RESUMEN DEL PROYECTO DE TESIS

La seguridad en redes de computadores es un tema que ha sido extensamente investigado. Esa investigación se justifica al observar las dimensiones del problema que se afronta. Es fácil identificar diferentes tipos de redes, una gran cantidad de protocolos de red, y una cantidad ingente de aplicaciones de usuario que hacen un uso extensivo de las redes para llevar a cabo la tarea para la que fueron diseñadas. Todo ello conforma un vasto campo de investigación, donde es posible para un investigador fijar su interés en un conjunto de amenazas, vulnerabilidades o tipos de ataques, y diseñar mecanismos para prevenir el ataque, mitigar sus efectos o reparar los daños causados, basándose en las características específicas de cada escenario.

Nuestro grupo de investigación en Redes de Computadores ha estado trabajando en ciertos tipos de riesgos para la seguridad de las redes de computadores, especialmente aquellos que afectan a las redes inalámbricas. En trabajos doctorales previos, se han propuesto métodos de detección y exclusión para enfrentarse a nodos maliciosos en redes móviles ad hoc (MANETs), desde el punto de vista de cada nodo de la red por separado, utilizando una técnica llamada Sistema de Detección de Intrusiones (IDS, de Intrusion Detection Systems) basada en Watchdogs. En este ámbito, se pretende optimizar la productividad de la red exluyendo de la misma a aquellos nodos cuyo comportamiento no sea considerado adecuado por sus nodos vecinos, de forma que no participen en los diferentes procesos de comunicación de la red. Esta tarea la desarrollarán específicamente los sistemas basado en Watchdogs.

Cuando las técnicas de seguridad aisladas en cada nodo obtienen buenos resultados con un tipo de ataques, una posible manera de mejorar esos resultados podría ser el establecimiento de un mecanismo de cooperación entre nodos legítimos para intercambiar información, de forma que se acelerase la detección de nodos maliciosos y se incrementase la exactitud de la detección. Obviamente, un mecanismo de este tipo tiene unos costes en términos de información transmitida por la red, y en necesidades de computación en el nodo para el análisis de la información recibida y la obtención de una opinión sobre un nodo concreto. La clave es equilibrar adecuadamente la sobrecarga que estos mecanismos introducen con las mejoras obtenidas si se les compara con mecanismos no colaborativos.

El principal objetivo de esta tesis es explorar la aplicabilidad y el rendimiento que los mecanismos cooperativos pueden alcanzar, al ser utilizados por nodos de redes inalámbricas entre pares, para afrontar ciertos tipos de riesgos de seguridad, como nodos egoístas o nodos de tipo 'black hole'. Lógicamente alineados con investigaciones previas de nuestro grupo, enfocaremos nuestra atención sobre las redes MANET.

La utilización de watchdogs en estas redes inalámbricas sin infraestructura suele conducir a la obtención de una gran cantidad de detecciones incorrectas, tanto por el lado de los falsos positivos como de los falsos negativos, debido a las características del canal como a la movilidad de los nodos. Nodos legítimos pero detectados como maliciosos pueden conducir a la partición de la red. Nodos maliciosos no detectados pueden dañar los procesos de comunicación entre los restantes nodos. Por tanto, esta investigación debe centrarse en mejorar dos métricas del proceso de detección: exactitud, recuciendo la aparición de falsos positivos y falsos negativos; y velocidad de detección, esforzándose para obtener una caracterización de cada nodo sospechoso lo antes posible. Nuestra percepción es que los métodos colaborativos mejorarán ambas métricas, comparados con métodos no colaborativos.