**Resumen**

* Asume que el tráfico de paquetes puede es útil para modelar tano el comportamiento de los nodos de una WSN, como la misma WSN.
* Presenta una metodología para realizar dicho modelado.
* Muestra como las anomalías de la red pueden ser detectadas a partir del monitoreo de la evolución del perfil de comportamiento nodo/red.

**Introducción**

* El rango de actividades de los nodos, así como de la red, se manifiestan en el tráfico de paquetes.
* Por lo que el tráfico de paquetes es una fuente de datos útil para modelar tanto el comportamiento de los nodos individuales, como de la red en su totalidad.
* La interacción de personas con una WSN se da a través de interface predefinidas, por lo que el impacto de incertidumbre subjetiva en un nodo y en la red se minimiza.
* Debido a que el comportamiento de un nodo/red de sensores se puede modelar, entonces es posible obtener perfiles nodo/red.
* Debido a que los problemas de fiabilidad y de seguridad pueden causar cambios a otros perfiles de comportamiento red/nodo, entonces con el monitoreo de la evolución de perfiles de red/nodo (i.e. basado-en-tráfico-de-paquetes) es posible detectar anomalías.
* En el artículo se muestra la detección de anomalías en la WSN, para mejorar la seguridad y fiabilidad de la red.

**Modelado básico de paquetes de tráfico**

* La tarea del modelado de tráfico es encontrar propiedades, estadísticamente invariantes, del tráfico de paquetes. Las cuáles pueden ser usadas para identificar los tipos de tráfico de paquetes.
* El tráfico puede ser diferenciado por sus aplicaciones, asociadas, ubicación, tiempo, etc.
* Algunas características que son utilizadas para caracterizar el tráfico de paquetes son: tamaño y longitud del tren de paquetes, tiempo entre paquetes y el tamaño de la carga útil.
* [2] De acuerdo a su implementación subyacente, las características de tráfico se pueden agrupar en: características básicas, características basadas en tiempo y características basadas en conexión

|  |  |
| --- | --- |
| Características básicas | Tipo de protocolo, dirección de fuente/destino, tamaño de la carga útil |
| Características basadas en tiempo | Tiempo entre paquetes, frecuencia, secuencia de paquetes |
| Características basadas en conexión | Tamaño del tren de paquetes, longitud del tren de paquetes |

* Una o varias combinaciones de características de tráfico pueden ser usadas para un modelo estadístico de cierto tipo de tráfico de paquetes.
* En WSN el tráfico asociado a un nodo puede ser usada para modelar el comportamiento de dicho nodo.
* El tráfico de encaminamiento puede ser usado para modelar protocolos de encaminamiento, ETC.

**Modelado del Perfil de Nodo**

* Para modelar un nodo, únicamente podemos usar el conjunto de paquetes observados por dicho nodo.

*Modelado de un perfil basado en secuencia de paquetes*

* Un ejemplo de secuencia es que un mensaje de Routing Reply (RREP) siempre viene después de un mensaje de Routing Request (RREQ), esto es especificado por el protocolo de encaminamiento.
* [3] se propone usar una maquina finita de estados (FSM) para especificar el comportamiento correcto de vector de demanda ad hoc (AODV[[1]](#footnote-1)).
* [4] Usa un modelo FSM para corregir en comportamiento de encaminamiento para otro protocolo de encaminamiento.
* Mediante las especificaciones de secuencia es posible modelar las relaciones entre algunos tipos especiales de paquetes.
* Mediante entrenamiento pueden aprenderse las relaciones entre tipos generales de paquetes (en [5] el mismo autor presenta una metodología para esto).
* [5] El conjunto, de relaciones de secuencia de paquetes, aprendido es único para cada nodo. Un nodo es modelado únicamente por sus relaciones de secuencia de paquetes.

*Clasificación de Paquetes*

* Propone clasificar los paquetes de manera que el conjunto de categorías obtenidas puedan ser mapeadas a un conjunto de caracteres single-byte ASCII.
* También propone que la secuencia de relaciones aprendida (a partir del conjunto anterior) pueda reflejar únicamente el comportamiento del nodo de interés.
* **Ejemplo: *Clasificación*** de acuerdo a: tipo de paquete y {fuente, destino},
  + Para controlar el número de categorías y hacer un esquema escalable de clasificación de paquetes se mapea el espacio real de direcciones de nodo aun espacio abstracto de direcciones.
  + Espacio abstracto de direcciones {yo; vecino; local; no-local; y sink/cluster-head} esta clasificación se hace desde la perspectiva del nodo de interés.
  + local son los nodos que mediante aprendizaje (del destino y la fuente de los nodos que ha transportado) conocen al nodo de interés.
  + Durante el aprendizaje ningún nodo puede ser clasificado como no-local.
  + Cuando se tiene un conjunto estable de nodos clasificados, si se hace una clasificación no-local, esto puede ser señal de una anomalía.
  + ***Traducción,*** paquete-mapeo-traducción



* + ***Extracción de paquetes,*** ejemplo, si consideramos el tamaño de paquete k=4 y tenemos la siguiente secuencia de arribos AABBDCC

Podemos obtener el siguiente conjunto de patrones: AABB, ABBD, BBDC y BDCC. Podemos refinar más el método de extracción de patrones si consideramos que los paquetes son usualmente enviados por ciertas conexiones.

El tiempo entre paquetes puede indicar aproximadamente cuando se trata de dos paquetes sucesivos que provienen de diferentes conexiones.

El conjunto de patrones puede ser reducido si consideramos solo los patrones que han sido observados en los últimos 2 o más instantes.

El máximo tamaño de patrones sólo debe ser considerado cuando un patrón contiene otro patrón que tiene el mismo número de ocurrencias.

*Modelado de perfil de nodo basado en tráfico de la fuente*

* En los escenarios de recolección de datos event-driven, cuando un evento de interés se detecta, la fuente de tráfico puede surgir en una esquina del área monitoreada.
* [8] Se ha simulado el arribo de tráfico en una WSN event-driven.
* [9] Aunque no hay un fundamento sólido para hacerlo, pues los procesos de Poisson suponen un modelo ON/OFF.
* Como los sensores son independientes entre sí, cada uno sólo depende sólo de sus propiedades físicas y de su ambiente, entonces los modelos de fuente basados en aprendizaje pueden ser usados para especificar el perfil de comportamiento de un nodo.

*ON/OFF Model*

**

* Algunas de las propiedades que se pueden obtener de este modelo son: el número de periodos ON en intervalo dado, la distribución de la duración de los periodos ON, la distribución de la duración de los periodos OFF
* Esas propiedades se pueden aprender cuando el modelo ON/OFF se aplica para modelar la fuente de tráfico asociada a un sensor dado.
* El modelo ON/OFF junto con sus propiedades de aprendizaje especifican el perfil d la fuente de tráfico de un sensor.

*Caso de Estudio: Fuente de tráfico modelada para el seguimiento de objetivos en WSN*

* Una WSN típica para el seguimiento de objetivos, se forma de una distribución de nodos que monitorean colaborativamente un objetivo móvil. El objetivo será descubierto cuando este en el área de monitoreo de algún nodo.
* Se realizó una simulación [9], encontrando que los nodos experimentan diferentes tipos de situaciones de reporte de datos, esto depende de su localización y el modelo de movilidad que usa el objetivo móvil.
* Aplicando el modelo ON/OFF a la simulación, se encontró que el tráfico de la fuente para cada nodo se describe únicamente en términos de la frecuencia de observación de los periodos ON, la distribución de duración de los periodos ON y de los periodos OFF. Esto provee un perfil para el nodo de interés.

**Modelado del Perfil de la Red**

* Además del perfil de los nodos, también la red completa puede ser modelada identificando las estadísticas invariantes que se exhiben en el tráfico de paquetes de toda la red.

*Monitoreo del Tráfico de Paquetes de Toda la Red*

* + Como todos los paquetes en una WSN vana hacia el sink, se puede adjuntar un monitor de tráfico en la estación base.

*Clasificación del Tráfico de Paquetes de Toda la Red*

* + Las características que describen un (o un grupo de) paquetes es visto como un vector de características de datos, ie que tenemos un conjunto de vectores de datos que describen el paquete de paquetes en toda la red.
  + Para hacer la clasificación podemos aplicar un algoritmo de clustering que encuentre la estructura del conjunto de datos de la red.

*Caso de Estudio: Agrupando Nodos Sensores*

* + Tenemos un WSN con los siguiente tipos de sensores:
    1. 10 sensores de CO2, hacen reportes periódicos (12veces/hora)
    2. 10 sensores de temperatura que hacen 60 reportes/hora
    3. 10 sensores detección, reportan datos de acuerdo a una distribución de Poisson con media de 15 reportes/hora
  + Asumimos que todos los paquetes tiene un retardo caracterizado por ruido Gaussiano N(0,4).
  + Para cada nodo i se guardan 100 lecturas (*xi,1..10*) de sus arribos por hora al sink.
  + A partir de las lecturas tomadas, la media y la varianza son representaciones del nodo i, ie cada nodo tiene dos coordenadas asociadas [media, varianza].



* + A partir de la gráfica anterior usamos K-means para clasificar los tipos de nodos.
  + Vemos que con este método podemos clasificar a los nodos cuando no tenemos un conocimiento previo de los tipos de nodos de la red.

**Detectando Anomalías a partir de Perfiles de Nodo/Red**

* Debido a que un nodo solo desempeña sus operaciones necesarias y especificadas, entonces tenemos como único perfil nodo al conjunto de secuencias de paquetes aprendidas.
* Una vez que se tiene un conjunto estable de patrones cualquier otro patrón o paquete subsecuente que pase por el nodo de interés puede ser señal de anomalía.

*Relacionar Patrones y Alarmas*

* Hacer esta relación es similar a hacer la extracción de patrones.
* Cada que llega un paquete se mapea con una ventana de patrones, si ningún patrón coincide hay un mismatch.
* Sean a y b dos secuencias de caracteres de tamaño k, si ai representa el carácter en la posición i, entonces podemos hacer la relación de la sig. Manera (mide la distancia entre ambas secuencias y se define un umbral de distancia mínimo para hacer la relación)



*Caso de Estudio: Descripción de Ataque Sinkhole*

* Algunos de los ataques que se pueden detectar con esta metodología son: spoofing, sinkhole y warmhole [5] Aquí se explicara la detección de sinkhole.
* Sinkhole es un nodo malicioso que atrae la creación de ruta hacía él, es decir actúa como un sink. Para ello el sink hole aparece muy atractivo para los demás nodos, es decir con rutas más cortas o rápidas.
* Este ataque puede violar el perfil normal del nodo malicioso, ya que atrae rutas que, en una situación normal, no pasarían a través de él. Algunos paquetes no-locales pueden observarse durante el ataque en el sink hole, por lo que al no coincidir los patrones se pueden asociar alarmas.

*Detectando Periodos ON/OFF Anormales*

* Anteriormente se llegó a utilizar un modelo ON/OFF para representar el comienzo abrupto de envío de paquetes para una fuente event-driven.
* Ya que la probabilidad de escuchar periodos ON/OFF largos, entonces un periodo ON inusualmente largo puede sugerir que el nodo está teniendo un ataque de eliminación de energía. Por otro lado un periodo OFF largo puede indicar un fallo en el link o en un nodo.

*Metodología de Detección de Periodos ON/OFF Anormalmente Largos*

* + Ya que la distribución de las duraciones de los periodos ON/OFF pueden ser aprendidas después de cierto periodo de tiempo, de la misma manera podemos obtener los límites superiores probabilísticos para diferentes periodos de ON/OFF. Figura 6
  + [9] Por ejemplo para una WSN que sigue un objetivo móvil se tiene que los periodos de seguimiento ON/OFF son cortos, ósea que en este caso con seguridad se puede detectar una anomalía a tener haber un inusual periodo largo de ON/OFF.



*Detectando Cambios en los Perfiles de la Red*

* Los cambios en el comportamiento de nodos individuales de la red o de enlaces provocan cambios en el perfil de la red.
* Al detectar cambios en el perfil de la red se pueden detectar anomalías, considerando las similitudes entre las actualizaciones del perfil de la red y los viejos perfiles.
* Los cambios en el nuevo perfil de la red se pueden detectar revisando la similitud entre la nueva clasificación de los objetos de la red y la vieja clasificación.

*Medidas de similitud entre dos clasificaciones*

1. La rutas se crean bajo demanda, cuando se solicita una ruta (RREQ), propagación de al información se crea una y cuando se obtiene se envían un RPLEY al origen [↑](#footnote-ref-1)