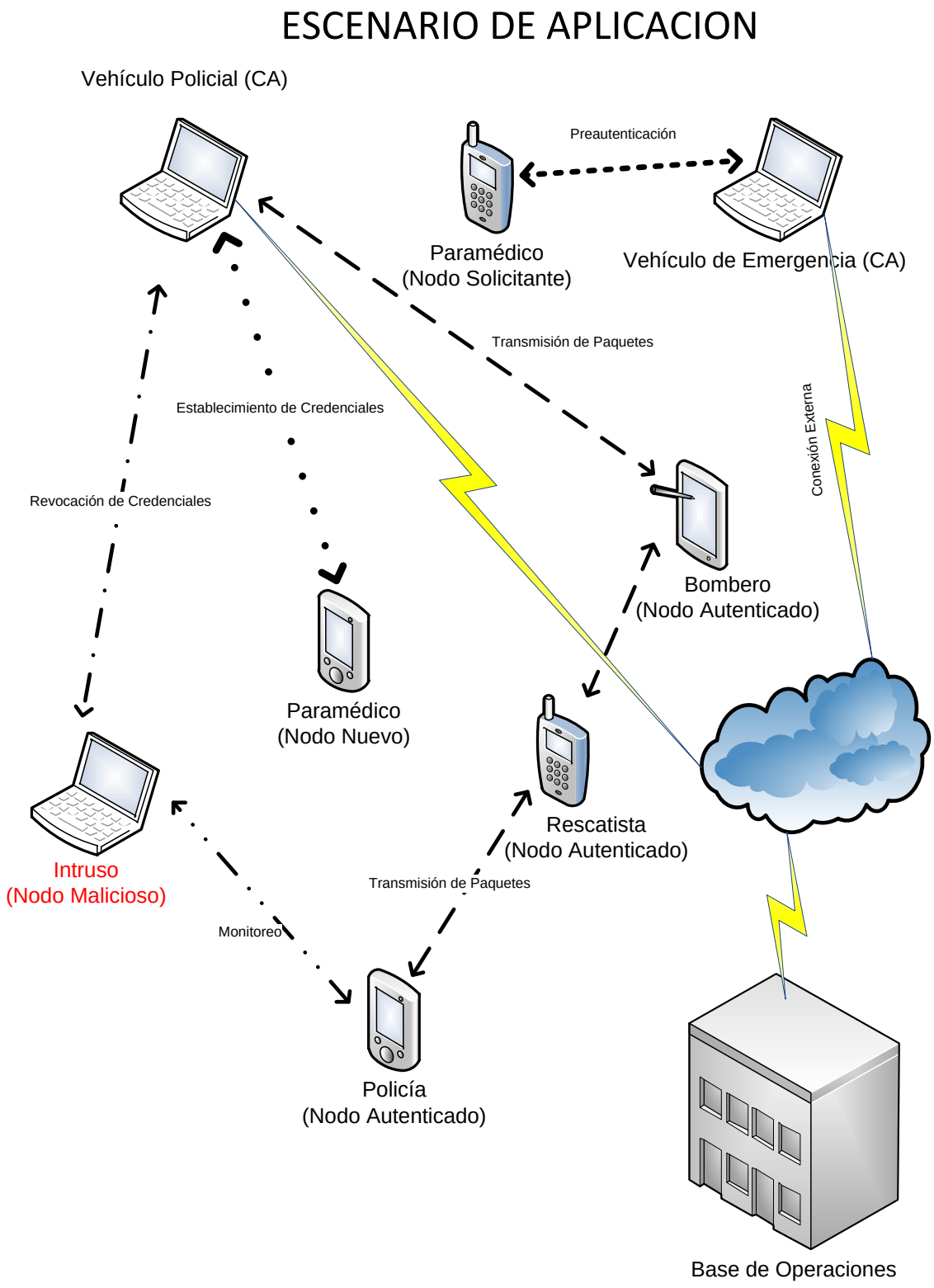

Figura 4.3.3.1 Escenario de Aplicación

4.3.4. Autenticación

En esta etapa, la comunicación entre el nodo solicitante y el nodo que autentifica es validada por el destino usando las credenciales otorgadas. No es sino hasta que se hayan cumplido todas las etapas anteriores, que un nodo se considera autenticado, lo que significa que está habilitado para utilizar los recursos protegidos por el autenticador. En la figura 4.3.4.1 se muestra el esquema de autenticación propuesto a nivel de enlace de datos se refuerza en la capa de red, realizando un hashing (firma de claves) a las claves asignadas a nivel de enlace de datos, esto con el propósito de fortalecer la autenticación lograda en etapas anteriores y también con el fin de volver más ágil el proceso de enrutamiento. En la figura 4.2.1.1 los nodos KGC (Key Generation Center), estarían representados por los CA de la Figura 4.3.4.1, los cuales son los vehículos de emergencia en el caso de este escenario en particular, sin embargo si hablamos de otro tipo de escenario más hostil como un campo de batalla las CA, serían los vehículos de abastecimiento y comunicaciones, estos son los candidatos ideales porque están mejor resguardados y poseen buena cantidad de energía y poder computacional para atender la demanda que implica la generación de claves, revocación monitoreo de estado, control de rutas, etc.

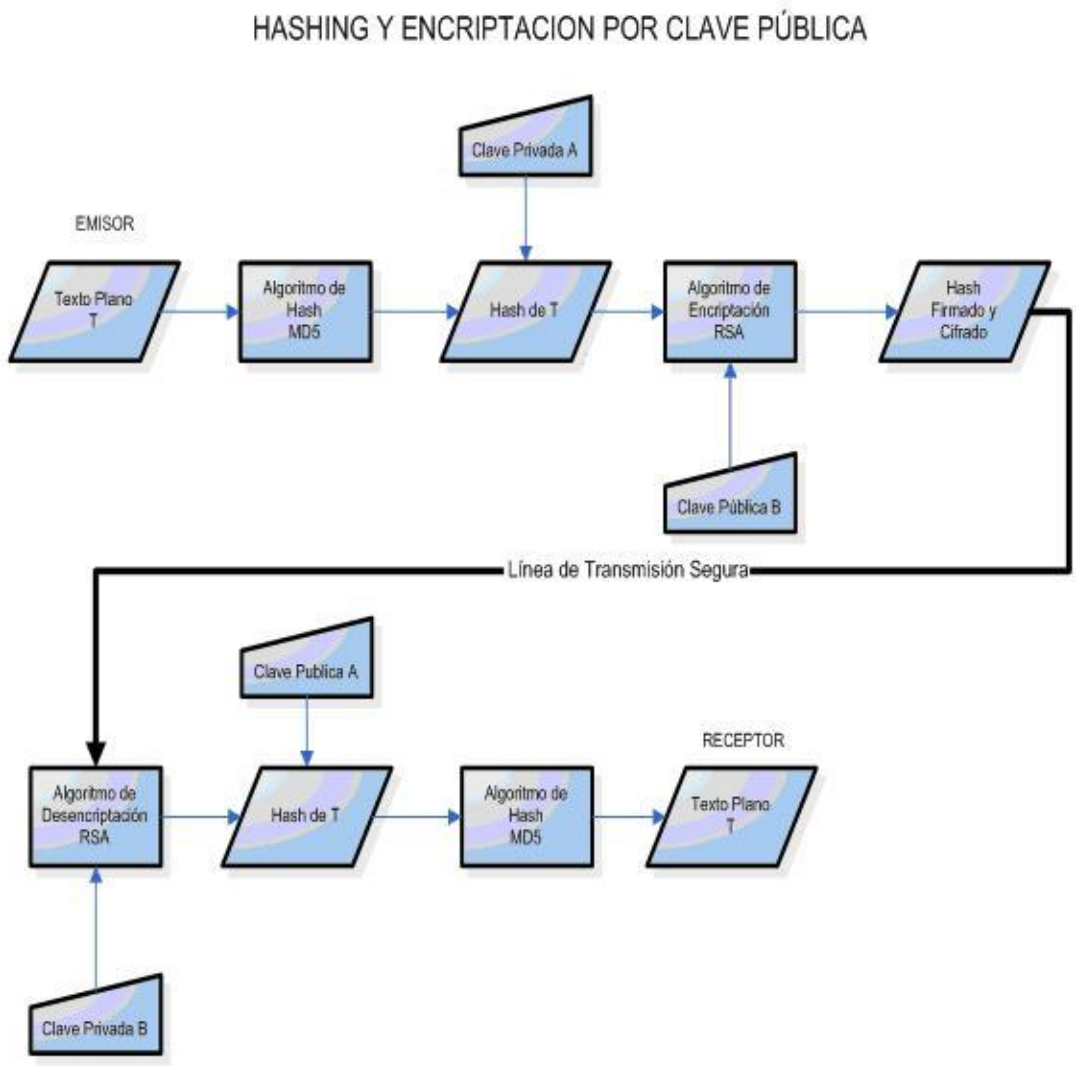

Figura 4.3.4.1 Hashing y Encriptación por Clave Pública

4.3.5. Monitoreo de Comportamiento

Mientras un nodo se encuentra autenticado, se debe monitorear su comportamiento para verificar si este ha sido comprometido o su comportamiento no es el apropiado, es decir, que se encuentra realizando actividades que pueden comprometer el rendimiento de la red como por ejemplo la resistencia de un nodo a retransmitir información de enrutamiento, o la manipulación de la información fabricando mensajes de error falsos, actividades que resultan en latencia de la red, desvío de información y en el peor de los escenarios la suspensión de la comunicación. Un nodo que muestra un comportamiento con estas características debe ser aislado y su credencial

debe ser revocada, este monitoreo se realiza a nivel de enlace de datos con el manejo de estadísticas de cooperación y a nivel de capa de red a través del protocolo de enrutamiento seguro ARAN. Los criterios para determinar un comportamiento indeseable y la frecuencia de monitoreo depende de la aplicación.

4.3.6. Revocación

En esta última fase se deben considerar dos aspectos: el primero de ellos debe responder a la pregunta ¿cuándo un nodo debe ponerse en lista de revocación?, y el segundo aspecto debe responder ¿cómo esta lista de revocación debe repartirse entre los demás nodos? Estas preguntas las resuelve la estrategia MANET-IDAKE, entre otras alternativas. La revocación de claves a nivel de enlace de datos las realiza la estrategia MANET-IDAKE, a través de la observación de nodos vecinos y esquemas de acusación. Esto se logra usando un esquema de umbral para las acusaciones y difundiéndolos a toda la red. En este esquema de revocación cada nodo mantiene una clave pública con la lista de revocación, la cual incluye también la lista de acusación como se encuentra definido en el esquema de vigilancia de vecinos, además de las acusaciones que otros nodos hacen de su vecino con comportamiento no deseado. IDAKE utiliza cuatro mecanismos para realizar la revocación de claves. Primero los nodos deben ser capaces de revocar sus propias claves públicas. En segundo lugar los nodos pueden revocar las claves públicas de los nodos comprometidos o sospechosos, a esta acción se la conoce como acusación. El tercer mecanismo es una manera de informar a todos los nodos en la red acerca de estas revocaciones. Y finalmente, necesitamos un mecanismo para que los nodos que se unen recientemente obtengan un listado de todas las claves públicas revocadas o acusadas. El llevar a cabo esta acción implica que se suspenda el enrutamiento que el nodo comprometido haya realizado hasta el momento, teniendo este que solicitar una nueva clave a nivel de enlace de datos, ya que como hemos explicado anteriormente esta acción sucede en la capa de enlace de datos. El otorgamiento de una nueva clave por parte de las CA implica un

tiempo de espera que el nodo debe soportar como sanción a su comportamiento inapropiado. En el escenario mostrado en la Figura 4.3.3.1 los vehículos de emergencia operan como CA, mientras que los agentes móviles son nodos comunes que dependen de los CA.

4.4. Segunda Fase De Seguridad

En la segunda fase entra en vigencia la protección del enrutamiento, en esta fase se realiza el hashing de las claves asignadas en la primera fase, comprobando de este modo la identidad del nodo participante. Se inicia también el protocolo de enrutamiento seguro y en el reenvío seguro, para ejecutar esta tarea se recomienda la utilización del protocolo ARAN por sus características de seguridad. Sin embargo como sus propios autores afirman, se puede optimizar este con la utilización de cadenas de hash, lo que vuelve al protocolo más liviano y menos demandante de recursos computacionales. En esta fase se realiza también un monitoreo de los nodos para verificar que las acciones de enrutamiento que se están llevando a cabo no comprometen el buen funcionamiento de la red.

4.4.1. Enrutamiento y Reenvío Seguros

El proceso correspondiente en esta fase trata de las estrategias utilizadas para llevar a cabo el enrutamiento, el cual no solo debe considerar la generación y mantenimiento de rutas, sino que además debe monitorear el comportamiento inadecuado de los nodos participantes. Para esta sección se recomienda el uso del protocolo de enrutamiento seguro ARAN, el cual según los autores es inmune a una serie de ataques de seguridad existentes. De este tema se habla con mayor detalle en el capítulo 1 en la sección 1.6.1.

4.4.2. Manejo de Sesiones y Control de Aplicaciones

Estas dos últimas fases corresponden al uso de estrategias de red generales, que no se han desarrollado exclusivamente para redes MANET, se sugiere por lo tanto para la capa de transporte el uso de encriptación SSL, en caso del uso de navegadores web, o el uso de SSH para manejo remoto de sesiones, ya que

ambos protocolos han demostrado ser muy eficientes en el control de seguridad a este nivel. Para la capa de aplicación se recomienda el uso de un firewall para el control de las aplicaciones maliciosas que no pueden controlarse en los otros niveles, sin embargo debemos tomar en cuenta que el uso de más elementos de seguridad disminuye el rendimiento general y demanda mayores recursos de los nodos intervinientes.

4.5. Modelo De Seguridad Por Capas

En la tabla 4.5.1 se muestran un resumen de los protocolos de seguridad que son parte del modelo distribuidos por capas de acuerdo al modelo de OSI. En La figura 4.5.2 se muestran las fases de operación del modelo distribuidas por capas, donde se detallan también las etapas que se ejecutan en cada capa.

Capa	Requerimientos de Seguridad	Fases	Etapas	Protocolos Aplicados	Observaciones
Aplicación	Asegurar, Aplicaciones	SEGUNDA FASE	Control de aplicaciones	Firewall / ACL	Estas estrategias de seguridad están dirigidas hacia entornos externos donde se requiere un nivel mayor de protección.
Transporte	Asegurar el canal de transmisión		Encriptación de Sesiones	SSL/SSH	Sistemas de encriptación utilizados una vez que se ha iniciado sesión como miembro de la red
Red	Asegurar los protocolos de enrutamiento		Hashing de Credenciales Enrutamiento Seguro	ARAN	En este nivel deben cumplirse tanto el enrutamiento seguro como el reenvío seguro de paquetes, sin embargo se optimizará utilizando generación de hash para mejorar el rendimiento.
Enlace de Datos	Asegurar el establecimiento y mantenimiento de claves. Así como también el monitoreo de los nodos.	PRIMERA FASE	1. Preautenticación 2. Establecimiento de Credenciales 3. Autenticación 4. Monitoreo de Credenciales 5. Revocación de Credenciales	MANET-IDAKE	Se debe controlar a este nivel, los nodos egoístas y el mal comportamiento
Física				MANET-IDAKE	El compromiso de un nodo físicamente, requeriría el secuestro o destrucción del mismo. Sin embargo el compromiso de un nodo a este nivel se controla por el mismo esquema MANET-IDAKE, revocando el certificado de este.

Tabla 4.5.1 Modelo de Seguridad por Capas

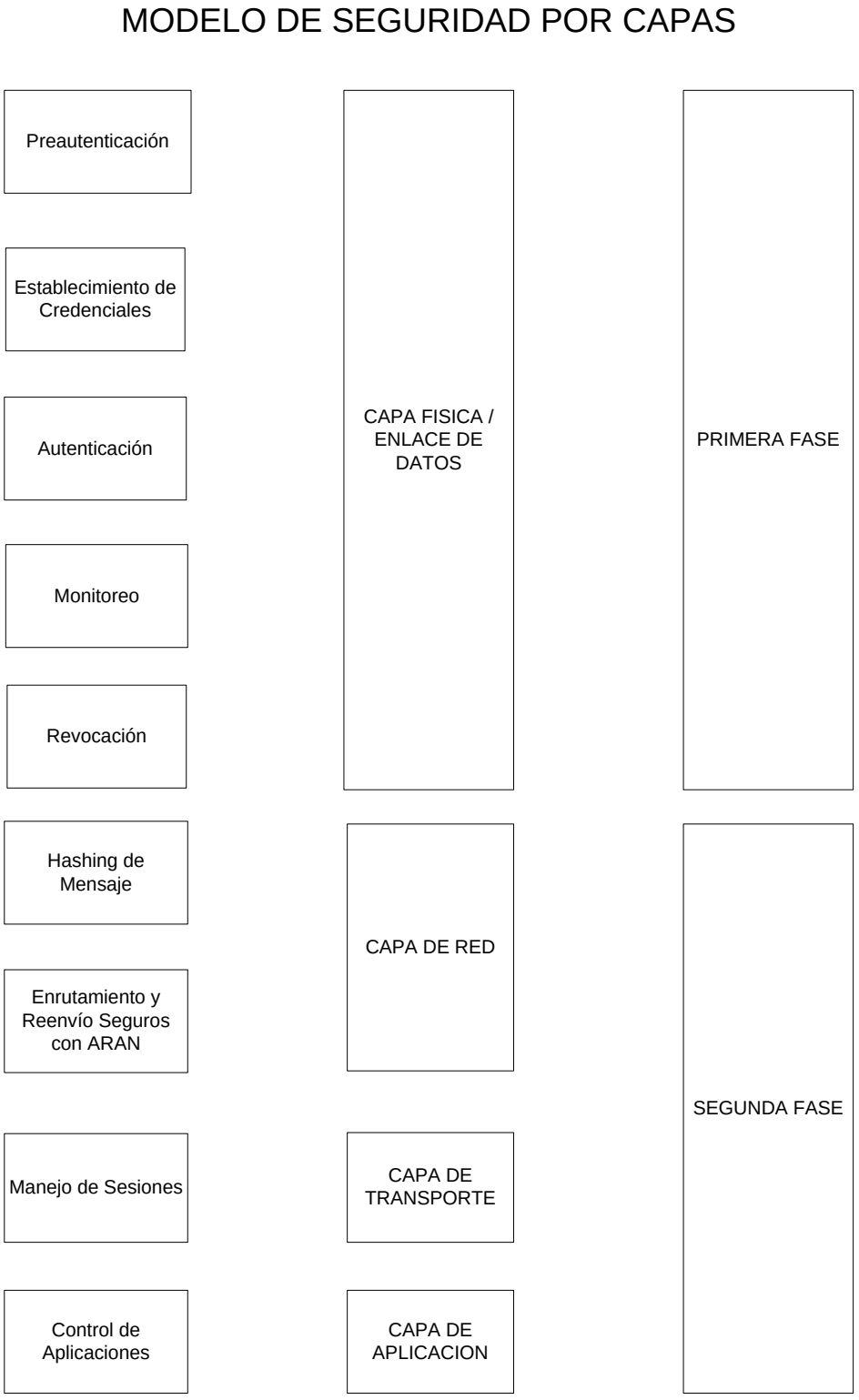

Figura 4.5.2 Modelo de Seguridad por Capas (Fases)

4.6. Operación Del Modelo De Seguridad

En la Figura 4.6.1 se detallan los procesos que el modelo de seguridad ejecuta en las diferentes fases y las estrategias de establecimiento de credenciales y revocación de las mismas.

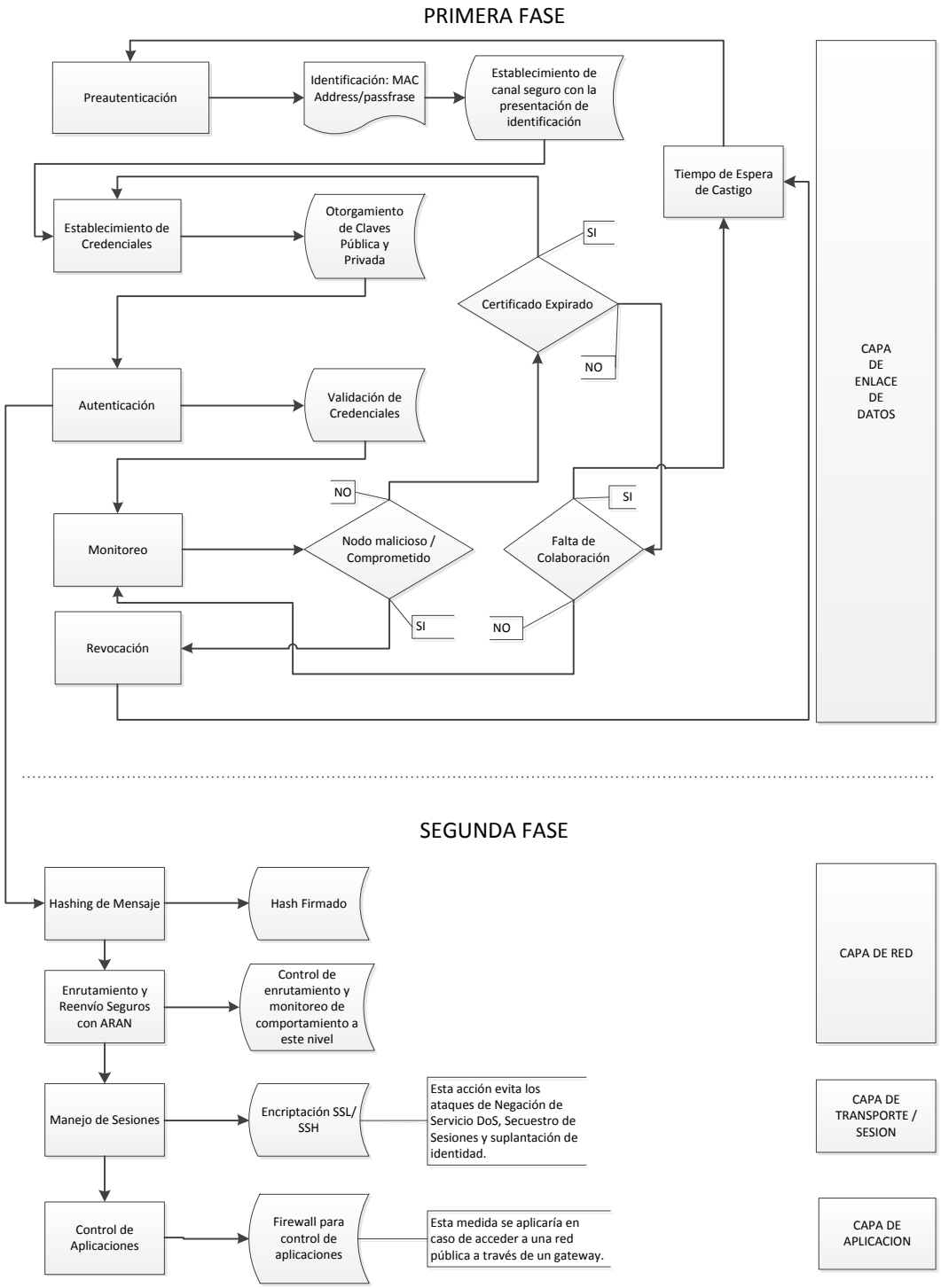

Figura 4.6.1 Operación del Modelo de Seguridad

CAPITULO V

5. ANALISIS Y DISCUSIÓN DE RESULTADOS

5.1. Problema De Nodos Físicamente Comprometidos

El modelo propuesto integra una serie de características de seguridad, que lo hace ventajoso frente a otras propuestas de seguridad presentadas y analizadas previamente. La principal característica importante sería el manejo de arranque y preautenticación que permite un mayor control de los nodos intervinientes que se suman a la MANET para su formación, esta característica es especialmente necesaria al momento del despliegue temporal en un ambiente hostil o potencialmente hostil, donde no conocemos la afectación de que uno de los nodos sea destruido o secuestrado, si fuera este el caso dicho nodo que ha sido comprometido debe ser aislado de inmediato para evitar intrusiones no deseadas dentro de la red. La primera fase del modelo trata este problema y toma acción para detener el acceso a través de estos nodos, así como evitar el enrutamiento de paquetes utilizando los mismos como medio de comunicación.

5.2. Problema de Comportamiento No Deseado A Nivel de Enlace de Datos

En esta fase se tratan también los problemas de comportamiento inapropiado, realizando un análisis del estado de los paquetes y su comportamiento respecto a esta información, utilizando a sus vecinos como evaluadores de comportamiento y utilizando la estrategia de revocación de certificados cuando este tipo de problemas han sido detectados. La principal tarea de monitoreo de los nodos vecinos consiste en informar si efectivamente se han enviado las tramas correspondientes hacia su destino.

Los ataques de monitoreo o espionaje son prácticamente imposibles de realizar debido al esquema de autenticación utilizado, en el esquema presentado el nodo en primer lugar debe presentar sus credenciales para que se le asignen sus correspondientes credenciales y se autentique al nodo para que este pueda formar parte de la red. Transcurrida esta fase el nodo debe realizarse el firmado de la clave a través de un hashing en la capa de red, luego entra en funcionamiento el protocolo ARAN para el control del enrutamiento.

Así mismo los ataques de negación de servicio son prácticamente nulos debido al monitoreo permanente de los nodos vecinos y la revocación de credenciales que permanentemente está siendo monitoreado por los nodos CA de la red.

5.3. Manejo De Ataques A Nivel de red

En una segunda fase se evitan problemas de espionaje como por ejemplo de un doble agente quien utiliza sus credenciales para poder robar o redirigir información hacia otro nodo malicioso que captura información para su análisiso uso posterior.

En el caso de que se inicie un ataque del tipo Black Hole donde se pretende reenviar la información hacia otro nodo que se encuentra fuera de la red formando se puede detectar un comportamiento no deseado y se puede revocar los certificados con un tiempo de sanción para que el nodo no pueda transmitir o recibir información. El ataque de agujero de gusano es más difícil de tratar, pero al utilizar un sistema de autenticación y firma digital por hashing y al detectar un comportamiento no deseado a nivel de enlace o de red, el hecho de revocar un certificado en la capa de enlace conlleva la suspensión de transmisión en la capa de red.

En el caso de intentarse un ataque de suplantación de identidad, el protocolo ARAN a través de su mecanismo de control de encriptación fuerte puede comprobar a cada momento la identidad del nodo y comprobar su veracidad, así mismo este protocolo tiene la capacidad de determinar mensajes falsos de error que puedan haber sido fabricados con la intención de crear bucles en la red, pero debido a que todos los mensajes están firmados y a través de los sellos de tiempo utilizados se puede verificar la autenticidad de los mensajes de ruta generados, debido a estas características, el no repudio de los mensajes de error (ERR) le permite al nodo verificar que es el generador de estos mensajes en cualquier momento, sin embargo a pesar de demostrar su autenticidad si un nodo genera en exceso este tipo de mensajes sean estos fabricados u originales,

debido al comportamiento inusual, estos mensajes serán evitados y ya no formarán parte de la tabla de mensajes de error.

5.4. Manejo De Ataques A Nivel De Transporte

Para esta capa se pueden utilizar cualquiera de los sistemas de cifrado actuales que lo único que hacen es asegurar el canal para evitar infiltraciones o robo de información una vez que se ha pasado de las capas inferiores hacia esta. El uso de esquemas de cifrado como SSL con apoyo de AES, aseguramos el canal de transmisión como lo hacen muchas aplicaciones de accesos remoto de uso comercial, sin embargo lo primordial es asegurar las capas inferiores que se servirán de soporte a las capas superiores, es por ello que se ha pretendido reforzar el modelo desde el nivel de enlace, pasando por la utilización de un protocolo de enrutamiento seguro a nivel de red y siguiendo el reforzamiento hacia las capas superiores.

5.5. Verificación del modelo

Basado en el flujo de información del modelo se puede determinar lo siguiente:

- Transmitir la información en dos fases, ambas fases están siempre monitoreadas por las CA como se explica en la figura 4.2.1.1, con la primera de ellas ejecutándose en las capas inferiores obliga a que la información pase por filtros para poder realizar la comunicación entre nodos, ya que de otro modo esta no podría tener lugar. En la segunda fase en el momento mismo de iniciar los procesos de enrutamiento se realiza la firma de credenciales e iniciamos un proceso de control a nivel de la capa de red que está a cargo del protocolo de seguridad ARAN, el mismo que ya existe y está en proceso de mejoramiento.
- El esquema lógico de funcionamiento del modelo integra todas las actividades que forman parte de los requerimientos de seguridad y al utilizar protocolos ya existentes para todos estos procesos, no existen impedimentos para la construcción del mismo, ya que los protocolos utilizados existen, solamente habría que realizar unas pequeñas variaciones al modo de realizar la firma de hash en el protocolo ARAN, el cual según los autores se puede optimizar utilizando esquemas de hash, y en el caso de nuestro modelo donde ya se realiza la autenticación en una capa inferior, no debemos realizar la autenticación nuevamente en la capa de red sino solamente firmar la clave para de este modo optimizar el proceso de enrutamiento y tratamiento ante amenazas que los realiza el protocolo ARAN en la capa de red. Siguiendo este esquema lógico podemos decir que se puede reducir el nivel de amenaza y el compromiso de los nodos con el esquema de autenticación utilizado y la estrategia de preautenticación que se realiza previa la autenticación como tal.
- El modelo resultante esquematiza el proceso de protección de información, asegurando al canal en una primera fase mediante mecanismos de autenticación, los que posteriormente son reforzados en una segunda fase mediante mecanismos de control de enrutamiento y aseguramiento de las

capas superiores los que en definitiva resultaría en un blindaje del canal que difícilmente puede ser comprometido, ya que contamos con varias capas trabajando de manera integrada.

- Se ha seleccionado la verificación por diagrama de flujo debido a que la elaboración de un modelo de validación por simulación o matemático está más allá del alcance de este trabajo de investigación y habría requerido de muchos más recursos y tiempo de los estimados inicialmente.

CAPITULO VI

6. Conclusiones y Recomendaciones

6.1. Conclusiones

Los procesos de arranque y preautenticación llevados a cabo en la primera fase del modelo son una de las características más sobresalientes de este modelo, ya que se ejecutan a nivel de enlace de datos antes de iniciar operaciones de enrutamiento, lo que garantiza un primer nivel de aseguramiento evitando el no repudio de los nodos involucrados.

El uso de cadenas de hash evita la sobrecarga en el sistema, por lo que realizar este proceso asegurar un mejor rendimiento y un fortalecimiento adicional al esquema de autenticación al firmar la clave y realizando la correspondiente comparación con la función hash.

El monitoreo de los nodos en dos niveles asegura que la información que viaja a través del canal de comunicación establecido, reduce drásticamente el compromiso de los nodos cuyas acciones están bajo análisis de los nodos vecinos y bajo la supervisión de los CA diseminados a lo largo de la MANET.

La revocación de credenciales si bien es una acción penalizadora frente al comportamiento indeseado de los nodos, es también una medida absolutamente necesaria que se realiza a nivel de enlace de datos. Esta acción evita el robo o redirección de información hacia destinos fuera de la red, así como la falta de colaboración de los nodos intervinientes en los procesos de transmisión y mantenimiento de las tablas de enrutamiento.

Al realizar una comparación entre el modelo propuesto y mecanismos aislados de control podemos encontrar claramente las ventajas que ofrece la utilización de un modelo que asegure y controle la información transmitida en la red MANET, podemos encontrar varias ventajas que no podrían identificarse en modelos de seguridad cuyos mecanismos de control se reducen solo a la capa de red.

El diagrama de flujo presentado muestra el camino para minimizar los riesgos, mostrando el proceso y posibles variaciones dentro del flujo de información para lidiar con los nodos no colaborativos o con comportamiento indeseable para un buen desempeño de la comunicación, estas acciones conjuntas a fin de cuentas minimizarán los riesgos en ambientes hostiles.

6.2. Recomendaciones

Siempre debemos realizar una preautenticación de los nodos con el fin de evitar el repudio de los mismos, si es que los usuarios de los mismos pretendieran argumentar su falta de participación en el proceso de intercambio legítimo de información. Se recomienda utilizar la dirección MAC del nodo como primera credencial válida para iniciar la autenticación en sí.

Se recomienda para el proceso de autenticación utilizar un esquema basado en identidad, el mismo que requiere la presentación de credenciales como se describe anteriormente, una vez que se han presentado credenciales los nodos designados como CA otorgan las claves pública y privada al nodo tal como se explica en el funcionamiento del protocolo MANET-IDAKE en la Figura 4.2.1.1.

Realizar el hashing en la capa de red donde se inician las operaciones de enrutamiento de paquetes, evita la sobrecarga del sistema por lo que se recomienda poner en práctica estas funciones para evitar que las claves sean alteradas durante la transmisión de información y evitar también procesos computacionales demasiado complejos.

El monitoreo de los nodos debe realizarse en la capa de enlace de datos a través del mecanismo de informar el comportamiento inadecuado de los nodos vecinos, cuando es evidente una falta de colaboración, además en los procesos de enrutamiento deben manejarse mecanismos similares con el fin de evitar desvío o robo de información a nivel de red.

Mi recomendación para la Universidad es que apoye de mejor manera a los estudiantes de la modalidad abierta con literatura especializada permitiendo el

acceso a las librerías digitales y demás recursos para facilitar los procesos de investigación.

Se recomienda a los estudiantes de la modalidad abierta iniciar investigaciones en las áreas de seguridad de redes en especial de las redes Ad Hoc ya que se requieren mayores esfuerzos de estudio en esa área. El desarrollo del reforzamiento de seguridad frente el ataque de agujero de gusano puede ser un interesante tema de investigación, que contribuiría a la comunidad científica.

6.3. Trabajo Adicional

El modelo esquematizado está apenas en su primera fase y el trabajo futuro deberá enfocarse en optimizar y reforzar las medidas contra las vulnerabilidades que se puedan haber derivado de las acciones en cada capa. Sin embargo, se ha procurado mantener un esquema de procesamiento interrelacionado y sincronizado para evitar desfases o fallas intermedias en el proceso de comunicación y mantenimiento de rutas.

Es preciso realizar mayores contribuciones frente a los ataques de agujero de gusano, agujero negro y agujero gris, ataques que tienen lugar en la capa de red, ataques que representan serias amenazas debido a que sus mecanismos de operación son todavía difíciles de detectar, causando brechas de seguridad que pueden derivar en la disminución del rendimiento total de la red.

Los esfuerzos de investigación hacia las capas superiores del modelo pueden ser temas de investigación para futuras tesis, ya que en las capas superiores no se han descrito mayores detalles de funcionamiento y pueden existir muchas otras alternativas de protección en esos niveles, por ejemplo se pueden plantear mecanismos de detección y tratamiento de malware en redes móviles que funcionen a nivel de aplicación.

Las CA distribuidas son todavía una de las características de seguridad que deben mantenerse y el aseguramiento de las mismas y los mecanismos de reacción frente al compromiso de estos nodos deben ser desarrollados de tal modo que la red pueda operar de manera momentánea hasta que la CA pueda

ser sustituida y cumpla las funciones para las cuales ha sido designada, de ese modo se reforzaría todavía más aquellos nodos que cumplen las funciones de cualquier nodo de la red además de un monitoreo general de los nodos involucrados, ejecutando tareas de penalización hacia aquellos nodos que no están realizando un adecuado trabajo de comunicación.

Proponer el esquema de validación de este modelo ya sea a través de un modelo matemático o a través de simulación, lo cual contribuiría en gran medida los esfuerzos de la comunidad científica en esta área de estudio.

6.4. Referencias

[1] Tomas Krag, Sebastian Büettrich (2004-01-24); Wireless Mesh Networking; http://www.oreillynet.com/pub/a/wireless/2004/01/22/wirelessmesh.html.

[2] Tom Karigyannis, Les Owens, Wireless Network Security, Special Publication 800-48, National Institute of Standards and Technology NIST.

[3] Iván Vidal, Carlos García, Ignacio Soto, José Ignacio Moreno; Servicios de Valor Añadido en Redes Móviles Ad-hoc, Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid.

[4] N. Shanti, Dept. of ECE, National Engineering College, K.R.Nagar, Kovilpatti, DR.LGANESAN, Dept. of CSE, AlagappaChettiar College of Engineering and Technology, Karaikudi, DR.K.Ramar, Dept. of CSE, National Engineering College, K.R.Nagar, Kovilpatti, Tamil Nadu, India; STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK.

[5] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei; A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks; Department of Computer Science and Engineering Florida Atlantic University.

[6] Erdal Çayirci NATO Joint Warfare Centre, Norway Chunming Rong University of Stavanger, Norway, Security in Wireless Ad Hoc and Sensor Networks, A John Wiley and Sons, Ltd, Publication, 2009.

[7] Georgy Sklyarenko, AODV Routing Protocol, Institutf¨urInformatik, FreieUniversit¨at Berlin, Takustr.9, D-14195 Berlin, Germany.

[8] David B. Johnson, David A. Maltz, Josh Broch, DSR: The Dynamic Source Routing Protocol forMulti-Hop Wireless Ad Hoc Networks, Computer Science DepartmentCarnegie Mellon UniversityPittsburgh, PA 15213-3891.

[9] Yih-Chun Hu and Adrian Perrig Carnegie Mellon University, USA DAVID B. JOHNSON Rice University, USA; Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks.

[10] Adrian Perrig Ran Canetti J. D. Tygar Dawn Song, The TESLA Broadcast Authentication Protocol, Most of this work was done at UC Berkeley and IBM Research.The authors can be reached at adrian+@cs.cmu.edu, canetti@watson.ibm.com, tygar@cs.berkeley.edu, skyxd@cs.cmu.edu.

[11] Yih-Chun Hu Carnegie Mellon University, Adrian Perrig Carnegie Mellon University, David B. Johnson Rice University, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, Rice University Department of Computer Science Technical Report TR01-384 December 17, 2001, Revised: September 25, 2002.

[12] P. Papadimitratos and Z. Haas, Secure Routing for Mobile Ad Hoc Networks, in Proc. SCS CNDS, Jan. 2002.

[13] Kimaya Sanzgiri, Elizabeth M. Belding-Royer, Dep. Of Computer Science, University of California, Santa Barbara, Daniel La Flamme, Bridget Dahill, Brian Neil Levine, Dep. Of Computer Science, University of Massachusetts, Amherst, Clay Shields, Dep. Of Computer Science, Georgetown University, Whashington; Authenticated Routing for Ad Hoc Networks.

[14] Refik Molva and Pietro Michiardi, Security in Ad Hoc Networks, Institut Eurecom 2229 Route des Crêtes 06904 Sophia-Antipolis, France

[15] Yih-Chun Hu, Adrian Perrig, Carnegie Mellon University, Pittsburgh, David B. Johnson, Rice University; SEAD: secure efficient distance vector routing for mobile wireless Ad Hoc networks, Houston

[16] C. E. Perkins, P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, in proceedings of SIGCOMM 1994.

[17] J. Broch, D. A. Maltz, D. B. Johnson, Y-C Hu, J. G. Jetcheva, A performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols, in proceedings of MOBICOM 1998.

[18] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, M. Degermark, Scenario-based Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks, in proceedings of MOBICOM 1999.

[19] L. Buttyan, J.-P.Hubaux, Nuglets: a virtual currency to stimulate cooperation in self organized Ad Hoc networks, Technical Report DSC/2001/001, Swiss Federal Institute of Technology -- Lausanne, 2001.

[20] S. Buchegger, J.-Y. Le Boudec, Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks, in proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing.

[21] P. Michiardi, R. Molva, CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, IFIP - Communication and Multimedia Security Conference 2002.

[22] Khin Sandar Win, Analysis of Detecting Wormhole Attack in Wireless Networks, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay.

[23] A. Baruch, R. Curmola, C. Nita Rotaru, D. Holmer, H. Rubens; On the Survivability of Routing Protocols in Ad Hoc, Converence on Security and Privacy for Emerging Areas Communications, Wireless Networks.

[24] Luo, H., Zerfos, P., Kong, J., Lu S., and Zhang, L., Self-securing Ad Hoc Wireless Networks, Procedings of IEEE Symposium on Computers and Communications (ISCC), Italy, 2002.

[25] Tanenbaum, Andrew, Redes de Computadoras, Capítulo 8 – SEGURIDAD EN REDES – Páginas 785 - PEARSON EDUCACIÓN – México – 2003.

[26] Tanenbaum, Andrew, Redes de Computadoras, Capítulo 8 – SEGURIDAD EN REDES – Páginas 753 - PEARSON EDUCACIÓN – México – 2003.

[27] Helen Tang, Mazda Salmanian, Connie Chang; Strong Authentication for Tactical Mobile Ad Hoc Networks, defence Research and Development Canada; TECHNICAL MEMORANDUM DRDC Ottawa TM 2007-146 July 2007.

[28] IEEE 802.11, Standard Specifications for Wireless Local Area Networks, http://standards.ieee.org/wireless/

[29] Bellovin and Merritt. Encrypted key exchange: Password based protocols secure against dictionary attacks. In Proceedings 1992 IEEE Symposium on Research in Security and Privacy, pages 72–84. IEEE Computer Society, 1992.

[30] L. Lamport, Password authentication with insecure communication, Communication of the ACM, vol. 24, no. 11, 1981, pp. 770-772.

[31] A.Weimerskirch and D. Westho; Zero Common-Knowledge Authentication for Pervasive Networks; Tenth Annual International Workshop on Selected Areas in Cryptography (SAC 2003), 2003.

[32] A.Weimerskirch and D. Westho; Identity Certified Authentication for Ad-hoc Networks; Proceedings of the 1st ACM workshop on Security of Ad Hoc and sensor networks (SASN), 2003, ACM Press, ISBN:1-58113-783-4, 2003, pp. 33-40.

[33] L. Zhou and Z.J. Haas.Securing Ad Hoc Networks, IEEE Network Journal, vol. 13, no. 6, 1999, pp. 24-30.

[34] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang.Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks, International Conference on Network Protocols (ICNP) 2001, 2001.

[35] A. Shamir. Identity-based Cryptosystems and Signature Schemes, Advances in Cryptology-CRYPTO '84, G.R. Blakley, D. Chaum (Eds.), LNCS 196, Springer-Verlag, pp. 47-53, 1984.

[36] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen, Institute of Computing Technology, School of Software Tsinghua University, Computer Network Information Center of Chinese Academy of Sciences, Computer Network Information Center of Chinese Academy of Sciences, Bell Labs Research China

[37] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions , UCLA Computer Science Department.

[38] Katrin Hoeper and Guang Gong, Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation, Department of Electrical and Computer Engineering University of Waterloo, Waterloo, ON, N2L 3G1, Canada.

ANEXOS