

Detección de Intrusos en Redes Inalámbricas Ad-Hoc usando Agentes Móviles Cooperativos (Preguntas sobre el tema)

Carlos Felipe Téllez Castaño
Junio 2006

En general, para redes MANET (Mobile Ad-Hoc Network) es necesario tener en cuenta las limitaciones atribuidas por las características propias de este tipo de redes. Estas características son las limitaciones de energía, la topología dinámica, los enlaces de ancho de banda limitado y de capacidad variable, la capacidad de procesamiento en los nodos y la seguridad física limitada. Esto, sin dejar de lado el alcance de las Garantías de Calidad del Servicio, que podrían llegar a proporcionar el descubrimiento, de servicios de valor agregado en este tipo de redes con topología variable. Todas estas características, muestran un reto en la investigación para alcanzar una estabilidad y una estandarización, definida para el trabajo con dispositivos móviles que tengan un rendimiento óptimo y confiable. Sin embargo, para el presente proceso de investigación, se desea realizar un aporte en materia de Detección de Intrusos y generalmente en Seguridad, para las redes inalámbricas con nodos móviles. La detección de intrusos, se basara en un sistema de Agentes Móviles que realizan tareas de forma cooperativa y que deben proporcionar QoS en la red.

Seguridad, QoS y enrutamiento:

Teniendo en cuenta, que se deben cumplir requisitos de confidencialidad, integridad, autenticación, no-repudiación y disponibilidad, para garantizar la seguridad en las redes inalámbricas móviles Ad-Hoc:

- ¿Cuál sería el algoritmo de enrutamiento efectivo sobre el que debería estar soportado un sistema de detección de intrusos basado en agentes móviles cooperativos, que sea funcional y que además, garantice QoS en la Red?

El planteamiento de esta pregunta, es debido a que los distintos algoritmos de enrutamiento para redes Ad-Hoc se dividen en tres grandes grupos: algoritmos proactivos, algoritmos reactivos y protocolos basados en clustering o agrupamiento por densidad de nodos. Esto afecta el comportamiento del IDS (Sistema de Detección de Intrusos) y mucho más si se trabaja con agentes móviles que pretenden garantizar QoS.

Estandarización y Mecanismo Apropriado de IDS:

Dentro de los ataques que se pueden proporcionar a una red MANET, se encuentran una gran variedad de métodos de intrusión, así como mecanismos de desrutamiento y daño a la red. Ya existen algunos algoritmos usados para detectar este tipo de anomalías, sin embargo, al mayoría sólo las detecta, no las ataca, otros son muy puntuales, pues atacan un problema específico, y para atacar todo tipo de problemas tendrían que usarse todo tipo de soluciones es decir usar varios algoritmos sobre limitadas redes como las MANET y otros problemas se encuentran sin forma de ser contrarrestados:

- ¿Qué tipo de Mecanismo IDS se puede diseñar, de tal forma que sea aplicable para cualquier tipo de problema de seguridad y que además ataque puntualmente el problema de intrusión, garantizando que se realice una estandarización para los equipos móviles, en su opción de conectarse con una red Ad-Hoc?