Capítulo 8

8. Sincronización y Seguridad

8.1 Coordinación en tiempo

Por ejemplo, si el movimiento de un carro es detectado en dos tiempos diferentes a lo largo de un camino, mucho antes de determinar en que dirección el carro se mueve, debemos de ser capaces de comparar significativamente los tiempos adquiridos. Así mismo, claramente debemos transformar estos dos tiempos de detección en una referencia que permita conocer la dirección y velocidad del vehículo.

La estimación de la diferencia de los tiempos entre los nodos es parte importante en la localización de los nodos [ELS01]. Por ejemplo, muchos de los algoritmos de localización usados para estimar la distancia entre los nodos intermedios, requieren medir el tiempo que toma en transmitir la información de un nodo a otro. Otros factores que influyen para la sincronía es la velocidad que se tiene dependiendo del medio de propagación para el tipo de señal que se usa.

Mientras que en el mundo alámbrico, los protocolos de tiempo de sincronización tales como NTP [MIL94] han sido exitosos y ampliamente usados para lograr una coordinación de tiempo universal (UTC), está solución sin

embargo, no pueden ser transferida fácilmente a las redes inalámbricas de sensores. Esto protocolos alámbricos, asumen la existencia de relojes maestros de alta precisión en los nodos de la red (relojes atómicos) y, aún más importantes, ello requieren que los pares de nodos estén conectados y experimenten comunicación constantemente en los intercambios de información.

Desafortunadamente, ninguna de estas suposiciones es generalmente válida en las redes de Sensores, ya que no existen relojes maestros disponibles, las conexiones son efímeras y los retrasos en la comunicación son inconsistentes e impredecibles.

8.2 Retrasos en la Comunicación

Los relojes en las computadoras funcionan en base a osciladores, que proveen el tiempo local de cada sensor en la red. A un tiempo t el reloj de la computadora indica el tiempo $C(t)$, el cual puede o no ser el mismo que t.

Para un reloj perfecto de hardware, la derivada de $dC(t)/dt$ debería ser igual a 1. Si este no es el caso, estamos hablando de un reloj que sesga. Este reloj puede tener cambios en base a las condiciones ambientales, tales como la temperatura y humedad, pero debemos asumir que este se mantiene limitado o restringido a estar cerca de 1.

$$1-\rho \leq \frac{dC(t)}{dt} \leq 1+\rho \qquad \text{(Ec. 8.1)}$$

donde,

ρ = sesgue máximo (valor típico de ρ es de) [ELS01].

t = tiempo real.

$C(t)$ = tiempo del dispositivo de computo.

$dC(t)/dt$ = derivada tiempo del dispositivo de computo con respecto al tiempo real.

Una pequeña fluctuación en el sesgue es usualmente modelado con un ruido aleatorio Gausiano [ELS01]. Es importante que dado que existe un sesgue, inclusive en los relojes de dos nodos sincronizados, se puede presentar que a un punto dado de tiempo en el futuro no estén sincronizados.

Para que los nodos se encuentren sincronizados, debemos tener por un periodo un canal de comunicación donde la transmisión de mensaje pueda ser estimada confiablemente. La actividad en el canal puede descomponerse en cuatro partes [ELS01]:

- Tiempo de envío: es el tiempo que le toma al que envía construir el mensaje, añadiendo los retrasos por las operaciones de llamada del sistema, switcheo y el acceso de la información a la interfase de la red.

- Tiempo de acceso: este retraso ocurre mientras se está en espera de acceder al canal de transmisión debido a la contención, colisiones y similares.
- Tiempo de propagación: es el tiempo que le lleva al mensaje viajar a través del canal al nodo destino. Este puede ser altamente variable.
- Tiempo de recepción: este tiempo es de la parte de la interfase de la red del lado del receptor para adquirir el mensaje y notificar al nodo destino de su llegada.

Por ello, debemos satisfacer la necesidad de sincronía de manera local en vez a lo global, como procesos de colaboración. En suma, para muchas aplicaciones que involucran un razonamiento en cuanto al tiempo del sensado del fenómeno de estudio, solo el tiempo cuando se solicita la detección de un evento importa.

Adicionalmente a la Sincronía, se tiene un factor muy importante como la Seguridad en las redes de Sensores. Esto como resultado en parte a los ataques que sufren estos sistemas de comunicación como se menciona enseguida.

8.3 Vulnerabilidad

Dado que las redes de Sensores tienen una comunicación inalámbrica, la cual presenta vulnerabilidad a una gran variedad de ataques. La seguridad muy importante dado que los nodos sensores que conforman la red, cooperan y colaboran entre sí, con confianza para detectar el evento en un área cualquiera e

informar del mismo. En un conjunto de nodos sensores en una localidad dada, el intercambio de información mediante los enlaces debe tener un alto grado de certeza.

Los tipos de ataques básicos que pueden sufrir estas redes a nivel capa de red se en listan en [KAR03]. La criptografía es una solución que se basa en claves simétricas y publicas, más no encajan del todo dado que se requiere de un alto procesamiento en los nodos y esto no cuenta con esa capacidad de cómputo.

Protocolos de ruteo puede verse afectados por **Spoofing** o ruteo alterado durante el intercambio de información entre los nodos. *Spoofing* es una técnica en la cual el acceso a las computadoras no es permitido, por el que un nodo o dispositivo intruso tiene como tarea enviar mensajes a otros nodos con una identificación diferente a la real, indicando que el mensaje está viniendo de un nodo confiable dentro de la red sin ser cierto. El nodo intruso busca obtener una identificación para impersonificar al nodo confiable. Ya después modifica información que luego envía a los jefes de conjuntos o nodos centrales. Eso podría llevar a errores en el ruteo, mayor índice de ruptura con los enlaces de comunicación, llegando a que la red se encuentre segmentada.

Un ataque tipo **Sybil** [DOU02] ocurre cuando un nodo se presenta de múltiples formas a los nodos de la red. Esto ocasiona un mal funcionamiento en algoritmos de ruteo que funcionan en base a la geografía del la red. La encriptación y la autentificación comparten de manera global una llave que previene este tipo de ataques que pretende corromper el intercambio de mensajes en la red.

Un ataque selectivo por otra parte, se da cuando ciertos nodos no retransmiten la información. Dado que una red de Sensores sustenta la comunicación por medio de repeticiones de mensajes de información a través de los nodos, es importante que se difunda la información. Un ejemplo claro es un ataque **Sinkhole**, donde un nodo corrupto se ve favorecido dado el alto índice de intercambio de información. En este caso el rutea la información pretendiendo ser un nodo central que almacena y coordina la información. De esta forma, influye en muchas de las tareas que los nodos deben realizar. Otra tipo de ataque es el **Wormhole**, donde el tráfico se ve afectado, ya que la información se manda por enlaces muy largos y con poca eficiencia en el ancho de banda. Los nodos son engañados, ya que las tablas de ruteo son alteradas. Estos dos tipos de ataques son difíciles encontrar dado que la información que brindan los nodos es muy difícil de verificar en cuanto a su veracidad.

No obstante, protocolos geográficos de ruteo no se ven afectados por estos ataques, ya que los enlaces se analizan en base a las coordenadas de localización de los nodos, por lo que las distancias pueden ser verificadas. Algunos de los protocolos que pueden mejorar la calidad en una red de Sensores son:

- Localización de Encriptación y Autentificación (LEAP) [ZHU03].
- Ruteo Tolerante a Intrusos [DEN03].
- Seguridad en redes de Sensores [PER01].